EPA United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: ServiceNow (SNOW) Enterprise Service ()	
Preparer: Vincent Ross	**Office:** OEI/EDSD
Date: October 26, 2017	**Phone: 919-767-7321**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐	

Note: 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 platform. This platform will be used for EPAs incident and problem management solution. ServiceNow is slated to replace the current EPA Remedy solution, but will provide more functionality.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements 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, 1360 “Aliens and Nationality”44 U.S.C. § 3101 “Records Management by Federal Agency Heads.”

1.2 Has a system security plan been completed for the information system(s) supporting the system?

In Progress, System Security Plan for EPA ServiceNow instance is currently being developed and documented as required.

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.

EPA ServiceNow is NOT covered by the Paperwork Reduction Act (PRA).

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 information captured (collected) by the End User Services (EUS) ServiceNow solution have been detailed in Appendix A of this form.

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

The SNOW collects a varity of information from EPA employees and EPA contractors as they open up self service help request or when they call into the EPA Call Center.

All data elements captured by the End User Services (EUS) ServiceNow solution have been detailed in Appendix A of this form. The ServiceNow solution utilizes Active Directory services, managed by the Directory Service group, to ingest certain data elements that are needed for ServiceNow Enterprise Service Desk support. The data elements ingested from AD have been identified and parsed out in a separate table in Appendix A.

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 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, 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. Non-EPA personnel cannot be checked in the Active Directory.

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 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

There is a risk that SPII (sensitive PII) is uploaded unnecessarily by users to create a service ticket.

<u>Mitigation</u>:

This risk is partially mitigated. In order to create a service request ticket, limited business and contact information about EPA personnel is 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 ServiceNow user portal 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, A-Numbers, Receipt numbers, EPA Online Account Numbers, home addresses, host names and dynamic IP addresses. This risk is partially mitigated because SPII that may be uploaded in an attachment, is not retrievable by unique identifier, and prior to the closing of a ServiceNow ticket any data within the notes field as well as any other documents/content are removed.

<u>Privacy Risk</u>:

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

<u>Mitigation</u>:

This risk is mitigated by 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 (EPA Call Center) 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 Uses of the Information

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

3.1 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;

.

3.2 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 leverages several unique identifiers, (i.e. user id, computer name, birth name, etc.). The use of multiple unique identifiers allows the Enterprise Service Desk technician multiple ways to verify an individual's authenticity as it relates to EPA.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

See Appendix A at end of document.

3.4 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

No System of Records (SOR) has been provided for EPA ServiceNow.

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

EPA ServiceNow does NOT use technology to discover or locate predictive patterns or anomalies.

3.6 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.

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.

Privacy Risk:

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

Mitigation:

The risk is mitigated through role-based access rules governing technical support personnel usage. EPA personnel are able to 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 are able to 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 regards to protecting PII. Users have been trained to provide only the minimum amount of PII necessary to complete a service request.

Section 4.0 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.

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

EPA ServiceNow users receives general notice through the publication of this PIA. The EPA provides a Privacy Act Statement prior to the collection of any information on ServiceNow portal as required by Section (e)(3) of the Privacy Act. The Privacy Act Statement notifies the individual 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.

4.2 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.

4.3 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 5.0 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.

5.1 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?

EPA ServiceNow user accounts are managed through EPA Infrastructure Active Directory (LDAP) authentication. Users authenticate through LDAP to gain access to EPA ServiceNow. ServiceNow IT support staff deploys user role-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each operational role is assigned to the set of system authorizations required to support the intended duties of that role. The assigning of roles to associated authorizations enhances adherence to the principle of least privilege. This need-to-know is determined by the respective responsibilities of the user. These are enforced through EPA email request and request tickets.

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

No. Access to EPA ServiceNow, including ServiceNow portal and ITSM, is limited to only EPA personnel. Non-EPA personnel are denied access to EPA ServiceNow.

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

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, as long as 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 EUS contractors will have access to data/information to peform administrative duties, and meet reporting requirements as define by contract SLAs..

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

5.4 What procedures are in place to determine which users may access the information and how does the system determine who has access?

