Privacy Impact Assessment

Information Technology Infrastructure (ITI) / ServiceNow

Office of the Chief Information Officer

Version 1.0

June 9, 2023

Document Revision History

Date	Version	PIA Name/Description	Author
06/09/2023	1.0	ServiceNow PIA-initial release new template	OCIO Oasis Systems, LLC
06/5/2023	DRAFT	ServiceNow PIA-initial release new template	OCIO Oasis Systems, LLC

Table of Contents

The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Name/System/Subsystem/Service Name: ServiceNow-cloud service in the ITI FISMA boundary.

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform)

The data is stored in the FedRAMP authorized cloud on an encrypted ServiceNow database.

Date Submitted for review/approval: August 4, 2023.

Note: When completing this PIA do not include any information that would raise security concerns or prevent this document from being made publicly available.

1   Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as "project"). Explain the reason the project is being created.

ServiceNow is a component within the ITI Core subsystem. It is used by the NRC Customer Service Center (CSC) staff , who interact with NRC staff and contractors, to handle hardware requests that need to be shipped to a remote or offsite teleworker's personal residence.

Please mark appropriate response below if your project/system will involve the following:

☐	PowerApps	☐	Public Website
☐	Dashboard	☐	Internal Website
☐	SharePoint	☒	None
☐	Other		

1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.

Mark appropriate response.

	Status Options
☒	New system/project ServiceNow replaces the legacy Remedy Change Management Tool
☐	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.*
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☐	Other (explain)

1.3 Points of Contact: (Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.)

	Project Manager	System Owner/Data Owner/ Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Richard Rowe	Gwen Hayden (Acting)	Julie Hughes	N/A	Ben Cantatore	N/A
Office/ Division /Branch	Contractor	OCIO/ITSDOD	OCIO/GEMSD/CSB/IAT	N/A	Contractor	N/A
Telephone	N/A	301-287-0761	301-287-9277	N/A	N/A	N/A

2 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.

Mark with an "X" on all that apply.	Authority	Citation/Reference
☐	**Statute**	
☐	**Executive Order**	
☐	**Federal Regulation**	
☐	**Memorandum of Understanding/Agreement**	
☒	**Other (summarize and provide a copy of relevant portion)**	In order to support NRC staff and contractors for hardware requests, name and home address are necessary to collect from those that are teleworking. Otherwise, they have the option to come to the NRC to pick up equipment.

2.2 Explain how the information will be used under the authority listed above (*i.e., enroll employees in a subsidies program to provide subsidy payment*).

ServiceNow is used by the NRC Customer Service Center (CSC) staff who interact with NRC staff and contractors to handle hardware requests that need to be shipped to remote or offsite teleworkers. The requestor will provide their shipping address to the CSC representative who will then input that information directly into the Notes section of the Request console. If approved by the user's supervisor, the request (ticket) is then routed to the Hardware Asset Manager (NRC) who will then either approve or deny the request based on agency criteria for equipment allowed for offsite workers. If approved, the Request (ticket) will be converted into a Work Order which is then assigned to the Asset and Logistics team (contractors). The asset team will then use this information to ship the approved equipment to the requestor's provided address.

The other way to make the hardware request is through the NRC Service Catalog. The requestor, logs in to the NRC Service Catalog via the NRC Homepage and selects the Hardware, Software, and Custom Solutions tab. The requestor selects the hardware type they need and enters the shipping details directly into the Request ticket. This Request then follows the same path outlined in the previous paragraph, routing to immediate supervisor, then to the Hardware Asset Manager and finally to the Asset and Logistics team for processing and shipment to the requestor's provided address.

If the project collects Social Security numbers, state why this is necessary and how it will be used.

ServiceNow does **not** collect social security numbers.

3   Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
☒	Federal employees
☒	Contractors
☐	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☐	Licensees
☐	**Other**

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table 2023.

Categories of Information			
☒	Name	☐	Resume or curriculum vitae
☐	Date of Birth	☐	Driver's License Number
☐	Country of Birth	☐	License Plate Number
☐	Citizenship	☐	Passport number
☐	Nationality	☐	Relatives Information
☐	Race	☐	Taxpayer Identification Number
☒	Home Address	☐	Credit/Debit Card Number
☐	Social Security number (Truncated or Partial)	☐	Medical/health information
☐	Gender	☐	Alien Registration Number
☐	Ethnicity	☐	Professional/personal references
☐	Spouse Information	☐	Criminal History
☐	Personal e-mail address	☐	Biometric identifiers (facial images, fingerprints, iris scans)
☐	Personal Bank Account Number	☐	Emergency contact e.g., a third party to contact in case of an emergency

Categories of Information			
☐	Personal Mobile Number	☐	Accommodation/disabilities information
☐	Marital Status	☐	**Other**
☐	Children Information		
☐	Mother's Maiden Name		

3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/ databases, response to a background check).

The name and home address of the requestor is either provided over the phone to the CSC representative who then enters the information into the application, or the requestor types their own information into the service request catalog when they make their own request.

3.2 If using a form to collect the information, provide the form number, title and/or a link.

N/A.

3.3 Who provides the information? Is it provided directly from the individual or a third party.

Information is provided over the phone by the requestor or entered through the service catalog by the requestor.

3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.

The information is provided directly from the individual making the request.

3.5 Will PII data be used in a test environment? If so, explain the rationale.

No.

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

The requestor can call the CSC to have them make the correction.

4 Data Security

4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

NRC-badged ServiceNow administrators have access to the data. The CSC Help Desk personnel take the information, and the NRC mailroom staff create the mailing labels.

4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.

N/A.

4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

N/A.

Identify what agreements are in place with the external non-NRC partner or system in the table below.

