Privacy Impact Assessment for the VA IT System called:

Government Community Cloud – Enterprise Veterans Affairs Central Office (VACO) Infrastructure Operations

Date PIA submitted for review:

January 13, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	(202) 632-8423
Information System Security Officer (ISSO)	Joseph Decoteau	Joseph.Decoteau@va.gov	(802) 624-2480
Information System Owner	Prashanthi Kuchikulla	Prashanthi.Kuchikulla@va.gov	(202) 277-9536
Record Officer	Jannette D. Street	Jannette.Street@va.gov	(264) 455-5055

Abstract

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

ServiceNow is a single, unified platform with a shared data model. ServiceNow is a Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) with strong origins in Information Technology (IT) Service Management (ITSM) anchored to the Information Technology Infrastructure Library (ITIL) framework. The official registered system name is Government Community Cloud – Enterprise (GCC-E) but the Commercial off the Shelf (COTS) IT system acronym is ServiceNow-High-Enterprise. This instance is owned and operated by the Veterans Affairs (VA) Office of Information Technology (OIT) – Infrastructure Operations (IO). ServiceNow data resides in a Federal Risk and Authorization Management Program (FedRAMP) approved Cloud environment. ServiceNow empowers organizations to automate business workflow processes and connects various data sources on a single data model. Many common non-IT business functions, such as Human Resources and Finance, are available as licensable modules. Configuration of the environment is possible and allows each organization to leverage the platform in multiple ways that save time, improve work, and provide insight into operations. ITIL framework capabilities are embedded in SaaS capabilities, to include Incident Management, Problem Management, Change Management, Release, Service Request, Service Level Management and Reporting, Integrated Configuration Management Database (CMDB), Asset Management, Knowledge Management, IT Business Management (ITBM) and IT Operations Management (ITOM).

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. The IT system name and the name of the program office that owns the IT system.

The official VA registered system name is Government Community Cloud – Enterprise (GCC-E) but the Commercial off the Shelf (COTS) IT system name is ServiceNow. This instance is owned and operated by the Veterans Affairs (VA) Office of Information Technology (OIT) – Infrastructure Operations (IO). When referenced throughout this document, the identified name of the information system will be ServiceNow.

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

The purpose of the IT system is to allow business process automation and, at the maximum benefit to the Government, any existing service management tools requiring modernization via ServiceNow. The scope includes the people, processes, and tools required to provide a healthy, reliable, scalable, interoperable, and adaptable service management solution inclusive of software configuration, development, testing, integration, modernization, expansion, customization, implementation, provisioning, administration, and operations and maintenance support services.

ServiceNow empowers organizations to automate business workflow processes and connects various data sources on a single data model. Many common non-IT business functions, such as Human Resources and Finance, are available as licensable modules. Configuration of the environment is possible and allows each organization to leverage the platform in multiple ways that save time, improve work, and provide insight into operations. ITIL framework capabilities are embedded in SaaS capabilities, to include Incident Management, Problem Management, Change Management, Release, Service Request, Service Level Management and Reporting, Integrated Configuration Management Database (CMDB), Asset Management, Knowledge Management, IT Business Management (ITBM) and IT Operations Management (ITOM).

C. Indicate the ownership or control of the IT system or project.

The official VA registered system name is Government Community Cloud – Enterprise (GCC-E) but the Commercial off the Shelf (COTS) IT system name is ServiceNow. This instance is owned and operated by the Veterans Affairs (VA) Office of Information Technology (OIT) – Infrastructure Operations (IO).

ServiceNow provides a highly available cloud infrastructure through its Advanced High Availability (AHA) architecture. As ServiceNow's data centers are arranged in pairs, all customer production data is hosted in both data centers simultaneously and kept in sync using real-time asynchronous database replication. Both data centers are always active, in a master- master relationship, with data replicated from the active (read-write) data center to the passive (read-only) data center. Each single data center in a pair is implemented so it can support the combined production load of both locations. Within the regional data center pair there is no concept of a fixed primary location for any customer instance. Although requests are not being actively served from both data centers at the same time, they are both "warm" at all times. As there is no data center affinity mechanism, two instances from the same customer could be operating out of different data centers at the same time. ServiceNow has two distinct processes relating to ensuring instance availability: transfers and failover.

The Cloud Service Provider (CSP) contract details the accountability, security, and privacy of VA data. A prohibition on unauthorized disclosure: "Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA." This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data – General, FAR § 52.227-14(d).(1).

A requirement for data breach notification: Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access, the Contractor/Subcontractor shall immediately notify the Contract Officer Representative (COR), including the designated ISO, and Privacy Officer (all three) for the contract. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. See VA Handbook 6500.6, Appendix C, paragraph 6.a.

A requirement to pay liquidated damages in the event of a data breach: "In the event of a data breach or privacy incident involving Sensitive Personal Information (SPI) the contractor processes or maintains under this contract shall be liable to VA for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals." However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports
3) Data breach analysis
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

A requirement for annual security/privacy awareness training: "Before being granted access to VA information or information systems, all Contractor employees and Subcontractor employees requiring such access shall complete on an annual basis either: (i) the VA security/privacy awareness training (contains VA security/privacy requirements) within 1 week of the initiation of the contract, or (ii) security awareness training provided or arranged by the contractor that conforms to VA's security/privacy requirements as delineated in the hard copy of the VA security awareness training provided to the Contractor. If the Contractor provides their own training that conforms to VA's requirements, they will provide the COR or CO, a yearly report (due annually on the date of the contract initiation) stating that all applicable employees involved in VA's contract have received their annual security/privacy training that meets VA's requirements and the total number of employees trained. See VA Handbook 6500.6, Appendix C, paragraph 9.

A requirement to sign VA's Rules of Behavior: "Before being granted access to VA information or information systems, all Contractor employees and Subcontractor employees requiring such access shall sign on annual basis an acknowledgement that they have read, understand, and agree to abide by VA's Contractor Rules of Behavior which is attached to this contract." See VA Handbook 6500.6, Appendix C, paragraph 9, and Appendix D. Note: If a medical device vendor anticipates that the services under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the vendor's designated representative. The contract must reflect by signing the Rules of Behavior on behalf of the vendor that the designated representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing VA's information and information systems.

The disclosure or breach of ServiceNow data could cause irreparable harm to the CSP and the individuals based on the data in the system identified below in 1.1.

2. Information Collection and Sharing

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

ServiceNow is expected to have 500,000 – 600,000 users of the system. ServiceNow stores data for all users and more than 20 million Veterans. This is a system hosted in a FedRAMP certified government cloud (categorized high) and does not fall under a region.

E. A general description of the information in the IT system and the purpose for collecting this information.

The purpose of the IT system is to allow business process automation and, at the maximum benefit to the Government, any existing service management tools requiring modernization via ServiceNow. The scope includes the people, processes, and tools required to provide a healthy, reliable, scalable, interoperable, and adaptable service management solution inclusive of software configuration, development, testing, integration, modernization, expansion, customization, implementation, provisioning, administration, and operations and maintenance support services.

