EPA United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: ServiceNow	
System Owner: Willie Abney	
Preparer: Gloria Meriweather	**Office: Office of Mission Support**
Date: April 10, 2024	**Phone: 202-566-0652**
Reason for Submittal: New PIA____ Revised PIA____ Three-Year Review __X__ **Rescindment ____**	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

EPA ServiceNow is a suite of natively integrated applications designed to support IT service automation (ticketing & configuration activities), resource management, and shared support services throughout the agency. ServiceNow uses a modular approach that allows customers to use specific services within the EPA's instance for viewing, editing, and updating configuration items or tickets that are routed for distribution to various regions and groups across the agency. ServiceNow is customizable to support various applications that cover all of the Information Technology Infrastructure Library (ITIL) processes and is natively integrated within one single platform for providing web intuitiveness and process automation. To support these various services, ServiceNow is built on several automated modules that allow dashboard viewing, project tracking/reporting, as well as project planning and reporting.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The specific legal authority for this collection of information is 5 U.S.C. § 301 "Departmental Regulations".

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes, the System Security Plan has been completed. A new Authority to Operate (ATO) will be issued in Fiscal Year 24. The current ATO expired on March 11, 2024.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

ServiceNow is not subject to the PRA.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

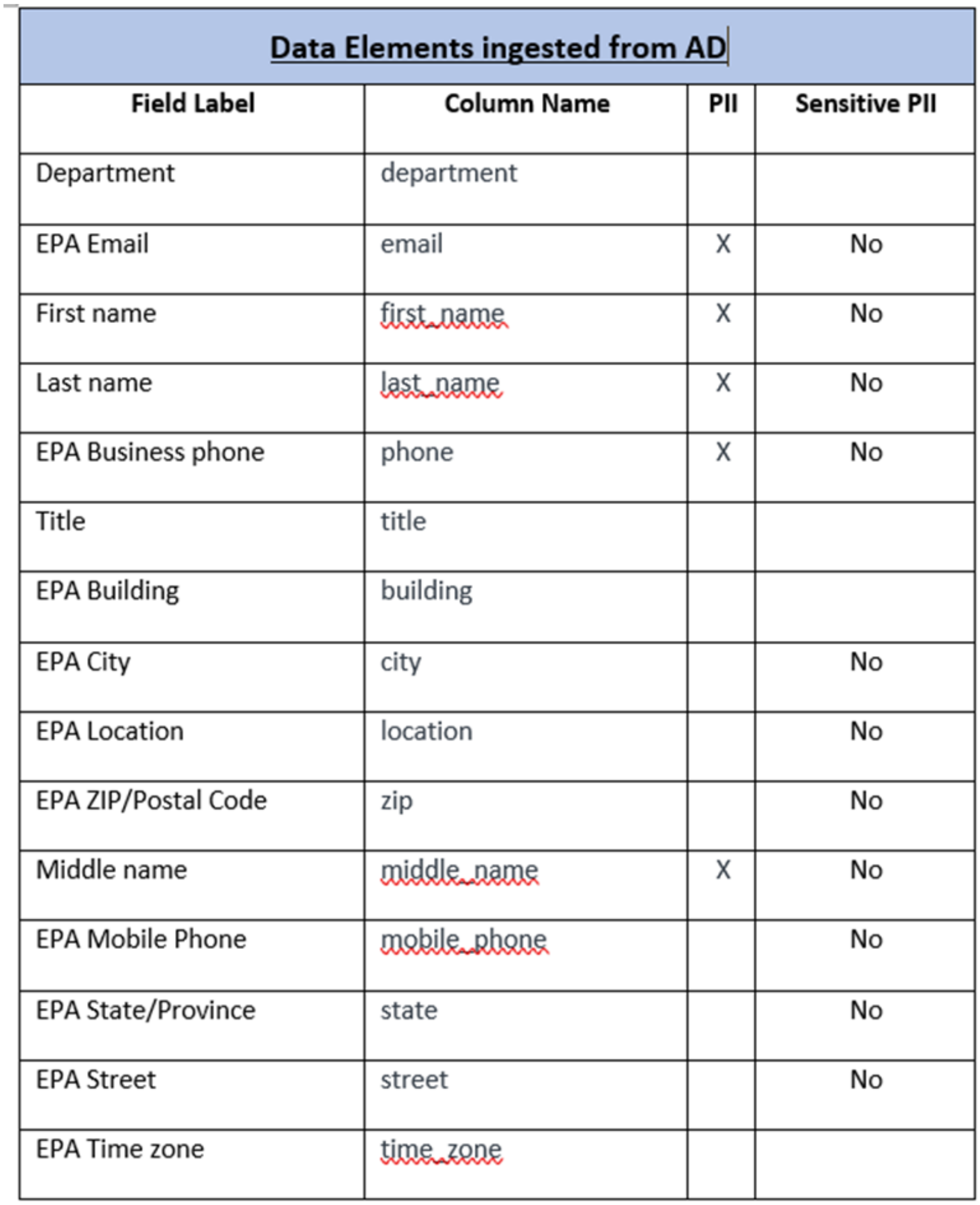
Yes, data will be stored in the EPA Cloud, and ServiceNow is FedRAMP approved. This is a SaaS cloud service provider.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

