

PRIVACY IMPACT ASSESSMENT

ServiceNow PIA

1. Contact Information

A/GIS Deputy Assistant Secretary

Bureau of Administration

Global Information Services

2. System Information

(a) **Date of completion of this PIA:** January 2022

(b) **Name of system:** IRM ServiceNow

(c) **System acronym:** SN

(d) **Bureau:** IRM

(e) **iMatrix Asset ID Number:** 177245

(f) **Child systems (if applicable) and iMatrix Asset ID Number:** N/A

(g) **Reason for performing PIA:**

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(h) **Explanation of modification (if applicable):** N/A

3. General Information

(a) **Does the system have a completed and submitted data types document in Xacta?**

☒ Yes ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) **Is this system undergoing an Assessment and Authorization (A&A)?**

☒ Yes ☐ No

If yes, has the privacy questionnaire in Xacta been completed?

☒ Yes ☐ No

(c) **Describe the purpose of the system:**

ServiceNow is a cloud-based Service (SaaS) solution that provides enterprise business productivity services and software used for collaboration, process management and approvals. ServiceNow (SN) customers are bureaus/offices at the Department of State (Department) who need commercial platform solutions to meet mission goals and manage information workflows. It is used both domestically and overseas by

organizations throughout the Department. SN is a secure, flexible, cloud-based platform on which to build out-of-the box, and custom automation workflows.

NOTE: Any office/bureau/post using ServiceNow to collect, maintain, store, or disseminate PII is responsible for completing the required privacy compliance documents.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

ServiceNow is used to support broad processing needs of Department personnel. Users will have access to a variety of suites and modules available via ServiceNow's cloud-based platforms and will employ them as tools in the course of their official business duties.

The Department of State's policy and guidelines restrict the information to the following elements of PII within IRM ServiceNow's User Profile (used by Active Directory to support Single Sign-On access to supported platforms):

- First Name
- Last Name
- Email Address (Government / business only)
- Telephone (Government / business only)
- Telephone (Personal)
- Title (Government / business only)
- Manager Name
- Employee Type
- Username
- Work Location
- Office Symbol

Note: While IRM maintains the Department's ServiceNow Platform, it does not own the data or processes stored within the system. Information contained in ServiceNow is owned by the collecting office/bureau/post. Each of these offices/bureaus/posts is responsible for completing a use-PIA for any collection that includes PII.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

22 U.S.C. 2581 (General Authority of the Secretary of State)

Additional authorities governing the collection of PII by ServiceNow application owners will be dependent on the functional authority of the office.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒ Yes, provide:

- SORN Name and Number:
STATE-56 – Network User Account Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
December 12, 2017

☐ No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐ Yes ☒ No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒ Yes ☐ No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
Legacy A-03-003-05 Configuration and Change Management Records
- Disposition Authority Number:
DAA-GRS-2013-0005-0005
- Length of time the information is retained in the system:
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.
- Type of information retained in the system:
Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems.

Additional retention schedules governing the collection of PII by ServiceNow owners will be dependent on the functional authority of the office.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- ☐ Members of the Public
- ☒ U.S. Government employees/Contractor employees
- ☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

- ☐ Members of the Public
- ☐ U.S. Government employees/Contractor employees
- ☐ Other
- ☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- ☐ Yes ☒ No ☐ N/A

- If yes, under what authorization?

(d) How is the PII collected?

User information is pushed from the Department of State managed Active Directory (AD) to ServiceNow and creates a user profile stored in a user table. AD receives the PII from IRM's MyProfile which must be updated by the user every 60 days.

(e) Where is the information housed?

- ☐ Department-owned equipment
- ☒ FEDRAMP-certified cloud
- ☐ Other Federal agency equipment or cloud
- ☐ Other

- If you did not select "Department-owned equipment," please specify.

ServiceNow Government Community Cloud (GCC) is authorized for FedRAMP High and Department of Defense (DoD) Impact Level 4 data and workloads. Information hosted in the ServiceNow GCC platform is stored in FedRAMP approved ServiceNow Data Centers. The GCC is physically and logically separated from other ServiceNow offerings.

(f) What process is used to determine if the PII is accurate?

There is a sync between AD and SN to update the information. When a user updates their information in AD, it is then updated in SN during the sync.

Upon receipt of request for a ServiceNow account, IRM validates that each request has been properly completed, routed, and approved by the necessary personnel.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Yes, all information is current. Updates between AD and ServiceNow are done on an hourly basis.

