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-Radio System
Bureau/Office: Office of the Chief Information Officer
Date: January 10, 2018
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, Mail Stop 7112 MIB, 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 Radio 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 a pilot 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 Radio is a shared service management solution between DOI bureaus and offices and the USDA Forest Service. DOI system administrators will manage the system, and the Forest Service will be 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 of the service to: update their contact information, submit service requests for changes or to report outages or failures and to also view outage notices, self-help, training, and frequently asked questions (FAQ) regarding Field Com. The system will also be used by the service support technicians and managers in the shared service environment to: maintain inventory, configuration and life-cycle of Field Com assets, perform the service requested and to manage the services provided to the customers

C. What is the legal authority?

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

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: 010-000000342; ServiceNow System Security Plan

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			

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)*
DOI-58, Employee Administrative Records, 64 FR 19384, April 20, 1999.

☐ 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.*

Individual information that may be collected includes full name, Active Directory (AD) Alias, work email address, work phone and work cell phone number, office address, organizational code, line of business/mission area, and assigned government assets (property and a vehicle, vessel, or aircraft that has a radio associated with it).

An individual's Personal Cell Phone Number, while not required by ServiceNow-Radio nor required to receive radio support service, may be provided by the customer to expedite service. It could also be inadvertently entered into the ServiceNow-Radio system directly by the customer in their Contact Information "Work Cell Phone Number" field.

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 via interview over the phone or face to face interaction with the

individual. Individuals may enter or update their own information directly in the DOI ServiceNow website after login. Active Directory (AD) is used to authenticate a user's access to ServiceNow and to populate customer contact information in ServiceNow.

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
☒ Other: *Describe*

Individuals may provide information to a service technician who will enter that information into ServiceNow-Radio that is received via an email, interview over the phone, or a face to face interaction. Individuals may enter or update their own information in the DOI ServiceNow-Radio website after login. Active Directory (AD) is used to authenticate a user's access to ServiceNow and to populate customer information in ServiceNow-Radio.

Any Fax received by a service technician may include the individual's name, email address and work phone and Fax number which may be entered into ServiceNow-Radio by the service technician to support future communications with the individual. The individual will be instructed to call the service technician in advance to make sure they are at the fax machine when a document is sent. In addition, the fax machine will be in a secure facility.

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

The information is collected to identify the individual and to provide contact information so service can be coordinated and provided, to determine the individual's eligibility to receive radio support services; authenticate the individual's access the DOI ServiceNow-Radio system; and determine what service technician or service group will provide the support to the individual, and what type of equipment the individual uses and what kind 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.*

The bureaus/offices using the system will see and use the data to identify and contact the customers requesting the service in their assigned support area only. The customers requesting the service will see only the service technician information to support their request. Bureau service managers will see and use the data for the entire bureau to identify and contact the

customers. ServiceNow-Radio system administrators will see and use all customer data to identify and contact the customers for ServiceNow-Radio account management.

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

In a shared service environment, a service technician using the system will see and use the data to identify and contact the customers requesting the service in their assigned support area only and those customers may be from another bureau/office. The customers requesting the service will see only the service technician information to support their request, which may be from another bureau/office. Shared service area managers will see and use the data to identify and contact the customers who may be from another bureau/office but only for those customers in their assigned service area. ServiceNow-Radio system administrators will see and use the all customer data to identify and contact the customers for ServiceNow-Radio account management.

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

In a shared service environment, a service technician, who may be from another Federal agency, using the system will see and use the data to identify and contact the customers requesting the service in their assigned support area only and those customers may be from another Federal agency. The customers requesting the service, who may be from another Federal agency, will see only the service technician information to support their request, and they may be from another Federal agency. Shared service area managers, who may be from another Federal agency, will see and use the data to identify and contact the customers from another Federal agency. ServiceNow-Radio system administrators will only be from DOI, and will see and use all customer data to identify and contact the customers for ServiceNow-Radio account management.

