Privacy Impact Assessment Process
U.S. Nuclear Regulatory Commission (NRC)
Privacy Program

Office of the Chief Information Officer (OCIO)

Version 2.1
March 01, 2024

Document Revision History

Date	Version	Description	Author
March 01, 2024	v2.1	Annual review-minor edits	NRC Privacy Officer Oasis Systems, LLC
February 28, 2024	DRAFT v2.1	Annual review-minor edits	NRC Privacy Officer Oasis Systems, LLC
March 29, 2023	2.0	Major revisions based on new processes and requirements	NRC Privacy Officer Oasis Systems, LLC
March 24, 2023	DRAFT of 2.0	Major revisions based on new processes and requirements	NRC Privacy Officer Oasis Systems, LLC
February 2014	1.0	Initial Release	NRC Privacy Officer

Table of Contents

1 Overview

Federal laws recognize the ever-increasing amount of information stored in government systems and the speed with which computers can process and transfer data. Section 208 of the E-Government Act of 2002 (E-Gov Act), along with Office of Management and Budget (OMB) Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, require agencies to conduct a privacy impact assessment (PIA) before undertaking certain activities involving IT systems or electronic information collection.

The PIA analyzes how personally identifiable information (PII) is collected, stored, protected, shared, and maintained. The PIA demonstrates that data/system owners have consciously incorporated privacy protections throughout the development of a system.

The PIA is also designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act. The Privacy Act balances the government's need to maintain information about individuals with the right of individuals to be protected against unwarranted invasion of their privacy. Part of the PIA requirement is to identify the legal authority and/or agreement to collect the PII (i.e., statute/law, Federal regulation, Executive order).

In addition, the E-Government Act of 2002 requires an agency to make PIAs publicly available, except when an agency, in its discretion, determines publication of the PIA would raise security concerns or reveal classified (i.e., national security) information or sensitive information (i.e., potentially damaging to a national interest, law enforcement effort, or competitive business interest). The PIA helps the public understand what information the agency is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be securely stored.

Another purpose of the NRC's PIA review process is to ensure that data collections will adhere to the Paperwork Reduction Act (PRA), if applicable, and will comply with Federal requirements for managing the lifecycle of agency records.

At the NRC, the PIA is created along with the Security Categorization Report by the system owner / information owner / data steward, and/or information systems security manager (ISSM) during Step 2: Categorize, of the National Institute of Standards and Technology and (NIST) Risk Management Framework. This effort is conducted in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business functions and/or risk management responsibilities).

2 When Does a PIA Need to be Completed

A PIA must be completed before the agency:

- Develops or procures IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public, or makes substantial changes to an existing IT system that manages information in identifiable form.

- Initiates a new electronic collection of information in identifiable form for 10 or more members of the public consistent with the PRA, which governs how Federal agencies collect information from the public.

2.1 What is PII

PII is information that can be used to identify or contact a person uniquely and reliably or can be tracked back to a specific individual. That is, PII is a person's name, in combination with any of the following information: relatives' names, postal address, email address, home or cellular telephone number, personal characteristics, Social Security number (SSN), date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or other information that would make the individual's personal identity easily traceable and could make it usable for unauthorized purposes.

PII may include direct identifiers (i.e., passport information) that can identify a person uniquely, or quasi-identifiers (i.e., race) that can be combined with other quasi-identifiers (i.e., date of birth) to successfully identify an individual. PII can be sensitive and non-sensitive.

- **Sensitive PII** if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII are sensitive as stand-alone data elements, for example, an individual's SSN, driver's license number, or State identification number.

- **Non-sensitive PII** includes information that could be in a public record, such as an individual's birthday or phone number. It cannot directly identify the individual by itself, but it can identify the individual when used in combination with other personal linkable information.

A comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table 2023.

Note: Consistent with the Privacy Act and NRC PII policies, PII is to be collected and maintained only where necessary for proper performance of the agency's mission/functions. In response to OMB guidance, the NRC has also developed and implemented a plan to eliminate the unnecessary collection and use of SSNs.