A ServiceNow instance generates detailed log and audit information regarding activities which take place within it. ServiceNow's default application logging capabilities include verbose transaction, client, event, email, and system logs. Refer to the "ServiceNow Audit Management Policy," section 4.2 Audit Generation, for more information.

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

ServiceNow maintains the underlying physical infrastructure. A Memorandum of Understanding and Interconnection Security Agreement's (MOU/ISA) is required between the VA and VA contractors when VA data is stored or processed external of the VA security boundary. The vendor specific agreements will describe the data ownership and storage requirements. The parties agree that transmission, storage, and management of VA sensitive information residing in ServiceNow is the sole responsibility of the VA employees or designated contractors/vendors assigned to manage the system. Thus, all agreements on data and system responsibilities will not be covered in this base agreement (MOU/ISA).

ServiceNow is a major application and contains the following functionalities:
Enterprise Asset Management: Nuvolo. Nuvolo's suite of applications help organizations solve business problems with various capabilities for aligned to Operation Technology Management for Healthcare, Labs, Manufacturing and Facilities. Collect and monitor VA Medical Facility assets.

IT Asset Management: Asset Management. Asset Management automates your IT asset lifecycles with intuitive workflows. Make informed decisions about asset capacity, refresh, and vendors. Collect and monitor VA Commodity and Infrastructure Operation (IO) Assets.

IT Asset Management: Software Asset Management. Software Asset Management runs on a single-architecture platform, enabling faster outcomes to slash spending and license compliance risks. Collect and monitor VA Commodity and IO software installed on asset. Used for usage and reporting and compliance.

IT Business Management: Agile. Enable your teams to use agile methods to pull together software development workflows into one system and connect them to other ServiceNow activities. Manage, assign, and track project "development" tasks and requirements following the VA Software Development Life Cycle (SDLC) process.

IT Business Management: Application Portfolio Management. Track, manage, and analyze applications by category, manufacturer, family, and scores. Monitor business applications on an interactive timeline to track versions and lifecycle.

IT Business Management: Demand Management. Centralizes business and IT requests, streamlining the investment process for new products, services, repairs, and enhancements. Centralizes business and IT requests, streamlining the investment process for new products, services, repairs, and enhancements.

IT Business Management: Project and Portfolio. Provides visibility for demand, resources, and project portfolios to improve productivity.

IT Business Management: Test Management. The ServiceNow Test Management 2.0 application streamlines the management of testing processes to help deliver software products more efficiently and with fewer errors. Centralized location for Test Teams to build, store, and execute test cases/steps validating functionality within their system.

IT Operations Management: Discovery. Provides complete visibility for resources on-site (on-prem) and in the cloud. Tracks changes occurring within your on-prem, cloud, and serverless infrastructure in the Configuration Management Database (CMDB). Sets a strong foundation with accurate data and relationship views for ITSM change management, Software Asset Management, Customer Service Management (CSM), Security Operations, and more. Populates the Platform's CMDB with configuration items (CI) found on the VA's network. These CIs are used throughout the platform leverage by many modules.

IT Operations Management: Event Management. Reduce event noise generated by monitoring tools by using predictive intelligence, such as machine learning techniques, to correlate events and produce actionable alerts and incidents. Helps to correlate the root cause of IT issues much faster and reduce Mean Time to Repair (MTTR), when used with Service Mapping and Operational Intelligence. Get a single pane of glass with the Operator Workspace to view service performance at scale, see related alerts, and drilldown to solve issues. Centralized location to view the Alerts for the various VA Monitoring tools on a single Dashboard. Alerts contain information about the CIs that created the event in the source application.

IT Operations Management (ITOM): Service Mapping. Gain visibility into the IT infrastructure that makes up your business services. Accurate service maps use traffic-based discovery and infrastructure information in the ServiceNow Configuration Management Database (CMDB) to show the mix and relationship of applications, IT components, and cloud services. Build out service "maps" which identifies from the top-down all the CIs that make up a service's architecture. Mostly related to IT CIs allowing the other modules to report on uptime/downtime and to see services/systems in degraded state.

Information Technology Service Management (ITSM): Change and Release. With ServiceNow Change and Release Management, you control every aspect of the IT change processes from creation to approval. Minimize change impact with clear information on risk and scheduling conflicts. Accelerate change management using the Change Advisory Board (CAB) Workbench to schedule, plan, and manage CAB meetings from one place. VA users can manage changes to their IT systems following the VA change control process through the user of approvals, workflows, and schedules.

ITSM: Incident. Keep employees productive and happy by ensuring they can easily contact support to track and fix issues with ServiceNow Incident Management. Users can connect with IT through web or mobile self-service and virtual agents powered by natural language understanding (NLU). All VA users have access to submit an incident to the Enterprise Service Desk (ESD) for support. The incidents range from IT to non-IT related issues.

ITSM: Knowledge Management. Expose available knowledge through the Service Portal and allow employees to search, browse, and view articles from their desktop or mobile device. Managed by the VA

Knowledge Management team, the content in the articles provide self- service information to the VA user community for both IT and non-IT topics.

ITSM: Problem Management. ServiceNow Problem Management minimizes the business impact of service disruptions and reduces future disruptions using ITIL-proven practices. Run trend and root cause analyses and service configuration reviews, document solutions and workarounds, and keep stakeholders informed as you remediate issues. Proactively schedule changes from within any problem record and achieve a streamlined incident-problem-change lifecycle across IT. Centralized location to record and track IT related reoccurring problems.

ITSM: Request Management. ServiceNow Request Management delivers employee self- service through a published catalog of services, automated workflows, and service level agreements. Mobile capabilities give employees the freedom to request services anytime, from any device—and get automated status updates to ensure expectations are met. Centralized location for your IT Portal users to request common VA services.

Platform: Configuration Management Database (CMDB). To effectively manage and improve the system, provides visibility of assets in the IT environment and have current, accurate configuration data. With an accurate CMDB, provides service impact analysis, asset management, compliance, and configuration management. Centralized location for IT related (Configuration Items (Cis), business, and technical services.

Platform: Performance Analytics (PA). Create statistics and capture point-in-time data values for historical reporting.

Platform: Virtual Agent. Artificial Intelligence (AI) chatbot that interacts with your IT Portal users to provide content from Knowledge Base (KB) articles or direct user to the Incident or Request item related to the user's inquiry.

Platform: Users. Syncs VA user information from VA Active Directory. Allows the Platform to authenticate and communicate with the user as well as provide automated routing based off the user's location (e.g., Incident tickets).

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

While AHA is the primary means to recover data and restore service in the case of a disruption, in certain cases it is desirable to use ServiceNow's more traditional data backup and recovery mechanism. It works in concert with AHA and acts as a secondary recovery mechanism. Backups of the two production databases and the single sub-production database are taken every day for all instances. The backup cycle consists of four weekly full backups and the past six days of daily differential backups that provide 28 days of backups. All backups are written to disk, no tapes are used, and no backups are sent off site. All the controls that apply to live customer data also apply to backups. If data is encrypted in the live database, then it will also be encrypted in the backups. Regular, automated tests are run to ensure the quality of backups. Any failures are reported for remediation within ServiceNow.