☐ 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, using the system will see and use the data to identify and contact the customers requesting the service in their assigned support area only and those customers may be from within the same bureau, in another bureau and from another Federal agency and may also be a contractor. The customers requesting the service, who may be a contractor, will see only the service technician information to support their request and they may be a contractor within the same bureau, in another bureau or from another Federal agency. Shared service area managers, who may be contractors, will see and use the data to identify and contact the customers which may be contractors within the same bureau, in another bureau and from another Federal agency. ServiceNow-Radio system administrators will not be contractors. ServiceNow-Radio system administrators will see and use all customer data to identify and contact the customers for ServiceNow-Radio 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 "customer" may choose to decline identifying themselves within ServiceNow and receive service manually by contacting their service support technician via phone, email or Fax. The service technician would then document the work within ServiceNow-Radio as "anonymous" and the work will be associated with the equipment and not the individual. Service Technicians, Service Managers and System Administrators must identify themselves to get access to the system, use the system and perform their service work. Service Technicians must identify themselves to get access to the system and to monitor and provide service through the system. Service Managers and System Administrators must identify themselves to get access to the system and perform their duties.

☐ 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.*

This information is requested under 5 U.S.C. 301 and the Consolidated Appropriations Act (Public Law 113-76, Sec. 430) for the purpose of managing Department of the Interior shared support services for radio and field communications. Information will be used to determine eligibility to receive radio support services, authenticate user access, report outage and failure, manage service requests and provide services. Information may be disclosed to agency officials to facilitate compliance with Federal and agency reporting requirements, and to the U.S. Department of Justice, other Federal, State, local or foreign agencies, congressional office, or other organization as described in the routine uses in the DOI-58, DOI Employee Administrative Records, system of records notice, which may be viewed at https://www.doi.gov/privacy/sorn. Providing the information is voluntary, however not providing the requested information may delay service requests.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this privacy impact assessment and the published DOI-58, DOI Employee Administrative Records, system of records notice.

☒ Other: *Describe each applicable format.*

Upon logging into the ServiceNow-Radio system, individuals will be notified that their use of the system may be monitored. Their name and Active Directory 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.

☐ 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: 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 Administrators and Security Administrators are appointed by the system owner in which no more than five will be assigned. They will conduct manual or configure automated report generation on account activities for system security reasons. These reports will be based on account activities and conditions 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 also making 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 customers and service technicians, as well as, service ticket numbers, location, agency and bureau or offices, transaction dates and equipment and assets. These will not be shared.

Customers 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?

1. 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-Radio.
2. The individual may update their information (Self-Service) within ServiceNow-Radio after login.
3. Updates to records provided by changes in Active Directory through System to System data sharing.

B. How will data be checked for completeness?

1. Checklist used when a person contacts the help desk.
2. Check of all mandatory field completion and data entry validation for Self-Service by the individual within the ServiceNow-Radio system.
3. Use the check and balance processes within Active Directory for accuracy of data provided to ServiceNow-Radio from Active Directory.

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

1. Records will be updated each time the person contacts the help desk.
2. Self-Service by the individual within the system will be required after logging-in every 6 months while their account is active.
3. Updates provided by changes in Active Directory 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-Radio 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 individuals 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 384 Department Manual 1 and NARA guidelines. ServiceNow-Radio'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 a minimal privacy risk to due to the limited personal information maintained in the system. 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, ensuring they complete extensive training on IT security, Privacy, and controlled unclassified information, and agree to adhere to the DOI Rules of Behavior.

There is also a risk 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 Procedure (SOP)s where the system security administrator will be reviewing logs looking for inappropriate use of the system and data.

There may be a risk that paper and Fax records may not be properly destroyed. This risk is mitigated by conducting background checks on all system users, service technicians and administrators, and providing extensive training on IT security, Privacy, and controlled unclassified information. The training specifically includes handling and disposal of paper with sensitive information and also the proper procedures for handling Faxed information.

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-Radio 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 policy 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.

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 Active Directory 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.

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 established by 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-Radio system and Federal Acquisitions Regulations (FAR) contract Clause 52.224-1, Privacy Act Notification (APR 1984), and FAR contract Clause 52.239-1, Privacy or Security Safeguards (AUG 1996) are included in the contract agreement.

☐ 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-Radio 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-Radio is provided by and hosted by FedRAMP certified 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-Radio is provided by and hosted by FedRAMP certified service provider who has met all requirements for non-customer 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-Radio is provided by and hosted by FedRAMP certified service provider who has met all requirements for non-customer 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-Radio 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-Radio 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-Radio 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.