EPA ServiceNow user accounts are managed through EPA Infrastructure Active Directory (LDAP) authentication. Users authenticate through LDAP to gain access to EPA ServiceNow. ServiceNow IT support staff deploys user role-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each operational role is assigned to the set of system authorizations required to support the intended duties of that role. The assigning of roles to associated authorizations enhances adherence to the principle of least privilege. This need-to-know is determined by the respective responsibilities of the user. These are enforced through EPA email request and request tickets.

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

Currently the EPA ServiceNow instance is inheriting records retention capabilities from the ServiceNow FedRAMP SaaS. A EPA Records Control Schedule has not yet been developed/assigned for this system.

5.6 Does a records retention schedule approved by the National Archives and

Records Administration (NARA) exist?

Currently a records retention schedule approved by NARA does not exist for the EPA instance of ServiceNow. A SORN for this system has not been generated.

5.7 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 with the stated purpose and mission of the system.

Privacy Risk:

There is a risk that EPA ServiceNow is not meeting the Federal guidelines and requirements for records retention by a government information system.

Mitigation:

To mitigate this risk, EPA ServiceNow will work with the SaaS provider (ServiceNow) to develop a records retention plan that meets all applicable Federal guidelines, mandates and requirements.

Section 6.0 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.

6.1 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.

Not Applicable –to ServiceNow.

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

Not Applicable - ServiceNow does not share data with other agencies.

6.3 Does the agreement place limitations on re-dissemination?

Not Applicable - ServiceNow does not share data with other agencies.

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

Not Applicable - ServiceNow does not share data with other agencies.

6.5 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?

Not Applicable –to ServiceNow.

6.6 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:

There is no privacy impact related to external information sharing because EPA ServiceNow information is not shared with external entities

Mitigation:

N/A

Section 7.0 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.

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

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.

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

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 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.

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.

7.3 How does the system notify individuals about the procedures for correcting their information?

This PIA explains how an individual may correct his or her information once obtained by EPA ServiceNow.

7.4 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:

N/A

Mitigation:

N/A

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.

Section 8.0 Auditing and Accountability

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

8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

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 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.

8.2 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 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.

8.3 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.

Appendix A: DATA ELEMENTS

A) ServiceNow Data Elements ingested from Active Directory Services;

Data Elements ingested from AD			
Field Label	**Column Name**	**PII**	**Sensitive PII**
Active	active		
Department	department		
EDU Status	edu_status		
Email	email	X	No
Employee number	employee_number	X	No
First name	first_name	X	No
Last name	last_name	X	No
Business phone	phone	X	No
Title	title		
User ID	user_name		
Employee ID	u_employee_id	X	No

B) Data Elements captured by ServiceNow

Data Elements captured by ServiceNow			
Field Label	**Column Name**	**PII**	**Sensitive PII**
Active	active		

Average Daily FTE Hours/Hours Per Person...	average_daily_fte		
Building	building		
City	city	X	No
Company	company	X	No
Cost center	cost_center		
Country code	country	X	No
Date format	date_format		
EDU Status	edu_status		
Failed login attempts	failed_attempts		
Gender	gender	X	No
Home phone	home_phone	X	No
Prefix	introduction		
Last login device	last_login_device		
Last login time	last_login_time		
Last password	last_password		
Location	location	X	No
Locked out	locked_out		
Zip / Postal code	zip	X	No

B) Data Elements captured by ServiceNow (continued)

Data Elements captured by ServiceNow (continued)

Field Label	Column Name	PII	Sensitive PII
Manager	manager		
Middle name	middle_name	X	No
Mobile phone	mobile_phone	X	No
Name	name	X	No
Notification	notification		

Password needs reset	password_needs_reset		
Photo	photo	X	No
Language	preferred_language		
Schedule	schedule		
State / Province	state	X	No
Street	street	X	No
Time sheet policy	time_sheet_policy		
Time zone	time_zone		
Password	user_password		
CID	u_cid	X	No
Notes	u_notes		
Office/Cubicle Number	u_office_cubicle_number	X	No
ORD-NCCT	u_ord_ncct		
Portfolio	u_portfolio		
Premier	u_premier		
Sensitive AT	u_sensitive		
VIP	vip		