3. Legal Authority and SORN

H. A 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 - Loan Guarantee Fee Personnel and Program – VA
- System of Record Notice (SORN) –
  27VA047 - Personnel & Acct Integrated Data system
- System of Record Notice (SORN) –
  55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- System of Record Notice (SORN) –
  168VA005 - Health Information Exchange –
- 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, *and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program*
- VA Directive and Handbook 6502, *Privacy Program*
- VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.
- VA Directive and Handbook 6513, *Secure External Connections*
- VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2
- Title 38 U.S.C § 5701: Confidential Nature of Claims

BELOW- See VA Handbook 6500.6, Appendix C and D.

ServiceNow is a major application and contains the following functionalities:
Enterprise Asset Management: Nuvolo. Nuvolo's suite of applications help organizations solve business problems with various capabilities for aligned to Operation Technology Management for Healthcare, Labs, Manufacturing and Facilities. Collect and monitor VA Medical Facility assets.

IT Asset Management: Asset Management. Asset Management automates your IT asset lifecycles with intuitive workflows. Make informed decisions about asset capacity, refresh, and vendors. Collect and monitor VA Commodity and Infrastructure Operation (IO) Assets.

IT Asset Management: Software Asset Management. Software Asset Management runs on a single-architecture platform, enabling faster outcomes to slash spending and license compliance risks. Collect and monitor VA Commodity and IO software installed on asset. Used for usage and reporting and compliance.

IT Business Management: Agile. Enable your teams to use agile methods to pull together software development workflows into one system and connect them to other ServiceNow activities. Manage, assign, and track project "development" tasks and requirements following the VA Software Development Life Cycle (SDLC) process.

IT Business Management: Application Portfolio Management. Track, manage, and analyze applications by category, manufacturer, family, and scores. Monitor business applications on an interactive timeline to track versions and lifecycle.

IT Business Management: Demand Management. Centralizes business and IT requests, streamlining the investment process for new products, services, repairs, and enhancements. Centralizes business and IT requests, streamlining the investment process for new products, services, repairs, and enhancements.

IT Business Management: Project and Portfolio. Provides visibility for demand, resources, and project portfolios to improve productivity.

IT Business Management: Test Management. The ServiceNow Test Management 2.0 application streamlines the management of testing processes to help deliver software products more efficiently and with fewer errors. Centralized location for Test Teams to build, store, and execute test cases/steps validating functionality within their system.

IT Operations Management: Discovery. Provides complete visibility for resources on-site (on-prem) and in the cloud. Tracks changes occurring within your on-prem, cloud, and serverless infrastructure in the Configuration Management Database (CMDB). Sets a strong foundation with accurate data and relationship views for ITSM change management, Software Asset Management, Customer Service Management (CSM), Security Operations, and more. Populates the Platform's CMDB with configuration items (CI) found on the VA's network. These CIs are used throughout the platform leverage by many modules.

IT Operations Management: Event Management. Reduce event noise generated by monitoring tools by using predictive intelligence, such as machine learning techniques, to correlate events and produce actionable alerts and incidents. Helps to correlate the root cause of IT issues much faster and reduce Mean Time to Repair (MTTR), when used with Service Mapping and Operational Intelligence. Get a single pane of glass with the Operator Workspace to view service performance at scale, see related alerts, and drilldown to solve issues. Centralized location to view the Alerts for the various VA Monitoring tools on a single Dashboard. Alerts contain information about the CIs that created the event in the source application.

IT Operations Management (ITOM): Service Mapping. Gain visibility into the IT infrastructure that makes up your business services. Accurate service maps use traffic-based discovery and infrastructure information in the ServiceNow Configuration Management

Database (CMDB) to show the mix and relationship of applications, IT components, and cloud services. Build out service "maps" which identifies from the top-down all the CIs that make up a service's architecture. Mostly related to IT CIs allowing the other modules to report on uptime/downtime and to see services/systems in degraded state.

Information Technology Service Management (ITSM): Change and Release. With ServiceNow Change and Release Management, you control every aspect of the IT change processes from creation to approval. Minimize change impact with clear information on risk and scheduling conflicts. Accelerate change management using the Change Advisory Board (CAB) Workbench to schedule, plan, and manage CAB meetings from one place. VA users can manage changes to their IT systems following the VA change control process through the user of approvals, workflows, and schedules.

ITSM: Incident. Keep employees productive and happy by ensuring they can easily contact support to track and fix issues with ServiceNow Incident Management. Users can connect with IT through web or mobile self-service and virtual agents powered by natural language understanding (NLU). All VA users have access to submit an incident to the Enterprise Service Desk (ESD) for support. The incidents range from IT to non-IT related issues.

ITSM: Knowledge Management. Expose available knowledge through the Service Portal and allow employees to search, browse, and view articles from their desktop or mobile device. Managed by the VA Knowledge Management team, the content in the articles provide self-service information to the VA user community for both IT and non-IT topics.

ITSM: Problem Management. ServiceNow Problem Management minimizes the business impact of service disruptions and reduces future disruptions using ITIL-proven practices. Run trend and root cause analyses and service configuration reviews, document solutions and workarounds, and keep stakeholders informed as you remediate issues. Proactively schedule changes from within any problem record and achieve a streamlined incident-problem-change lifecycle across IT. Centralized location to record and track IT related reoccurring problems.

ITSM: Request Management. ServiceNow Request Management delivers employee self-service through a published catalog of services, automated workflows, and service level agreements. Mobile capabilities give employees the freedom to request services anytime, from any device—and get automated status updates to ensure expectations are met. Centralized location for your IT Portal users to request common VA services.

Platform: Configuration Management Database (CMDB). To effectively manage and improve the system, provides visibility of assets in the IT environment and have current, accurate configuration data. With an accurate CMDB, provides service impact analysis, asset management, compliance, and configuration management. Centralized location for IT related (Configuration Items (Cis), business, and technical services.

Platform: Performance Analytics (PA). Create statistics and capture point-in-time data values for historical reporting.

Platform: Virtual Agent. Artificial Intelligence (AI) chatbot that interacts with your IT Portal users to provide content from Knowledge Base (KB) articles or direct user to the Incident or Request item related to the user's inquiry.

Platform: Users. Syncs VA user information from VA Active Directory. Allows the Platform to authenticate and communicate with the user as well as provide automated routing based off the user's location (e.g., Incident tickets).

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, GCC-E, VA ServiceNow does not have a System of Record of Notice (SORN). GCC-E VA ServiceNow is not a System of Record (SOR) nor does it generate records, only an incident ticket to track various listed requests. ServiceNow does utilize sources from VA information to validate, sort, approve and complete official VA business. The Memorandum of Understanding/Interconnection Security Agreement (MOU/ISA) was updated April 2022, and the Privacy Threshold Assessment (PTA) was updated December 30, 2022, to cite the Cerner Corporation – Remedy ticketing system, external interface. The PHI/PII information shared with Cerner is to provision a clinical account for Cerner Millennium. The PHI and PII is not patient/clinical data but is used to provision an Electronic Health Record Management (EHRM) account for clinical practitioners to access clinical systems.