EPA uses ServiceNow to create and manage service tickets. To create a service ticket, EPA ServiceNow collects the following information from the users who have made a service request:



Data Elements ingested from AD

Field Label	Column Name	PII	Sensitive PII
Department	department		
EPA Email	email	X	No
First name	first_name	X	No
Last name	last_name	X	No
EPA Business phone	phone	X	No
Title	title		
EPA Building	building		
EPA City	city		No
EPA Location	location		No
EPA ZIP/Postal Code	zip		No
Middle name	middle_name	X	No
EPA Mobile Phone	mobile_phone		No
EPA State/Province	state		No
EPA Street	street		No
EPA Time zone	time_zone		

* SPII (SSNs, home addresses, and financial information) related to privacy incident response maybe maintained within ServiceNow.

2.2 What are the sources of the information and how is the information collected for the system?

ServiceNow collects information from EPA employees (contractors & Feds), EPA contractors, federal, state, and local government partners. The information is collected when employees or partners engage the Enterprise Information Service Desk(EISD) service desk.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ServiceNow does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Data is collected directly from all EPA users who make a request. Data collected from email and telephone requests are manually entered into EPA ServiceNow by EISD Support Technicians. For individuals who call into the EPA Call Center, the EISD Support Technician asks a series of questions to confirm the caller's identity, according to the Service Desk Standard Operating Procedures (SOP), to assist with the inquiry, and prevent the unauthorized disclosure of information. EPA ServiceNow automates the Help Desk accuracy by mapping an EPA user's full name to the associated Active Directory account.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is a risk that SPII is uploaded unnecessarily by users to create a service ticket.

Mitigation:

This risk is partially mitigated. In order to create a service request ticket, limited business and contact information about EPA personnel or non-EPA personnel are obtained directly from the requestor. Only the minimum amount of information is gathered in order to identify an individual and distinguish him or her from other users with similar attributes (e.g., same first and last name). Only EPA personnel have access to myIT to upload files that may be relevant to users' requests for service and support. Due to technical limitations, there are no restrictions placed on the types of files uploaded, or the content they may contain. As such, it may be possible for EPA personnel to upload files that contain sensitive PII and may include SSNs, home addresses, etc. This risk is partially mitigated because SPII that may be uploaded in an attachment, is not retrievable by unique identifier.

Privacy Risk:

There is a risk that service requests received by phone are inaccurately entered into EPA ServiceNow.