Also, ServiceNow works with the State Enterprise-Identity, Credential, and Access Management (SE-ICAM) Program Management Office (PMO) and leverages the Department's authoritative enterprise cloud-based multi-factor authentication service as the application's Identity Provider (IdP). ServiceNow leverages SE-ICAM Okta information to ensure currency of the user information.

For ServiceNow applications, maintaining accurate information is the responsibility of each office/bureau/post that has an application deployed on the ServiceNow platform.

(h) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use information from commercial sources or publicly available information.

(i) How was the minimization of PII in the system considered?

IRM ServiceNow is concerned with the privacy of potential and current customers. ServiceNow inherits the controls from SE-ICAM Okta as the only method of access. No additional information is collected at the platform level. Any office/bureau/post using ServiceNow to collect, maintain, store, or disseminate PII beyond what is inherited from SE-ICAM is responsible for completing the required privacy compliance documents.

5. Use of information

(a) What is/are the intended use(s) for the PII?

The PII in ServiceNow is used to establish a user profile via information collected from AD and is intended to associate a user with a request in order to fulfill a process, which is integrated with SE-ICAM. If a user requires access to the SN platform, a request is submitted to grant them access to the Identity and Access Management (IdAM) solution SE-ICAM Okta. The requestor can be either the individual themselves or a person on behalf of an individual.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, all the information collected is necessary to establish a user's profile on ServiceNow. The user profile on the ServiceNow platform allows users the ability to submit support tickets within the IT Service Module.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☒No

(d) If the system will use test data, will it include real PII?

☐Yes ☒No ☐N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:

N/A

External:

N/A

(b) What information will be shared?

Internal:

N/A

External:

N/A

(c) What is the purpose for sharing the information?

Internal:

N/A

External:
N/A

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
N/A

External:
N/A

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal:
N/A

External:
N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

No, notice is not provided to the record subject by ServiceNow. The record subject's information is pushed from the AD to ServiceNow and creates a user profile stored in a user table. Thus, ServiceNow is not the original collector of the record subject's information. If the record subject is an enterprise user, then they are required to keep their PII updated in MyProfile, which feeds into AD. MyProfile sends reminders to ensure a record subject's info is updated every 60 days when logging into OpenNet. Non-Enterprise users can update their information in SE-ICAM which feeds directly to ServiceNow.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐ Yes ☒ No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

ServiceNow does not obtain PII directly from the record subject. Information is either pushed from the Active Directory Federated Service (ADFS) or SE-ICAM to ServiceNow and creates a user profile.

(c) What procedures allow record subjects to gain access to their information?

Record subjects cannot directly gain access to their information in ServiceNow. After the record subject enters information into Active Directory, they can view their information any time after submission using the MyProfile portal. Non-enterprise users can view their information in SE-ICAM.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒ Yes ☐ No

If yes, explain the procedures.

Enterprise Users can update their information in the MyProfile portal at any time. The information will then be updated in Active Directory which feeds into ServiceNow. Non-Enterprise Users can change their personal information in SE-ICAM by selecting the edit button on their profile which automatically updates in ServiceNow.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Enterprise users are notified every 60 days by MyProfile that their information needs to be updated. Non-Enterprise users do not receive a notification in SE-ICAM but they are able to access their information at any time to update.

For ServiceNow applications, notification of the procedures for record subjects to correct their information is the responsibility of each office/bureau/post that has an application deployed on the ServiceNow platform. Customers with custom applications that are processing and storing PII would need to submit their own PIA.

8. Security Controls**(a) How is all of the information in the system secured?**

Security is built into all levels of the system, from managing failed logins and encrypted password protection, to access control rules and audit logs. By default, on all ServiceNow Instances, the high security plugin is enabled. The high security plugin is a tool for enhancing security management and configuration. The plugin creates or updates hundreds of different configurations to control the level of security of the instance. These configurations mitigate many of the top Open Web Application Security Project (OWASP) attacks by enabling strict access control, input validation, and output encoding. It also enables a Default Deny security posture, which prevents use of read, write, create, and delete functionalities for all tables, unless explicit permission is given for a user or role in an Access Control List (ACL) rule. Once a user has successfully authenticated, access to parts of the instance interface, functions, and the data within it are controlled

with ACLs and role-based access control (RBAC). ACLs use the account ID and associated groups to determine what access should be granted to an object, e.g., read, write, delete, create, etc.