D. System Changes

J. Whether 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. Whether 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.

The Cloud Service Provider (CSP) contract details the accountability, security, and privacy of VA data. A prohibition on unauthorized disclosure: "Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA." This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data – General, Federal Acquisition Regulation (FAR) § 52.227-14(d).(1).

A requirement for data breach notification: Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access, the Contractor/Subcontractor shall immediately notify the Contract Officer Representative (COR), including the designated ISO, and Privacy Officer (all three) for the contract. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. See VA Handbook 6500.6, Appendix C, paragraph 6.a.

A requirement to pay liquidated damages in the event of a data breach: "In the event of a data breach or privacy incident involving Sensitive Personal Information (SPI) the contractor processes or maintains under this contract shall be liable to VA for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals." However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports
3) Data breach analysis
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

A requirement for annual security/privacy awareness training: "Before being granted access to VA information or information systems, all Contractor employees and Subcontractor employees requiring such access shall complete on an annual basis either: (i) the VA security/privacy awareness training (contains VA security/privacy requirements) within 1 week of the initiation of the contract, or (ii) security awareness training provided or arranged by the contractor that conforms to VA's security/privacy requirements as delineated in the hard copy of the VA security awareness training provided to the Contractor. If the Contractor provides their own training that conforms to VA's requirements, they will provide the COR or CO, a yearly report (due annually on the date of the contract initiation) stating that all applicable employees involved in VA's contract have received their annual security/privacy training that meets VA's requirements and the total number of employees trained. See VA Handbook 6500.6, Appendix C, paragraph 9.

A requirement to sign VA's Rules of Behavior: "Before being granted access to VA information or information systems, all Contractor employees and Subcontractor employees requiring such access shall sign on annual basis an acknowledgement that they have read, understand, and agree to abide by VA's Contractor Rules of Behavior which is attached to this contract." See VA Handbook 6500.6, Appendix C, paragraph 9, and Appendix D. Note: If a medical device vendor anticipates that the services under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the vendor's designated representative. The contract must reflect by signing the Rules of Behavior on behalf of the vendor that the designated representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing VA's information and information systems.

The disclosure or breach of ServiceNow data could cause irreparable harm to the CSP and the individuals based on the data in the system identified below.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ 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)

DEA Identification number: Unique identifier used by medical providers to administer regulated prescriptions
Electronic Data Interchange Personal Identifier (EDIPI): Used to validate active Department of Defense Common Access Card (CAC) holders accessing VA IT systems
Manager: Used to identify the user and the manager/supervisor for communication and the approval of workflow processes and business actions
National Provider Identifier (NPI): Unique 10-digit identification number adopted under HIPAA, used by healthcare providers for administrative and financial transactions such as claims and billing
Personal Identity Verification (PIV) Identification (ID): Used to validate the identity of VA system users to ensure an accurate match with the Id.Me account with the ServiceNow account; this field is not masked – Verify how this is being used within SNOW
Security Identifier (SecID): VA Employee Identification number
Social Security Number (SSN): Used as a unique identifier for Veterans Benefits Administration case record and retained for tracking benefit records
Taxonomy code: A unique 10-character (beginning and end date) Medicare administrative code for identifying the provider type and specialization for all Medicare claims and submissions
Username: Used to identify VA employees retained for providing reference for business uses (authorizations, resolving incidents, tracking benefits)
Work location: For equipment tracking and department assignment

PII Mapping of Components (Servers/Database)

ServiceNow consists of 20 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by ServiceNow 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	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
Active Directory Federation Services (ADFS)	Yes	Yes	SecID (Employee ID Number), Phone Number, Location, and Email	User account validation for proper system access	Security Controls in place, FedRAMP certified

Database Name of the information system collecting/storing PII	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
Active Directory Account Management (ADAM)	Yes	Yes	SecID (Employee ID Number), Phone Number, Location, and Email	Integration with Active Directory to update user records for PIV exemptions and Account Management.	Security Controls in place, FedRAMP certified
Asset Management	Yes	Yes	IP Addresses	Identification of Information Technology hardware/software assets	Security Controls in place, FedRAMP certified
Azure (Chatbot)	Yes	Yes	Full Name, Manager, Workstation ID, Work Phone Number, Work Location, and Work Email	Associated identification data to ensure accuracy of incident tracking and submittal	Security Controls in place, FedRAMP certified
BMC Remedy – Cerner Corporation; GCC-E – ServiceNow High - E	Yes	Yes	Last Name First Name MI EDIPI DEA number DEA Expiration NPI Taxonomy	This information provisions the Utilization Review Accreditation Commission (URAC) account for access to Cerner Millennium EHRM system	Security Controls in place, FedRAMP certified
Customer Service Management (VA- LGY)	Yes	Yes	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Associated identification data to ensure accuracy of incident tracking	Security Controls in place, FedRAMP certified
Data Access Services (DAS)	Yes	Yes	SSN, DOB, full-service treatment records from DoD, Disability exam records, community administered immunization information	Business process tool for exchanging sensitive Veteran data within VA organizations	Security Controls in place, FedRAMP certified

Database Name of the information system collecting/storing PII	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
Electronic Permissions Access Request (EPAS)	Yes	Yes	Full name, DOB, SSN, SecID (Employee ID Number), Workstation ID, Work Manager and Work Email	Associated identification data to ensure accuracy of incident tracking	Security Controls in place, FedRAMP certified
Facilities API	Yes	Yes	Name, Work Location, Work Email, Work Phone Number, IP Addresses	Associated identification data to ensure accuracy of incident tracking and submittal	Security Controls in place, FedRAMP certified
Health Data and Analytics Platform (HDAP)	Yes	Yes	Name, Social Security Number, Email (VA & personal), Biometrics, Financial Information, Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Physical Address, Phone Number, Date of Birth, Race/ethnicity, Vital Status, Gender, City of residence, County of residence, Zip code, Hospitalization dates, Date of diagnosis, Date of death, Private insurance status, Laboratory results, Medications and therapies, Outpatient/inpatient clinic visits, Physician name, Electronic Data Interchange	Associated identification data to ensure accuracy of incident tracking for Official VA business purposes	Internal connection

			Personal Identifier (EDIPI), Usernames, Vendor Taxpayer ID Number (TIN), Integration Control Number (ICN), Patient Generated Data (PGD) from Fitbit device, Next-of-kin information, COVID case information, Patient ID and VA Identifier		
Database Name of the information system collecting/storing PII	**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**
Human Capital Information Services (HCIS) - Human Resources Payroll Application Services (HR-PAS) - GS pay scale	Yes	Yes	Employee ID Employee Record Number Name Expansion, First Name Expansion, Last Email Address	HR-PAS serves as the central repository for combined HR, payroll data to perform business functions in support of VA Financial and Human Resource systems to interface data elements	Internal connection
Human Capital System & Services (HCSS) / Human Capital Management (HCM)	Yes	Yes	Username, Work Email Address, Domain and Work Phone Number	Serves as the central repository for combined HR, payroll data to perform business functions in support of VA Financial and Human Resource systems to interface data elements	Internal connection

Database Name of the information system collecting/storing PII	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
Identity and Access Management (IAM) Integration for Identity Proofing – for LGY	Yes	Yes	Name, SSN, DOB, Work Email, Phone Number, Addresses, Manager, IP Addresses	Associated identification data to ensure accuracy of incident tracking associated with Loan Guarantee program specifically for Veterans	
Incident Management	Yes	Yes	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Associated identification data to ensure accuracy of incident tracking	Security Controls in place, FedRAMP certified
Lightweight Directory Access Protocol (LDAP)	Yes	Yes	SecID (Employee ID Number), Work Phone Number, Work Location, and Work Email Address	User account validation for proper system access	Security Controls in place, FedRAMP certified
Nuvolo	Yes	Yes	N/A - IP Addresses	Identification of IT hardware/software assets	Security Controls in place, FedRAMP certified
The Office of Business Process Integration (OBPI) and Office of Financial Management (OFM) provide Data Quality and Fraud Prevention (DQFP) support	Yes	Yes	SSN, Files Number, Name and DOB	Associated identification data to ensure accuracy of incident tracking for Official VA business purposes	Internal connection
Problem Management	Yes	Yes	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Associated identification data of related incidents to ensure accuracy of incident tracking	Security Controls in place, FedRAMP certified

Database Name of the information system collecting/storing PII	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
Remote Access Portal (RAP) Database integration with ADAM	Yes	Yes	User's AD Domain, User's AD NT UserID, User's AD User Principal Name (UPN), User's AD Email address	Associated identification data of related incidents to ensure accuracy of incident tracking	Internal connection
Request Management	Yes	Yes	Name, SSN, DOB, Email, Phone numbers, Addresses, Manager, IP Addresses	Associated identification data to ensure accuracy of incident tracking	Security Controls in place, FedRAMP certified
Salesforce Functional Organizational Manual (SF-FOM)	Yes	Yes	VA organizational information to associate users with the organizational hierarchy.	Salesforce FOM provides accurate VA organizational information to associate users with the organizational hierarchy.	Security Controls in place, FedRAMP certified
ServiceNow (Software as a Service, SaaS)	Yes	Yes	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Validation of users, processing of benefits, and identification of Information Technology hardware/software assets	Security Controls in place, FedRAMP certified
Technology Business Management (TBM)	Yes	Yes	N/A - Username, Device Identification, Device Location	Allows TBM team to pull data from ServiceNow (Incidents, requests, CIs) for cost reporting.	Security Controls in place, FedRAMP certified
Users	Yes	Yes	Name, SSN, DOB, Work Email, Work Phone Numbers, Work Address, Manager, Work IP Addresses	Associated identification data to ensure accuracy of incident tracking	Security Controls in place, FedRAMP certified

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?

Information is collected from automated VA systems or manual entry methods from the person entering the information for the ticket request. VA Identity and Access Management (IAM) and Active Directory (AD) are sources of information already validated for general use and account provisioning. In this instance, automated secure processes are used for efficiency and to minimize the handling of sensitive private data when entered by hand.

ServiceNow can complete some specific fields within the ticket to assist and fulfill the request.

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.

All 20 modules of ServiceNow receive information entered into the ticket request by authenticated Department of VA users, verified network sources and from within the GCC-Enterprise in a FedRAMP authorized, secured and cleared facility. Ticket information never comes from any public website outside of the VA network boundary.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VA ServiceNow does not create information such as a score, analysis or report but does draw from other official VA systems to cross-reference, validate and correlate data fields for processing the ticket in a timely manner.

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?

For an incident ticket or any request created within ServiceNow, most are entered by hand. This method is used to accurately populate only the data needed for a request or an account provision to synchronize with organizational data. VA Identity and Access Management (IAM) and Active Directory (AD) are sources of information already validated for general use and account provisioning. In this instance, automated secure processes are used for efficiency and to minimize the handling of sensitive private data when entered by hand.

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

ServiceNow data collection forms are 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.

The purpose of the information collected, used, and created by ServiceNow 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 with additional workflow capabilities such as incident management, problem management, demand management, change management and asset management. The SPI collected and used within ServiceNow 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 If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The purpose of the information collected, used, and created by ServiceNow 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 with additional workflow capabilities such as incident management, problem management, demand management, change management and asset management. The SPI collected and used within ServiceNow 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).

1.5 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 user records are compared with incoming data from AD to validate the user's record within ServiceNow. In the case of duplicate records, Active Directory is the authoritative source for user SPI, PII and PHI data.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

Principle of Purpose Specification: 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: Sensitive Personal Information (SPI), including personal contact information, SSN/TIN, may be released to unauthorized individuals.

Mitigation: Profile based permissions will govern what access users have to the system. Profiles, including groups and roles within ServiceNow, 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.

Privacy Risk: Unsecured Sensitive Personal Information (SPI), including personal contact information, SSN/TIN, may be exposed.

Mitigation: To mitigate this risk, ServiceNow protects data by ensuring that only authorized users have access. Data security rules are assigned that determine which data

users can access. All data is encrypted in transfer. Access to ServiceNow is governed by HSPD-12, FIPS-201, and NIST SP-800 series standards for Personal Identity Verification (PIV) cards issued by the VA.

Privacy Risk: Data breach at the facilities level.

Mitigation: 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 no not physically leave the data center.

Privacy Risk: Data breach at the network level.

Mitigation: 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 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.

ServiceNow 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.

- **DEA Identification number**: Unique identifier used by medical providers to administer regulated prescriptions
- **Electronic Data Interchange Personal Identifier (EDIPI)**: Used to validate active Department of Defense Common Access Card (CAC) holders accessing VA IT systems
- **Manager**: Used to identify the user and the manager/supervisor for communication and the approval of workflow processes and business actions
- **National Provider Identifier (NPI)**: Unique 10-digit identification number adopted

under HIPAA, used by healthcare providers for administrative and financial transactions such as claims and billing

- **Personal Identity Verification (PIV) Identification (ID)**: Used to validate the identity of VA system users to ensure an accurate match with the Id.Me account with the ServiceNow account; this field is not masked – Verify how this is being used within SNOW
- **Security Identifier (SecID)**: VA Employee Identification number
- **Social Security Number (SSN)**: Used as a unique identifier for Veterans Benefits Administration case records and retained for tracking benefit records
- **Taxonomy code**: A unique 10-character (beginning and end date) Medicare administrative code for identifying the provider type and specialization for all Medicare claims and submissions
- **Username**: Used to identify VA employees retained for providing reference for business uses (authorizations, resolving incidents, tracking benefits)
- **Work location**: For equipment tracking and department assignment

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 receives, creates and stores data. ServiceNow performance analytics enables users to perform data analysis.

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 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?