Mitigation:
This risk is mitigated through administrative and technical controls. EPA IT Support Technicians ask a series of questions to confirm the caller's identity, according to the Service Desk SOP, to assist with the inquiry, and prevent the unauthorized disclosure of information. EPA ServiceNow automates the Service Desk accuracy by mapping a EPA user's full name to the associated EPA Active Directory account to ensure technical support reached the assigned technician and the appropriate individual seeking support. An electronic identity is created and assigned to a single individual in the EPA Active Directory, with the purpose of identifying and authenticating that user specifically. Non-EPA personnel cannot be checked in the Active Directory.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

There are preventative access controls within EPA ServiceNow enforced by internal application role-based permissions. These role-based controls provide separation of duties and limits access to data within the application to only individuals on a need to know. The assigning of roles enhances adherence to the principle of least privilege.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access to information is controlled through Active Directory Users and Computers (ADUC) via Access Control List (ACL). Access can be revoked or edited by the site owner using theses ACLs. The ACL groups determine the roles and what information can be access by which users.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, other components have assigned roles and responsibilities within ServiceNow.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

EPA ServiceNow, and the data contained within, will not be accessible to any external parties (i.e., the public, outside agency, or external companies/contractors). All internal EPA users will have access to ServiceNow IT. The appropriate FAR clauses have been incorporated into the contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

EPA ServiceNow is under EPA Records Control Schedule 1012(b).

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There is a risk that information may be retained longer than needed.

Mitigation:

ServiceNow adheres to EPA Records Schedule associated with data.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No. EPA does not share EPA ServiceNow information with external entities.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

No. EPA does not share EPA ServiceNow information with external entities.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

No. EPA does not share EPA ServiceNow information with external entities.

4.4 Does the agreement place limitations on re-dissemination?

No. EPA does not share EPA ServiceNow information with external entities.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Not Applicable.

Mitigation:

Not Applicable

Section 5.0 Auditing and Accountability

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

5.1 How does the system ensure that the information is used as stated in Section 6.1?

EPA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The US EPA implements a Rules of Behavior (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the EPA implementation of User Security and Privacy Awareness training which is provided annually. In addition, all EPA personnel receive annual refresher cybersecurity training to educate them regarding the use and management of sensitive data.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a risk that some EPA ServiceNow users may not complete required training.

<u>Mitigation</u>:

This is mitigated through policies that disables a user's account access to the EPA for not completing all required training. Disabling a user's account also removes their access to EPA ServiceNow. Additional measures are in place for EPA ServiceNow IT personnel that requires training to be completed before access is granted to any additional roles outside of regular EPA user.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

The EPA uses the data collected by EPA ServiceNow to provide technical support and other service-oriented activities to support EPA systems and applications. EPA technical support teams use a user's information to provide support for EPA IT systems, assets, and properties. Service orientated activities include the following:

- Managing and retrieving service request tickets
- Troubleshooting Issues
- Managing IT Assets
- Conveying outage information across EPA

<u>Privacy Risk:</u>

There is a risk that unauthorized users may access records in ServiceNow.

<u>Mitigation:</u>

This risk is mitigated. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. ServiceNow is a web-based application that is only available through the EPA network. Access to ServiceNow is granted to only a limited number of users through EPA. Users must authenticate their credentials to gain access to the system.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X__. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

EPA personnel are not able to query ServiceNow to retrieve information by a personal identifier. However, information is retrieved by incident ticket number.

6.3 What type of evaluation has been conducted on the probable or potential

effect of the privacy of individuals whose information is maintained in the system of records?

Not applicable.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is a low risk that sensitive or personal information can be used outside of the system or that information can be compromised outside of ServiceNow and used for an illegal purpose or to infiltrate other records in ServiceNow for various reasons.

Mitigation:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. Users must authenticate their credentials to gain access to the system.

Prior to gaining access to the system, EPA ServiceNow displays a warning banner on the login screen to advise all users about the proper and improper use of the data, that the system may be monitored to detect improper use, and the consequences of such use of the data. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This acts as a deterrent to unauthorized activity.

The risk is also mitigated through role-based access rules governing technical support personnel usage. EPA personnel can access the ServiceNow portal to create a service ticket and are only able to view their own service requests along with the status. General users cannot view service requests submitted by other users. IT Support Technicians can view information submitted by general users that contain only PII data as part of their duties in reviewing and responding to service request tickets. Users are informed of their roles and responsibilities in regard to protecting PII. Users have been trained to provide only the minimum amount of PII necessary to complete a service request.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: