U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: ServiceNow – OCIO Radio (ServiceNow – OR)
Bureau/Office: Office of the Chief Information Officer (OCIO)
Date: September 27, 2022
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

ServiceNow – OCIO Radio (ServiceNow – OR) is a cloud-based system sponsored by the Department of the Interior (DOI), Office of the Chief Information Officer (OCIO), Service Delivery, Telecommunications, Radio Program Management Office, to provide an enterprise and

shared IT service management solution customized for the DOI radio communications program needs. This system will support all DOI bureau and office mission areas that use radio and field communications. ServiceNow – OR also provides shared services between DOI bureaus and offices and the USDA Forest Service, Department of Justice (DOJ), and Department of Homeland Security (DHS) who are end users of the system.

This system will be used to manage the shared support services for radio and field communications (Field Com) by allowing users to update their contact information, submit service requests for changes or to report outages or failures. Users may also view outage notices, use the self-help information guide, training, and frequently asked questions regarding Field Com. ServiceNow – OR will be used by the service support technicians and managers to maintain an inventory, configuration, and lifecycle of the Field Com assets, perform the service requested, and manage the services provided to the users. Individuals may submit a request to the ServiceNow – OR helpdesk who will enter the required information for contact purposes and to process the request.

C. What is the legal authority?

5 U.S.C. 301; Consolidated Appropriations Act (Public Law 113-76, Sec. 430); Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service*; Presidential Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*; Presidential Memorandum, *Building a 21st Century Digital Government*; and Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource.*

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000000004; ServiceNow – OCIO Radio System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

INTERIOR/DOI-58, Employee Administrative Records, 64 FR 19384, April 20, 1999; modification published at 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021). DOI SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Other: *Specify the PII collected.*

Service technicians will verify individual's information that may be collected which includes full name, Active Directory (AD) alias, work email address, work phone and cell phone number, office address, agency or bureau or office, organizational code, line of business/mission area, and assigned government assets, such as property or vehicle, vessel or aircraft that has a radio associated with it. Name and email addresses of service technicians, help desk staff or other staff assigned or responding to the request are included in the service ticket.

An individual's personal cell phone number is not required for ServiceNow – OR to receive radio support service; however, customers may provide this information for the service technicians to easily contact them and expedite the service. This information could also be

inadvertently entered into the ServiceNow – OR system directly by the customer in their contact information in the "Work Cell Phone Number" field.

DOI bureau and office users, including the service technicians, are authenticated through the DOI AD. The Forest Service, DOJ and DHS users have to create a username and password to access the system.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

Individuals may provide information to a service technician who will enter that contact information into ServiceNow – OR. Individuals may enter or update their own information directly in the ServiceNow – OR website. AD is used to authenticate a DOI user's access to the system and the contact information is automatically populated into the DOI user's profile . Forest Service, DOJ, and DHS users will provide their contact information during the account creation process.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe*
☒ Other: *Describe*

Individuals may provide their information to a service technician via an email, interview over the phone, or a face-to-face interaction. Individuals may enter or update their contact information in the DOI ServiceNow – OR website. AD is used to authenticate users and contact information for the DOI users are automatically populated into the system. Forest Service, DOJ, and DHS users will provide their contact information during the account creation process.

Customers may also submit their request to the service technician via fax, which may include the customers' contact information for identity verification in order to provide the service. These documents contain the individual's name, email address, work phone number , as well as the fax number which may be entered into ServiceNow – OR by the service technician to support future communications with the individual. Individuals will be instructed to call the service technicians in advance to make sure they are waiting at the fax machine when a document is sent. In addition, the fax machine is located in a secured facility.

D. What is the intended use of the PII collected?

The information collected is used to identify the individual, coordinate and provide radio support services, determine the individual's eligibility to receive the services; authenticate the individual's access to the ServiceNow – OR system; and determine the service technician or service group that will provide the support to the individual, the type of equipment the individual uses, and the type of support service is required.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*
PII data is shared within OCIO to process service requests. The PII is only used for contact purposes. The OCIO service technicians can only access information of users located within their assigned support area . The OCIO users requesting the service may only access the service technician contact information that is supporting their request. OCIO service managers has access to all OCIO data ServiceNow – OR system administrators has access to all user data for ServiceNow – OR account management purposes.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

In a shared service environment, a service technician can only access data of bureau/office users requesting the service in their assigned support area only. The bureau/office users requesting the service may only access the service technician contact information supporting their request, who may be from another bureau/office. Bureau/Office shared service area managers may only access their bureau/office user information who are located in their assigned service area. ServiceNow – OR system administrators access all bureau/office user data for ServiceNow – OR account management purposes. All data shared with other bureaus/offices are only used to contact the users to process the service request.