ServiceNow information is housed on secure servers that are encrypted at rest and in transit by the FEDRAMP-approved ServiceNow Cloud.

All instances within the ServiceNow platform have Full Disk Encryption enabled. Additionally, Database encryption has also been enabled. With Database Encryption, all stored data is encrypted, and individual records or tables are decrypted in memory while being accessed. New or changed data is encrypted as it is entered into a table and associated activity log files (bin, redo, undo, and error) are also encrypted. All data is also encrypted in transit using Transport Layer Security (TLS) encryption. All end-user access to a ServiceNow instances attempted over HTTP are redirected to HTTPS. All data at rest is encrypted by default with full-disk encryption within the IRM ServiceNow environment. Additionally, all production instances use database (DB) encryption, which encrypts all data stored within the DB. Data is encrypted with Advanced Encryption Standard (AES) encryption and is decrypted in real time as its accessed.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Users: Access to this system is restricted to cleared Department of State (DoS) direct hire, eligible family members, and contractor employees. IRM ServiceNow relies on the Department to screen employees and contractor personnel as part of onboarding process and for changes to duty assignments to ensure that 12-FAH-10 H-282.2 criteria are met based on the individual, work location (domestic or abroad), and information access requirements. Users only have access to their own PII.

Privileged Users – Administrators (Platform Admin, Security Admin, Application Admin) create accounts and administer and manage the ServiceNow Platform. Platform administrators have logon identifications associated with their name that allows for user auditing. Platform administrators and Security Admins have access to username, business email, work location, employee type, manager name and email address and work and personal phone numbers. An Application Admin only has access to PII that is associated with the application they are supporting. The IRM System Owner must authorize personnel which have a need for permissions or privileges that require access to all user account PII.

(c) Describe the procedures established to limit system and data access to only those individuals who have an “official” need to access the information in their work capacity.

SN Platform Administrators are cleared DOS FTEs or contractors. Privileged access is granted by assigning administrator roles after System Owner (SO) and Information System Security Officer (ISSO) approval following the principles of least privilege.

When required, to restrict access to certain data, which may include PII, the admin override capability has been disabled. Additionally, an ACL for the table is assigned the nobody role, admin users cannot access the resource even when the Admin Overrides option is selected. However, the nobody role takes precedence over the Admin Overrides option. The IRM SN System Owner must authorize personnel which have a need for permissions or privileges that require access to user account PII. Privileged accounts are monitored continuously and reviewed on a quarterly basis.

(d) How is access to data in the system determined for each role identified above?

All access is enforced by user profiles according to the principle of the least privilege and the concept of separation of duties. By default, the High Security Plugin (HSP) is enabled on the platform. The HSP enables the high security settings, which includes some of the following: default deny property, which controls the security manager default behavior when the only matching ACL rules are the wildcard table ACL rules. Prevents read, write, create, and delete for all tables unless explicit permission is given for a user or role in an ACL rule.

Users – Users' only have access to their information and PII and other information which they are explicitly granted access to base on their organizational requirements and the determination of the information owner.

Privileged Users – Administrators (Platform Admin, Security Admin, Application Admin) create accounts and administer and manage the ServiceNow Platform. Platform administrators have logon identifications associated with their name that allows for user auditing. The IRM System Owner must authorize personnel which have a need for permissions or privileges that require access to user account PII. Access to the system is revoked once the privileged user terminates or is reassigned to a different position.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

The ServiceNow Platform records field changes in continuous database logging accessible by only ServiceNow Technical teams. Users with expired OpenNet credentials will be unable to access the ServiceNow platform.

Customer accessible audit logs will be available to each bureau/office and reviewed by local administrators to prevent the misuse of the information in SN.

Security event and audit data, which contain user identity along with system access and activity, is monitored by the Bureau of Diplomatic Security (DS) in accordance with State policy for security monitoring 12 FAM 500.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒ Yes ☐ No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

In regard to all of the roles identified in 8b that have access to PII on the ServiceNow Platform, all Department employees, Federal and contractor, are required to complete annual cyber security training (PS800), which includes a section on PII, and also a section on Protecting Department Information. Additionally, they are required to complete PA318 Privacy Training every two years. PA318 incorporates privacy-based legal requirements, updated Department policies, and lessons learned from past personally identifiable information (PII) breaches.