The Confidentiality, Integrity and Assessment (CIA) rating for VA ServiceNow – Enterprise is rated a high which includes additional precautions used for the system to be properly secured offsite. The facilities where ServiceNow operates is Federal Risk and Authorization Management Program (FedRAMP) certified building that operates in the Government Cloud Computing (GCC), also rated a high for proper system security and support. FedRAMP is a government-wide program that standardizes security assessment, authorization and continuous monitoring for cloud products and services. The Uniform Resource Locator (URL) is encrypted via https. The facility personnel follow similar government processes and procedures with cleared personnel performing work and support for this system.

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 – Enterprise is rated a high which includes additional precautions used for the system to be properly secured offsite. The facilities where ServiceNow operates is Federal Risk and Authorization Management Program (FedRAMP) certified building that operates in the Government Cloud Computing (GCC), also rated a high for proper system security and support. FedRAMP is a government-wide program that standardizes security assessment, authorization and continuous monitoring for cloud products and services. The Uniform Resource Locator (URL) is encrypted via https. The facility personnel follow similar government processes and procedures with cleared personnel performing work and support for this system.

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?

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; and this is enforced by ServiceNow 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. The use of groups and roles within ServiceNow 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. The use of groups and roles within ServiceNow 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 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
- DEA Identification number
- Electronic Data Interchange Personal Identifier (EDIPI)
- Employee Number
- Gender
- Internet Protocol (IP) Address Numbers
- Manager
- Name (full)
- National Provider Identifier (NPI)
- Personal Identity Verification (PIV) Identification (ID)
- Personal Phone Number
- Personal Email Address
- Security Identifier (SecID)
- Social Security Number (SSN)
- Tax Identification Number
- Taxonomy code
- Username
- Work location

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 has been classified to contain three types of information: Help Desk Services, Lifecycle/Change Management, and 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

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 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 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, "Guidelines for Media Sanitization" (January 2019), (https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=1003&FType=2). Additional procedures for SPI/data elimination are provided by the vendor, ServiceNow.

The Customer can initiate a request in HIWAVE (Federal Government Customer Support Site) to have data deleted from their environment. This request may come through via Customer Support, Sales, Account Manager or Sales Ops; however, an external facing incident ticket assigned to Customer Support must be opened to track the request. This request serves as the basis for identification of target data for deletion and must identify all the instances subject to data sanitization. Customer Support will open an internal facing Change ticket and assign it (Cloud) Sustained Operations. ServiceNow Operations initiates Customer Instance Migration necessitated by hardware lifecycle expiration, storage failure scenario, or logical or physical customer instance location change.

Cloud Operations reviews the request and identifies the possible sources of data per "Secure Data Deletion" Knowledge Article (KB0565364). Once determined, the information is entered in the Change ticket. This ensures that all relevant information is included in the Deletion phase of the process. Information entered in the ticket supports the Verification phase of the process.

Cloud Operations uses Secure Data Deletion Knowledge Article (KB0565364) to complete data destruction from the system at the sources identified. Due to technology

limitations and the shared nature of hardware deployment, the type of data deletion is -

i) Database Instances – Logical deletion
    (a) All Primaries (Prod, Sub-prod)
        (b) All Standby / HA (Prod, Sub-prod)
        (c) Read Replicas
        (d) DMZ Reporting servers
    ii) Database instance backups - Logical deletion
    iii) Application nodes – Block deletion
    iv) Splunk – Logical deletion
    v) Incoming mailbox – Logical deletion
    vi) Customer metadata
        (a) SNAC customer data snapshots – Logical deletion
        (b) Node triage logs – Block deletion

Note: In situations where hardware will remain in use and data is logically deleted but not physically, there is no confirmed risk since spinning hard drives and Fusion IO cards will be destroyed securely at the end of their life cycle when the servers are retired.

Verification of Instance Deletion
A CTASK is created and assigned to Security Engineering

a) Security Engineering verifies per their process and updates the ticket noting deletion occurred according "Secure Data Deletion" Knowledge Article (KB0565364).
b) Security Engineer completes the SNC Certificate of Instance Data Destruction template (KB0597435), recording all data pertinent to the process in the Change ticket, and collects the appropriate signatures.
c) Security Engineer attaches the Certificate of Instance Data Destruction to the Change ticket and closes it.
d) Customer Support provides the Certificate of Instance Data Destruction to customer via the original external facing incident ticket.
e) Customer closes the Incident ticket upon confirmation of receipt of Certificate of Instance Data Destruction.

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 has testing, development, sandbox, and training environments that are clones 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. 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). https://yourit-dev.va.gov. This environment is primarily used by developers, approximately 50 users.

Test Environment: 517,000 records; access: single sign-on (SSO). https://vaoittest.servicenowservices.com. This environment is primarily used by testers, approximately 25 users.

PreProd Environment: 517,000 records; access: single sign-on (SSO). https://vaoitpreprod.servicenowservices.com. This environment is primarily used by testers and product owners, approximately 100 users.

Training Environment: 517,000 records; access: single sign-on (SSO). https://vaoittrain.servicenowservices.com. This environment is primarily used by the Enterprise Service Desk (ESD)for training new hires, approximately 100 users.

Sandbox1 Environment: 517,000 records; access: manual (username/password). https://servicenowvasandbox.servicenowservices.com. This environment is primarily used by developers, approximately 50 users.

Sandbox2 Environment: 517,000 records; access: manual (username/password). https://snvasandbox.servicenowservices.com. This environment is primarily used by developers, approximately 50 users.

Sandbox3 Environment: 517,000 records; access: manual (username/password). https://snsandboxitx.service-now.com. This environment is primarily used by developers, approximately 50 users.

Production Environment: 517,000 records; access: single sign-on (SSO). https://yourit.va.gov. This is the Production Environment. Approximately 127,000 users logged in past 30 days.

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 is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, ServiceNow adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the ServiceNow 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 6500.1, Electronic Media Sanitization.

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***
Active Directory Federation Services (ADFS)	IAM, ADFS, Provisioning service self-service options for internal VA users for centralized creation, modification, deletion and suspension for user accounts based on business processes and interactions defined by application or systems	SecID (Employee ID Number), Personal Identity Verification Identification (PIV ID) Work Phone Number, Work Location, and Work Email	Active Directory
Active Directory Account Management (ADAM)	Is a Lightweight Directory Access Protocol (LDAP) compliant DS used for building directory-enabled applications	SecID (Employee ID Number), Work Phone Number, Work Location, and Work Email	Active Directory
Asset Management	Identification of Information Technology hardware/software asset	IP Addresses	Security Controls in place, FedRAMP certified
Azure (Chatbot)	Associated identification data to ensure accuracy of incident tracking and submittal	Full Name, Manager, Workstation ID, Work Phone Number, Work Location, and Work Email	Security Controls in place, FedRAMP certified
BMC Remedy – Cerner Corporation	This information provisions the Utilization Review Accreditation Commission (URAC) account for access to Cerner Millennium EHRM system	Last Name First Name, MI EDIPI DEA number DEA Expiration NPI Taxonomy	Bi-directional Business Partner Extranet IPSec encrypted tunnel through the VA Trusted Internet Connection (TIC) 2.0 connection
Customer Service Management (VA -LGY)	Associated identification data to ensure accuracy of incident tracking	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Security Controls in place, FedRAMP certified