It is important to note that not all information that is sensitive for personal privacy reasons will necessarily qualify as PII, because not all sensitive personal privacy information is useful for identifying an individual. Conversely, information qualifies as PII based on its usefulness in identifying an individual, not based on whether the individual considers the information to be, or treats the information as, sensitive, or private.

Personal identity is distinct from an individual's professional identity; that is, an employee's name, work title, work telephone number, work address (official work location), and work email address are not considered to be PII.

2.2 PIA Submittal Process

A PIA is completed during the early stages of system development and the system owner/information owner, data steward, and/or ISSM completes the assessment. Part of the

privacy assessment is to document the data elements that will be collected, the authority for collecting the information, how the data will be used, who will use the data, and how long it should be kept for business purposes. Those involved may need to coordinate certain responses with the NRC's privacy office, records management, and information collections subject matter experts.

Table 2.2-1: Submittal Process

Step	Responsible party	Description
1.	System owner / information owner / data steward and/or the ISSM	Complete the PIA: PIA template is available in ADAMS at ML050460335 Save the template and rename it to the following format: <system name_privacy_impact_assessment.doc> Provide responses to all questions in the PIA. Consult with the privacy office, records management, and information collection subject matter experts if there are any questions.
2.	System Owner / information owner / data steward and/or the ISSM	Submit completed PIA and NRC Form 665, *ADAMS Document Submissions*, to OCIO for review and approval to the email address below: Privacy.Resource@nrc.gov Completing the NRC Form 665 determines if the PIA can be designated as publicly available or non-public in ADAMS. All PIAs must be posted on the agency's website, unless doing so would raise security concerns or reveal classified or sensitive information.
3.	Office of the Chief Information Officer (OCIO) designee	Upon receipt of the PIA, the privacy team reviews the document for completeness. If there are any residual questions, the sponsoring office will be notified for further clarification.
4.	OCIO / Cybersecurity and Information Security Division (CISD) privacy office, and Data Information Management and Enterprise Governance (DIME) records management, and information collection subject matter experts	Once the PIA has been confirmed for completeness, the administrative assistant places the document into e-concurrence for review from the following groups within OCIO to include: • **Privacy Office**-determining applicability of the Privacy Act and any privacy risks to the NRC • **Information Collections**-reviewing the Paperwork Reduction Act for information collection requirements • **Records Management**-reviewing the Federal Records Act for records management requirements Once reviewed by all three groups, the PIA is provided to the OCIO/CISO.
5.	OCIO CISO	The CISO reviews the PIA and grants final approval, certifying that the office has prepared an adequate PIA for the project/system.

Table 2.2-1: Submittal Process

Step	Responsible party	Description
6.	OCIO Administrative Assistant	The administrative assistant finalizes the document by declaring it in ADAMS and closing it out through the e-concurrence process. A distribution notice will include the following: • Sponsoring office (program manager and system owner, ISSM) • Director SDOD • CISO
7.	Privacy Officer	The NRC Privacy Officer provides a link to the PIA document in the Public ADAMS on the NRC Privacy Program Web page available to the public.

2.3 When does a PIA need to be updated

The PIA is a living document that needs to be reviewed and updated as the program and/or system changes, not just when the program or system is initially deployed. PIAs must be reviewed annually and updated if necessary to ensure that they are accurate and up to date. If no changes are required, the responsible party must send an email to the NRC Privacy Officer certifying the PIA has been reviewed and that no changes are required.

For PIAs requiring updates, the responsible party will need to complete a new PIA template addressing the changes and send it back through the approval process described above in Table 2.2.1.

