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: EPA ServiceNow (SNOW)	
Preparer: Gloria Meriweather	**Office:** OMS-OITO-DSSD
Date: December 17, 2020	**Phone:** 202-566-0652
Reason for Submittal: New PIA____ Revised PIA____ Annual 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 Cloud Based Software as a Service (SaaS) Information Technology Service Management (ITSM) platform that is used for EPAs service request, incident and problem management solution.

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", 8 U.S.C § 1101, 1103, 1104, 1201, 1255, 1305, § 3101 "Records Management by Federal Agency Heads."

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. The ATO was issued on April 5, 2018 and it has an expiration date of April 3, 2021.

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.

No Information Collection Request (ICR) is required.

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, the data will be maintained or stored in a cloud. The CSP, ServiceNow - ServiceNow Service Automation Government Cloud Suite, is FedRAMP approved. The CSP provides SaaS.

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).

The following is a list of Data Elements captured by the EPA instance of ServiceNow (SNOW) and utilized by the EPA Enterprise Service Desk to perform their contractual duties. *All location based and phone related data elements listed in the table below are explicitly associated with business location details unless otherwise noted.*

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		
EPA Office/Cubicle Number	_office_cubicle_number		No

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

SNOW collects information from EPA employees, EPA contractors and federal, state and local government partners as they open self-service help request or when they call into the EPA Call Center.

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

EPA 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 IT Support Technicians. For individuals who call into the EPA Call Center, the EPA IT 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 EPA Active Directory account to ensure technical support reached the assigned technician and the appropriate individual seeking support. An electronic identity, uniquely defined by EPA Active Directory, is created and assigned to a single EPA individual with the purpose of identifying and authenticating that user specifically.

Information is checked for accuracy through self-verification by either the user or the EPA IT Support Technician entering information to process a service request. EPA Call Center personnel ensures data accuracy in EPA ServiceNow through program coding to mitigate or prevent inconsistencies in data. The data fields in the input screen are configured to limit the possibility of entering malformed data (e.g., the system rejects 000/000/0000 phone numbers). EPA personnel or EPA IT Support Technicians can review and edit information prior to and after their submission. Additionally, only authorized EPA IT Support Technicians can correct and edit inaccuracies brought to their attention at any stage of the process.

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 (sensitive PII) is uploaded unnecessarily by users to create a service request ticket.

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

Mitigation:

When a ticket is created by the customer or by the service help desk, the following message is displayed: Please do not submit Sensitive Personally Identifying Information (SPII) through this

form, including attachments. Examples include your social security number, credit card number, or any passwords. ServiceNow and the Environmental Protection Agency will never request these items.

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 basis approved by the system owner. 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 controls are documented in Service now Procedure.

Individuals must be an EPA employee or contractor with a valid EPA LAN account and PIV card in order to access ServiceNow. Once verification has been completed upon login, access is granted to application. Access to the system is authenticated by EPA identity access management, users using role-based access controls which enforces separation of duties.

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

No.

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 the ServiceNow IT services catalog, if they have a valid and active EPA LAN account. These users will have limited access to their ServiceNow profiles to allow verification and correction of information.

Only EPA End User Services contractors will have access to data/information to perform administrative duties and meet reporting requirements as define by EPA contract Service Level Agreements (SLAs).

Necessary FAR clauses have been included in the EPA EUS contract that was awarded to SAIC in March of 2017.

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 retains information under EPA records schedule 1012(b), Records Control Schedule destroys after 7 years after file closure, this is in accordance with EPA Policy to help support after the fact investigation.

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:

SNOW adhere to record control schedule associated with its 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.

SNOW does not share information externally.

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

EPA ServiceNow will only share externally for only authorized uses as stated in the FR Notice and SORN. As stated in the SORN, Citation 84-FR 2709, routine uses apply to this system because the use of the record is necessary for the efficient conduct of government. The routine uses – Disclosure for Law Enforcement, Disclosure Incident to Requesting Information, Disclosure to Congressional Offices and Disclosure to Department of Justice – are related to and compatible with the original purpose for which the information was collected.

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?

SNOW does not share information.

4.4 Does the agreement place limitations on re-dissemination?

SNOW does not share information.

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:

None. There is no external sharing either than the routine uses.

Mitigation:

N/A

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 ServiceNow ensures that the practices stated in the PIA are followed by leveraging training, policies, EPA Rules of Behavior, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user in order 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.

Mitigation:

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 service request tickets
- Retrieving incident information;
- Troubleshooting Issues
- Managing IT Assets
- Conveying outage information across the enterprise.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_ No___. 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.*)

Yes. EPA ServiceNow uses several identifiers such as user name or first and last name.

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?

[The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.]

The Security controls used to protect the PII data collected in EPA ServiceNow (SNOW) are in compliance with those required for an information system rated "MODERATE" for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 4.

Administrative Safeguards

- Elevated roles are limited to a few select administrators.
- Records in SNOW are reviewed before closure for sensitive/PII information prior to closure. Any unnecessary PII that should not be stored in the system is then removed.
- Electronic records are maintained in a secure, password protected electronic system stored in a FedRAMP approved cloud.

Physical Safeguards

- ServiceNow Inc. CSP maintains DoD level secure location with access-controlled areas or buildings.

By limiting strict access roles and privileges and implementing these security controls, ServiceNow is able to protect and limit the use of any PII data collected to the groups that use this information and will allow ServiceNow to maintain a "defense-in-depth" security posture.

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 risk that unauthorized users may access records in EPA ServiceNow.

There is a risk that EPA ServiceNow could be used for purposes outside the scope of IT support.

Mitigation:

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. 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 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 mitigated through role-based access rules governing technical support personnel usage. EPA personnel can access 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 regarding 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.

The required Privacy Act Statement notifying the individuals about the authority to collect the information requested, purposes for collecting it, routine uses, and consequences of providing or declining to provide the information to EPA is posted at the EPA Enterprise IT Service Desk (EISD) Call Center.

In addition to the Privacy Act Statement being posted at the Enterprise IT Service Desk, End User Services EPA ServiceNow (SNOW) provides a warning message at the bottom of the Customer Service Portal to not enter Sensitive PII (SPII) along with different types of examples (SSN, Credit Card information, etc.).

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?

Individuals can choose to not provide information to address their IT matter but doing so will prevent IT Support Technicians from addressing the individual's matter in an efficient and effective manner.

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:

There's risk that personal information is captured in ServiceNow without the user's consent.

Mitigation:

The risk is mitigated by the EPA ServiceNow user being able to cancel the self-service request before submitting any information that could be captured by ServiceNow.

EPA Enterprise Service Desk Support personnel verify that sensitive information isn't being

entered into ServiceNow when EPA user's call in for support. Prior to submitting service request tickets, Enterprise Service Desk Support personnel verify accuracy of information with requestor and verify the need of request submittal.

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.

EPA personnel who telephonically report a service request receive an EPA ServiceNow-generated email detailing the issue and status of the request. Only EPA personnel who submit a request through EPA ServiceNow portal may view their records. Additionally, individuals may seek access to his or her EPA records by filing a Privacy Act or Freedom of Information (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Any person, regardless of immigration status, may file a FOIA request.

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.

There is a system in place for individuals to correct inaccurate information about them. Individuals submit EISD service request to have inaccurate information changed.

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:

None. EPA will always provide access and amendment of ServiceNow records. EPA notifies

individuals of the procedures for correcting their information in this PIA, Privacy Act Statement, and through the EPA internal website (EPA personnel only) and ServiceNow user-based training

Mitigation:

N/A