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

In a shared service environment, a service technician, who may be a contractor, may only access information on users requesting the service in their assigned support area. These users may also be contractors. The users will only access the service technician information supporting their request. Shared service area managers, who may be contractors, may only access information on the users. ServiceNow – OR system administrators are not contractors. ServiceNow – OR system administrators will access all customer data to identify and contact the users for ServiceNow – OR account management.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

A user may choose to decline identifying themselves within ServiceNow – OR and receive service verbally by contacting their service support technician via phone, email or fax. The service technician would then document the work within ServiceNow – OR as "anonymous" and the work will be associated with the equipment and not the individual. However, there may be a delay in providing service if the service technician is unable to contact the user with any questions or for more information. Service Technicians, Service Managers and System Administrators must provide their information to access and use the system, and perform their service work.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act statement is provided to users on the system login website.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this PIA and the INTERIOR/DOI-58 SORN.

☒ Other: *Describe each applicable format.*

Upon logging into the ServiceNow – OR system, individuals will be notified that their use of the system may be monitored. Their name and AD account information are used to identify the user, the roles and permissions and any related service requests, government assets, and any service

history associated with them. Their contact information will be used to communicate with them regarding any radio communications services.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data may be retrieved by searching the customer's name, service ticket number, assigned government asset, phone number, email address, agency and bureau or office, office name or office address, system group association or role assignment, service area assignment, account activity and status, AD short name/alias, line of business, and system record or transaction dates.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

System and Security Administrators will conduct manual or configure automated report generation on account activities for system security reasons. These reports will provide user account activities such as: failed login attempts; account activity volume and timing; and expired, suspended, deleted, and active accounts. These reports may include full names, AD alias, contact email address and work phone number, account status, account type, and group and role assignment. These reports will be used to perform security assessments, account validation, and account changes. These reports will not be shared outside of the administrator group.

Service Managers will generate reports for the purpose of assessing service workload efficiency and to define problems areas with the service or equipment. They will conduct manual or configure automated report generation. These reports may include full names and work email address and phone number of users and service technicians, as well as, service ticket numbers, location, agency and bureau or offices, transaction dates and equipment and assets. These reports will not be shared.

Users may generate reports of their own, which may include their full name and contact information, status of their service request and the history of service request tickets that have been generated under their name.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Records will be verified and updated by a service technician or help desk each time the

individual makes contact for a services request unless they decline to be identified in ServiceNow – OR. The individual may update their information (Self-Service) within ServiceNow – OR. The records are updated due to changes in AD through system-to-system data sharing.

B. How will data be checked for completeness?

The service technician will go over the checklist used when a person contacts the help desk to verify user identity. They will check all mandatory field completion and data entry validation for Self-Service by the individual within the ServiceNow – OR system. They will use the check and balance processes within AD to ensure accuracy of data provided to ServiceNow – OR from AD.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Records will be updated each time the person contacts the help desk. Self-Service by the individual within the system will be required after logging-in every 6 months while their account is active. Updates provided by changes in AD will be implemented.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

The ServiceNow – OR system falls under DOI Departmental Records Schedule (DRS) 1.4. Short-term Information Technology Records, System Maintenance and Use, which is approved by the National Archives and Records Administration (NARA) (DAA-0048-2013- 0001-0013). These records have a temporary disposition and are determined obsolete when they are no longer needed for administrative, legal, audit, or other operational purposes, and destroyed no later than 3 years after cut-off. Once the individual leaves the organization, those records are archived and when the individual's assigned equipment is disposed of that record is also archived.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Disposition methods are in accordance with Departmental policy and NARA guidelines. ServiceNow – OR's Table Cleaner Program is an automated deletion process based on the expiration date setting for any records. This is automatically executed daily. Administrators also perform manual deletion and deletion scripts based on specific parameters such as employee name, equipment serial number, etc. Deleted record data is eventually overwritten by other data as the system is used.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is minimal privacy risk due to the limited official contact information which may include full name, AD alias, work email address, work phone and cell phone number, office address, agency or bureau or office, organizational code, line of business/mission area and maintained in the system to provide radio communications service to users. This risk is mitigated by implementing technical, physical, and administrative controls.