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***
Data Access Services (DAS)	Business process tool for exchanging sensitive Veteran data within VA organizations	SSN, DOB, Full-service treatment records from DoD, Disability exam records, community administered immunization information	Security Controls in place, FedRAMP certified
Electronic Permissions Access Request (EPAS)	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Full name, DOB, SSN, SecID (Employee ID Number), Workstation ID, Work Manager and Work Email	Internal connection
Facilities API	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Name, Work Location, Work Email, Work Phone Number, IP Addresses	Security Controls in place, FedRAMP certified
Health Data and Analytics Platform (HDAP)	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Name, Social Security Number, Email (VA & personal), Biometrics, Financial Information, Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Physical Address, Phone Number, Date of Birth, Race/ethnicity, Vital Status, Gender, City of residence, County of residence, Zip code, Hospitalization dates, Date of diagnosis, Date of death, Private insurance status, Laboratory results, Medications and therapies, Outpatient/inpatient clinic visits, Physician name, Electronic Data Interchange Personal Identifier (EDIPI), Usernames, Vendor Taxpayer ID Number (TIN), Integration Control Number (ICN), Patient Generated Data (PGD) from Fitbit	Internal connection

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*
		device, Next-of-kin information, COVID case information, Patient ID and VA Identifier	
Human Capital Information Services (HCIS) - Human Resources Payroll Application Services (HR-PAS) - GS pay scale	HR-PAS serves as the central repository for combined HR, payroll data to performs business functions in support of VA Financial and Human Resource systems to interface data elements	Employee ID Employee Record Number Name Expansion, First Name Expansion, Last Email Address	Security Controls in place, FedRAMP certified
Human Capital System & Services (HCSS) / Human Capital Management (HCM)	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Username, Work Email Address, Domain and Work Phone Number	Internal connection
Identity and Access Management (IAM) Integration for Identity Proofing – for LGY	Associated identification data to ensure accuracy of incident tracking associated with Loan Guarantee program specifically for Veterans	Name, SSN, DOB, Work Email, Phone Number, Addresses, Manager, IP Addresses	Security Controls in place, FedRAMP certified
Identity and Access Management (IAM) Integration with New Hire Equipment	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Name, SecID, Work Email Address, Work Phone Number	Security Controls in place, FedRAMP certified
Incident Management	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Security Controls in place, FedRAMP certified
Lightweight Directory Access Protocol (LDAP)	Is a Lightweight Directory Access Protocol (LDAP) compliant DS used for building directory-enabled applications	SecID (Employee ID Number), Work Phone Number, Work Location, and Work Email Address	Active Directory

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*
Nuvolo	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	IP Addresses, Identification of IT hardware/software assets	Security Controls in place, FedRAMP certified
The Office of Business Process Integration (OBPI) and Office of Financial Management (OFM) provide Data Quality and Fraud Prevention (DQFP) support	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	SSN, Files Number, Name and DOB	Internal connection
Problem Management	Associated identification data of related incidents for root cause analysis to ensure accuracy of incident tracking	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Security Controls in place, FedRAMP certified
Remote Access Portal (RAP) Database integration with ADAM	Using 2FA exemption detail and ServiceNow RITM number, ADAM sends RAP information for associated identification data to ensure accuracy of incident tracking	User's AD Domain, User's AD NT UserID, User's AD User Principal Name (UPN), User's AD Email address	Active Directory
Request Management	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Security Controls in place, FedRAMP certified
Salesforce Functional Organizational Manual (SF-FOM)	Salesforce FOM provides accurate VA organizational information to associate users with the organizational hierarchy	Employee status, Employee payroll earnings for the tax year, annual and sick leave balances, retirement and supplemental data or physicians and dentists	Security Controls in place, FedRAMP certified
ServiceNow (Software as a Service, SaaS)	Validation of users, processing of benefits, and identification of	Name, SSN, DOB, Email, Phone Numbers, Addresses, Manager, IP Addresses	Security Controls in place, FedRAMP certified

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
	Information Technology hardware/software assets		
Technology Business Management (TBM)	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Username, Device Identification, Device Location	Internal connection
Users	Associated identification data to match user data with Active Directory	Name, SSN, DOB, Work Email, Work Phone Numbers, Work Address, Manager, Work IP Addresses	Security Controls in place, FedRAMP certified

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; and this is enforced by ServiceNow best practices of assigning users to groups and roles based on job functions.

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. GCC-E VA ServiceNow is not a System of Record (SOR) nor does it generate records, only an incident ticket to track various listed requests. ServiceNow does utilize sources from VA information to validate, sort, approve and complete official VA business. The Memorandum of Understanding/Interconnection Security Agreement (MOU/ISA) was updated April 2022, and the Privacy Threshold Assessment (PTA) was updated December 30, 2022, to cite the Cerner Corporation – Remedy ticketing system, external interface. The PHI/PII information shared with Cerner is to provision a clinical account for Cerner Millennium. The PHI and PII is not patient/clinical data but is used to provision an Electronic Health Record Management (EHRM) account for clinical practitioners to access clinical systems.

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***
Cerner	Provision EHRM accounts which are encrypted inside of the	*- indicates items are PII, 6 total *Last Name *First Name *MI *EDIPI	Cerner MOU/ISA, updated April 2022	Rest API, https and a bidirectional dedicated VPN

	ServiceNow ticket	*DEA DEA Expiration *NPI Gender VA Email Business Address City State ZIP Code Business Phone Business Fax Facility TL Unit Location Telework Supervisor/POC Supervisor Email Department Sub-Department Job Title Credentials HPT Station Number EHRM Primary Role EHRM Secondary Role Clairvia Role EHRM Primary Specialty EHRM Secondary Specialty User Role Assigned Validated By Supervisor TMS ID Training Updates Training POC Training Facility SU Training Facility Environment Super User *Taxonomy *Taxonomy Code Begin Date *Taxonomy Code End Date *Medicare Specialty End User Updates Primary TMS Program Primary TMS Program Completed Additional TMS Programs Additional TMS Programs Completed Outreach Programs		connection to Cerner

		Provisioning Activity HeInt Provisioning Activity HeInt Solution Whitelist HeInt Personnel Group HeInt Attribution Group HeInt Scoring Group HeInt Org Member HeInt Org Admin Analytics Project Consumers HeCare Personnel Group EHRM Tertiary Role EHRM Quaternary Role Provisioning Complete *PIV User ID (FedUID) Pharmacy User Group DEA Drug Schedule Restrict/Legal Provider Groups Provider Specialty Bridge Role Cerner Direct HIE Reporting Cerner Sentinel iAccess CareAware Solutions (iCommand) 3M 360 EPI&724 (Olympus) Bedrock EPCS VitalsLink Dragon Comments Mobile Access SU Functions Contractor Compliance Asset Id ID Content Type Label setting Retention label Retention label Applied Label applied by Item Child Count Folder Child Count DoD Role Works with DoD HealtheIntent Comments Training Site Supporting Sites Remote Source Group CSS User Role		

		Parent Shifts Classification Provider Type Person Class-VA Code Area of Specialization Telework Definition Signature Block Name Signature Block TitleYes, VA-owned sensitive information/data is transmitted via this interconnection		
Cerner	Sharing of VA ServiceNow incident (record/ ticket) information	VA information/data - Name, SSN, DOB, Work email, Phone Numbers, work Addresses, Manager, Work IP Addresses is transmitted via this fully encrypted connection	Cerner MOU/ISA, updated April 2022	Rest API, https and a bidirectional dedicated VPN connection to Cerner

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: The VA has a critical need for a secure connection for bi-directional data exchange between the VA's ServiceNow and the Cerner Remedy Help Desk Tool in support of incident and change management tracking related to the Electronic Health Record Modernization (EHRM) effort.