Agencies must update their PIAs to reflect changes in information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form. Some examples of system changes are provided in the table below:

Table 2.3-1: System Changes

System Changes	Description
System Management Changes	New uses of an existing IT system, including application of new technologies, any change in how information in identifiable form is managed in the system
Anonymous to Non-Anonymous	Functions applied to an existing information collection from anonymous information into information in identifiable form
Conversions	Converting paper-based records to electronic systems
Significant Merging	Agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated
New Public Access	User-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public
Commercial Sources	Agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources
Alteration in Character of Data	New information in identifiable form, such as health or financial information, added to a data collection that raises the risks to personal privacy

2.4 Federal PIA Exemptions

In accordance with Federal guidance, certain types of IT systems may be exempt from the PIA requirement. These include any system where information relates to internal government operations or has been previously assessed under an evaluation like a PIA. A PIA is also not required:

- For government-run Websites, IT systems, or collections of information that **do not** collect or maintain information in identifiable form about members of the public, government employees, contractors, or consultants
- For government-run public Websites where the user is given the option of contacting the site operator for the limited purpose of asking questions or providing comments
- For national security systems
- When all elements of a PIA are addressed in a data matching or comparison agreement governed by the computer matching provisions of the Privacy Act
- When all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act
- When developing IT systems or collecting non-identifiable information for a discrete purpose that does not involve matching with or retrieval from other databases that generate individual or business identifiable information

2.4.1 NRC Exemptions

The NRC's external website contains a notice stating that any comments submitted to the NRC, including PII contained in comments, as well as documents submitted in public NRC adjudicatory proceedings, will generally be available to the public. Because submitters are advised not to include PII in their submittals, it is presumed that submitters who do include such information have no objection to its public release. Thus, it is not necessary to remove home addresses, home phone numbers, or home email addresses from adjudicatory filings, documents associated with agency rulemakings, or correspondence received from the public on regulatory matters.

2.5 PIA Requirements Related to the Privacy Act Systems of Records Notice (SORN)

The Privacy Act of 1974 prohibits the Federal Government from disclosing information about an individual without the individual's consent if the information is stored in a "system of records" — that is, a collection of records containing information about individuals, where the information is retrieved by the individual's name or by another identifier assigned to the individual. It balances the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy. It requires agencies to publish a SORN in the Federal Register for the public to view. The SORN describes the categories of records on individuals that the agency collects, uses, maintains, and retrieves by the name of the individual or by some identifying number, symbol, or another identifier assigned to the

individual. The Privacy Act prohibits the disclosure of information about individuals from a system of records absent the written consent of the subject individual unless the disclosure is pursuant to one of 12 statutory exceptions. The Privacy Act also provides individuals with a means by which to seek access to, and amendment of, their records and sets forth various agency record-keeping requirements.

If personal information is collected, but never retrieved by the unique identifier, it is **not** a system of records and a SORN is **not required**.

3 Privacy Threshold Analysis

If the sponsoring office (program manager/system owner and/or ISSM) anticipates that an IT system or project will **not** collect, maintain, or disseminate information about individuals, then a privacy threshold analysis (PTA) should be completed to document that a review of the data elements in the system or project has been performed and to confirm that there will be no information about an individual in the system or project.

PTAs are used to confirm that a system or project does not contain PII, and a PIA is not required, whether a SORN is required, and if any other privacy requirements apply to the system or project. PTAs should be submitted to the NRC Privacy Officer for review and approval.

The PTA submittal process is the same as the PIA submittal process as defined above in Table 2.2.1. The PTA template can be found in ADAMS ML091970114.

4 Further Assistance

For privacy questions: contact the NRC's Privacy Officer for assistance.

- Additional privacy guidance can be found on the NRC's internal Privacy Act Program Web page at:

  https://nuclepedia.usalearning.gov/index.php/Privacy_Act_Program

  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://usnrc.sharepoint.com/teams/Information-Collections/SitePages/Information-Collections-Guidance.aspx

- Records retention and disposition questions: contact the Agency Records Officer. Additional records retention and disposal information can be found at:

  https://usnrc.sharepoint.com/sites/information-records-management/SitePages/The-Lifecycle-of-NRC-Records.aspx