Agreement Type	
☒	Contract Provide Contract Number: **NG15SD27B/31310022F0026**
☐	License Provide License Information:
☐	Memorandum of Understanding Provide ADAMS ML number for MOU:
☐	Other
☐	None

4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.

The data is stored in an encrypted ServiceNow database in the cloud, and it is only accessible to NRC-badged ServiceNow administrators.

4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).

The data is encrypted and so is the communication using FIPS validated algorithms.

4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).

The data is stored in the ServiceNow FedRAMP authorized cloud.

4.7 Explain if the project can be accessed or operated at more than one location.

N/A.

4.8 Can the project be accessed by a contractor? If so, do they possess an NRC badge?

Yes. The contractors involved in processing PII for ServiceNow are NRC-badged.

4.9 Explain the auditing measures and technical safeguards in place to prevent misuse of data.

Data is stored in an encrypted ServiceNow database in the cloud and can only be accessed by NRC-approved ServiceNow administrators with an NRC privileged account.

4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.

N/A.

4.11 Define which FISMA boundary this project is part of.

ServiceNow is part of the ITI Core Services subsystem boundary.

4.12 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
☐	Unknown
☐	No *If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.*
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality-Moderate Integrity- Moderate Availability- Moderate

4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact EA Service Desk to get the EA/Inventory number.

ITI EA# 20090005.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
☐	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)**
☐	**List the identifiers that will be used to retrieve the information on the individual.**
☒	**No, the PII is not retrieved by a personal identifier.** **If no, explain how the data is retrieved from the project.** It is retrieved by the ticket #.

5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.*

Mark the appropriate response in the table below.

	Response
☐	*Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)* *Provide the SORN name, number, (List all SORNs that apply):*
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☒	**No, this system is not a system of records and a SORN is not applicable.**

5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided?

A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.

Mark the appropriate response.

	Options
☐	**Privacy Act Statement**
☒	**Not Applicable**
☐	**Unknown**

5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?

To receive the hardware, the name and home address of the requestor must be provided.

6   Records and Information Management-Retention and Disposal

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are **Temporary** (eligible at some point for destruction/deletion because they no longer have business value) or **Permanent** (eligible at some point to be transferred to the National Archives because of historical or evidential significance). Records/data and information with historical value, identified as having a "permanent" disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a "temporary" disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for NARA's Universal Electronic Records Management (ERM) requirements, and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at **ITIMPolicy.Resource@nrc.gov** for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

6.1 Does this project map to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules?

☐	NUREG-0910, "NRC Comprehensive Records Disposition Schedule
☒	NARA's General Records Schedules
☐	Unscheduled

6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	ServiceNow
Records Retention Schedule Number(s)	GRS 5.8 item 010 – Technical and administrative help desk operational records. GRS 3.1 item 020 – Information technology operations and maintenance records.
Approved Disposition Instructions	GRS 5.8 item 010. Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. GRS 3.1 item 020. Temporary. Destroy 3 years

	after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	N/A
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	N/A
Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	N/A

Note: Information in *Section 6, Records and Information Management-Retention and Disposal,* does not need to be fully resolved for final approval of the privacy impact assessment.

7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number"—before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

No.

7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?

No.

7.3 Is the collection of information required by a rule of general applicability?

No.

Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: https://intranet.nrc.gov/ocio/33456.

STOP HERE - The remaining pages will be completed by the Privacy Officer, Records Management, and Information Collections Team.

8 Privacy Act Determination

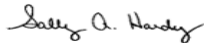**Project/System Name:** ServiceNow-cloud service in the ITI FISMA boundary.

Submitting Office: IT Services Development & Operations Division (SDOD).

Privacy Officer Review

	Review Results	Action Items
☐	This project/system **does not contain PII.**	**No further action** is necessary for Privacy.
☒	This project/system **does contain PII**; the Privacy Act does **NOT** apply, since information is NOT retrieved by a personal identifier.	**Must be protected with restricted access** to those with a valid need-to-know.
☐	This project/system **does contain PII**; the **Privacy Act does apply**.	**SORN is required-** Information is **retrieved** by a personal identifier**.**

Comments:

Since the agency practice is to retrieve by work order number, a system of records is not needed. If this practice changes the PIA would need to be updated and reevaluated.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 08/30/23	Privacy Officer

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
☒	No OMB clearance is needed.
☐	OMB clearance is needed.
☐	Currently has OMB Clearance. Clearance No._____

Comments:

The information being collected meets the exemption criteria in 5 CFR 1320.3(h)(1).

Reviewer's Name	Title
[signature] Signed by Cullison, David on 08/14/23	Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

	Review Results
☐	No record schedule required.
☐	Additional information is needed to complete assessment.
☐	Needs to be scheduled.
☒	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
[signature] Signed by Dove, Marna on 08/23/23	Sr. Program Analyst, Electronic Records Manager

11 Branch Chief Review and Concurrence

	Review Results
☒	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☐	This project/system **does** collect, maintain, or disseminate information in identifiable form.

I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Harris, Kathryn
on 09/06/23

_____

Chief
Cyber Security Branch
Governance and Enterprise Management
    Services Division
Office of the Chief Information Officer

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System:

ServiceNow-cloud service in the ITI FISMA boundary.

Date CSB received PIA for review:	**Date CSB completed PIA review:**
August 4, 2023	August 23, 2023

Action Items/Concerns:

Since the agency practice is to retrieve by work order number, a system of records is not needed. If this practice changes the PIA would need to be updated and reevaluated.

Copies of this PIA will be provided to:

Ledetria Beaudoin
Director (Acting)
IT Services Development and Operations Division
Office of the Chief Information Officer

Garo Nalabandian
Chief Information Security Officer (CISO)
Office of the Chief Information Officer