There is a risk that administrators could download or use records of individuals in the system for an unauthorized purpose. This risk is mitigated by conducting background checks on all administrators. All employees and contractors must complete Information Management and Technology (IMT) Awareness training, which includes cybersecurity, privacy, records management, Controlled Unclassified Information, Section 508, and Paperwork Reduction Act, as well as role-based privacy and security training on an annual basis, and agree to adhere to the DOI Rules of Behavior prior to accessing ServiceNow – OR.

There is also a risk of unauthorized access, unauthorized disclosure or that information may be used outside the scope of the purpose for which it was collected. This risk is mitigated by the access controls implemented to ensure only authorized personnel have access to the records needed to perform official duties. Access is based on "need-to-know" and grouped into Roles by the System Administrator. The grouping is established based on the role of the person and what data they require based on that role. User activity is monitored, and account access and denial are logged as well as any record changes are logged. These logs are reviewed in accordance with Standard Operating Procedures where the system security administrator will be reviewing logs for inappropriate use of the system and data.

There is a risk that records may be maintained longer than necessary and paper and fax records may not be properly destroyed. Records are maintained under a NARA approved records schedule. Records are disposed of in accordance with DOI policy and NARA guidelines. Service Technicians complete IMT awareness training, which specifically includes handling and disposal of paper with sensitive information and the proper procedures for handling faxed information. ServiceNow – OR Table Cleaner Program automatically deletes records on a daily basis. Administrators also perform manual deletion and deletion scripts. Deleted data is overwritten by other data as the system is used.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. ServiceNow – OR is provided and hosted by a FedRAMP certified service provider and has met all requirements for information categorized as Moderate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the moderate level. The use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards and National Institute of Standards and

Technology (NIST) guidelines. The cloud service provider is subject to all the Federal legal and policy requirements for safeguarding Federal information and is responsible for preventing unauthorized access to the system and protecting the data contained within the system.

There is a risk that the user information may be inaccurate. Users may enter their own information in the Self-Service page within the system. However, records will be verified and updated by a service technician or help desk each time the individual submits a services request unless they decline to be identified in ServiceNow – OR. Any updates to individual information in AD will be deployed through system-to-system data sharing.

There is a risk that individuals may not receive adequate notice on the use of their PII. Users are provided a Privacy Act statement when logging onto the system website, as well as a notification that their use of the system may be monitored. Notice is also provided through the publication of this PIA and the INTERIOR/DOI-58 SORN.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The full name and AD account information will be used to identify them in the use of the system, their roles, and permissions in the system and to identify any service requests, government assets, and any service history associated with them. Their contact information will be used to communicate with them regarding any radio communications services.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable. This system does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

Service Technicians can view and edit only the information within their service area, which is assigned by their roles.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access is established based on a "need-to-know" and grouped into Roles by the system administrator. The grouping is established based on the role of the person and what data they require based on that role.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved in the design and development of ServiceNow – OR system. DOI leveraged the Foundation Cloud Hosting Service to procure their cloud services from ServiceNow. The applicable Privacy Act Federal Acquisitions Regulations clauses and privacy terms and conditions were included in the contract.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

Account access and denials are monitored via audit logs to include event type (service request), date and time as well as action taken. These logs are reviewed by the system and security administrator.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

User activities captured in ServiceNow – OR include date and time of all actions taken within the system, such as failed login attempts, and service request type. These logs are reviewed by the system and security administrator.

M. What controls will be used to prevent unauthorized monitoring?

Access is established based on a "need-to-know" and grouped into Roles by the system administrator. The grouping is established based on the role of the person and what data they require based on that role. This would apply to monitoring the use of the system.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television

☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe*

ServiceNow – OR is hosted by FedRAMP certified cloud service provider who has met all requirements for Physical Controls for information categorized as Moderate.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*

In addition to the DOI controls listed above, ServiceNow – OR is hosted by FedRAMP certified cloud service provider who has met all requirements for DOI responsible controls for information categorized as Moderate.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. *Describe*

In addition to the DOI controls listed above, ServiceNow – OR is hosted by FedRAMP certified cloud service provider who has met all requirements for DOI responsible controls for an information system categorized as Moderate.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The DOI Telecommunications, Radio Spectrum Section Chief serves as the ServiceNow – OR Information System Owner and the official responsible for oversight and management of security and privacy controls and the protection of the information processed and stored by the ServiceNow – OR system. The Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within the system, in consultation with DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ServiceNow – OR Information System Owner is responsible for oversight and management of the security and privacy controls, and for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner is responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the Departmental Privacy Officer.