Mitigation: The signed Memorandum of Understanding and Interconnection Security Agreement (MOU/ISA), dated April 04, 2022, outlines the technical and administrative controls enforced by the VA and Cerner to ensure the security of data exchange. This is a dedicated connection from the VA to Cerner Corporation via a fully encrypted VPN tunnel.

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.

No, a Notice of Privacy Practice (NOPP) is not provided to users of ServiceNow.

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

Access to ServiceNow is contingent on implied consent within the VA National Rules of Behavior (VA Handbook 6500, Appendix A), and authorized access to VA information systems. https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

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.

Access to ServiceNow is contingent on implied consent within the VA National Rules of Behavior (VA Handbook 6500, Appendix A), and authorized access to VA information systems. https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

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, end-users always can decline to provide information without penalty. Use of the system does not require the use of PII by end-users.

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.

No. Use of the system does not require the use of PII by end-users.

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 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 Transparency: Has sufficient notice been provided to the individual?

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

Follow the format below:

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

Mitigation: The VA mitigates this risk by providing users with notice that the system exists, including the Privacy Act statement.

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 and Handbooks 6300.3, Procedures for Implementing the FOIA (https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=22&FType=2), 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.

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).

ServiceNow is not exempt from the provisions of the Privacy Act.

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.

N/A. Access to data within ServiceNow is based on group assignments and access control list restrictions.

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.

Users are able to correct inaccurate or erroneous information by submitting corrections to their Active Directory information via the Microsoft Identity Manager (MIM) tool: https://mim.va.gov/identitymanagement/default.aspx.

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.

ServiceNow is not a System of Record (SOR) or an authoritative data source.

ServiceNow user records may contain information that is not current. In this case, user will "Report an Issue" through https://yourit.va.gov/ or by contacting the Enterprise Service Desk by telephone at (855) 673-4357. The service agent will direct the Affected End User (AEU) to the authoritative System of Record to correct their information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***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.

If the individual discovers that incorrect information was provided, they simply follow the same contact procedures and process in 7.3, and state that the documentation they are now providing supersedes that previously provided.

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 a supervisor or other approving authority is inaccurate and decisions or other actions are made with incorrect information; and users could be unaware of access, redress, and correction procedures.

Mitigation: Workflow gateway checks within ServiceNow will alert appropriate users and log all actions within a workflow. These activity logs are monitored and audited regularly. Primary line of defense is ensuring users are aware of their data, and this is reinforced annually in the VA Privacy and Security Training and Rules of Behavior.

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 is an enterprise-wide accessible Software as a Service (SaaS). The back-end data is only accessible to ServiceNow contract administrators and VA authorized support personnel. Use of groups and roles limit 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. This process is documented in KB0061639, "ServiceNow: Request a new ServiceNow Assignment Group, Edit an Existing Group, or Decommission a Group."

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?

Information System owner.

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.

All users within the VA's Active Directory (AD) are provisioned a ServiceNow standard user account (SUA) with general access to ServiceNow when VA training is complete and a Personal Identity Verification (VA PIV) card has been issued. In most cases, AD accounts are synchronized nightly to ServiceNow and the SUA account is created. If an account with higher access is needed, a request will need to be submitted by the user's manager for approval.

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

1. Local User - User that does not authenticate through Active Directory (AD) - Used sparingly by Platform Administrators
2. Standard User Account (SUA) - VA User authenticated through Active Directory (AD)

3. Application Administrator - Administrator for specific support applications within the VA for dedicated functions and processes within the entire VA organization. (CMDB, Root Cause, Incident, ITIL, etc.)
4. Platform (System) Administrator - User has the ability to change platform configurations
5. Security Administrator - User that has the ability to create access controls
6. Service Account - Used for integrations to other systems and non-interactive activities, tied to VA integrations
7. External User accounts – VA Loan Guarantee (LGY) Users authenticated by VA Access or other non-AD Single Sign-on (SSO) mechanisms

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. Contractors sign a 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 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:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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

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

1. Security Plan status- Approved
2. Security Plan status date - July 7, 2020
3. Authorization status - Authorization to Operate (ATO)
4. Authorization date - June 18, 2020
5. Authorization termination date - June 18, 2023
6. Risk Review date – July 10, 2020
7. The FIPS 199 classification rating is - High

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)*

The Cloud Service Provider (CSP) Government Community Cloud (GCC) does have a FedRAMP ATO, granted on the same day as GCC-Enterprise (GCC-E). The GCC-FedRAMP ATO following the same guidelines as the GCC-E. ServiceNow is a single,

unified platform with a shared data model. ServiceNow is a Commercial off the Shelf (COTS), Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) with strong origins in Information Technology Service Management (ITSM) anchored to the ITIL framework.

The contract details the accountability, security, and privacy of VA data. A prohibition on unauthorized disclosure: "Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA." This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data – General, FAR § 52.227-14(d).(1).

A requirement for data breach notification: Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access, the Contractor/Subcontractor shall immediately notify the Contract Officer Representative (COR), including the designated ISO, and Privacy Officer (all three) for the contract. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. See VA Handbook 6500.6, Appendix C, paragraph 6.a.

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 the GCC.

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 the GCC.

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 GCC.

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 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**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.01.23 09:15:22 -05'00'

Privacy Officer, Tonya Facemire

Joseph W. Decoteau 123776

Digitally signed by Joseph W. Decoteau 123776
Date: 2023.01.18 08:48:49 -05'00'

Information System Security Officer, Joseph Decoteau

PRASHANTHI KUCHIKULLA

Digitally signed by PRASHANTHI KUCHIKULLA
Date: 2023.01.18 10:56:02 -05'00'

Information System Owner, Prashanthi Kuchikulla

Jannette D. Street 172766

Digitally signed by Jannette D. Street 172766
Date: 2023.01.22 21:10:06 -06'00'

Record Officer, Jannette D. Street

JOHN WORSHAM (Affiliate)

Digitally signed by JOHN WORSHAM (Affiliate)
Date: 2023.01.26 11:32:11 -06'00'

Reviewed for accuracy by PIA Support Analyst

APPENDIX A-6.1

Access to ServiceNow is contingent on implied consent within the VA National Rules of Behavior (VA Handbook 6500, Appendix A), and authorized access to VA information systems. https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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