Privacy Program Plan

U.S. Nuclear Regulatory Commission (NRC) Privacy Program

Office of the Chief Information Officer (OCIO)

Version 2.1

09/25/2023

Document Revision History

Date	Version	Description	Author
09/25/2023	2.1	Added metrics and expanded privacy risk management framework	NRC Privacy Office
05/22/2023	2.0	Major revisions based on new processes and requirements	NRC Privacy Office Oasis Systems, LLC
05/17/2023	DRAFT of 2.0	Major revisions based on new processes and requirements	NRC Privacy Office Oasis Systems, LLC
09/20/2020	1.0	Initial Release	NRC Privacy Office

Table of Contents

1 Introduction 1
1.1 Purpose of the NRC Privacy Program Plan 1
1.2 Overview of the NRC Privacy Program and Organization 1

2 SAOP Roles and Responsibilities 2
2.1 Privacy Workforce Management 4
2.2 Budget and Acquisition 4

3 Strategic Goals and Objectives for the NRC Privacy Program 5

4 Fair Information Practice Principles 7

5 Privacy Risk Management Framework 8

6 Privacy Control Requirements 8
6.1 NRC Privacy Continuous Monitoring Program 9

7 Privacy Impact Assessment 9

8 Privacy Threshold Analysis 10

9 System of Records Notices (SORNS) 10
9.1 Privacy Act Regulations 11
9.2 Privacy Act Statements 11

10 Overview of Handling and Protecting Personally Identifiable Information 12
10.1 Minimizing the Collection of PII 12
10.2 Handling and Transmitting PII 12
10.3 Contractors and Third Parties 13

11 Breach Response and Management 14
11.1 Privacy Program’s Role in Incident Response Process 15

12 Awareness and Training 15
12.1 New Employee Orientation Training 15
12.2 Role-Based Training 16

13 Privacy Reporting 16

14 Conclusion 16

1 Introduction

1.1 Purpose of the NRC Privacy Program Plan

The U.S. Nuclear Regulatory Commission (NRC) Privacy Program Plan is required by the Office of Management and Budget (OMB) Circular A-130 Managing Information as a Strategic Resource. The Privacy Program Plan includes:

- a description of the structure and mission of the NRC's Privacy Program;
- the resources dedicated to the NRC's Privacy Program;
- the role of the Senior Agency Official for Privacy (SAOP);
- the strategic goals and objectives of the Privacy Program;
- the Program Management controls in place to meet applicable Federal privacy requirements and manage privacy risks; and
- additional information deemed important by the NRC's SAOP to provide an overview of the NRC's Privacy Program requirements.

1.2 Overview of the NRC Privacy Program and Organization

The NRC's Privacy Program is under the purview of the Office of the Chief Information Officer (OCIO). The Privacy Program, within OCIO, develops and executes strategies to ensure that privacy is protected for all who entrust their personal information to the NRC, including the NRC employees, contractors, and the public, while promoting the integrity and usability of NRC's data—one of NRC's most valuable strategic assets. The Privacy Program is led by the NRC's Deputy Director of OCIO, who has also been formally designated as the NRC's SAOP pursuant to OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy.

The mission of the NRC Privacy Program is to preserve and enhance privacy protections for all individuals who entrust their personal information to the NRC by embedding and enforcing privacy protections throughout all of NRC's activities.

The Privacy Program implements requirements in the Privacy Act of 1974, as amended; the E-Government Act of 2002; and the Federal Information Security Modernization Act of 2014 (FISMA), as well as policy directives and best practices issued in furtherance of those Acts.

When the NRC officially transitions to implementing a Controlled Unclassified Information program at the agency, the NRC Privacy Program will implement requirements in 32 Code of Federal Regulations (CFR) Part 2002, "Controlled Unclassified Information," where current laws, regulations, and government-wide policies require safeguarding and disseminating controls for personally identifiable information (PII) and Privacy Act information. The requirements in 32 CFR Part 2002 do not override requirements found in laws, regulations, or government-wide policies for the protection of privacy information, such as requirements under the Privacy Act or requirements for PII protection found in government-wide policies issued by the Office of Management and Budget. When determining whether certain information must be protected under the Privacy Act, or whether the Privacy Act allows release of the information to an

individual, the decision must be based on the content of the information and the Privacy Act's criteria, regardless of whether the information is designated or marked as Controlled Unclassified Information (CUI).

The NRC Privacy Program also adheres to the policy framework embodied in the Fair Information Practice Principles (FIPPs) to ensure that individual privacy is protected throughout the collection, maintenance, use, and dissemination of all PII maintained by the NRC.

The NRC Privacy Program carries out the following core functions:

- Develops and administers NRC’s privacy policies and procedures
- Provides privacy awareness training to NRC personnel and contractors
- Assesses all new or proposed programs, systems, technologies, and business processes for privacy risks and provides recommendations to strengthen privacy protections
- Collaborates with NRC’s Chief Information Security Officer (CISO), Cybersecurity Branch (CSB) and Network and Security Operations Branch (NSOB) to implement and operationalize policies to secure the confidentiality, integrity, and availability of the NRC’s information and information systems
- Maintains a breach response plan to ensure that all incidents involving PII are properly reported, investigated, and mitigated, as appropriate
- Maintains updated privacy artifacts in compliance with legal requirements (e.g., System of Records Notices, Privacy Impact Assessments, Privacy Threshold Analyses, and Privacy Act Notices)

2 SAOP Roles and Responsibilities

The SAOP is designated by the NRC Chairman. The SAOP has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency’s development and evaluation of legislative, regulatory, and other policy proposals.

The SAOP is a voting member of the Human Capital Council (HCC), established by the NRC Executive Director for Operations (EDO) in collaboration with the Office of the Chief Human Capital Officer (OCHCO). The purpose of the HCC is to provide enterprise governance for agency-wide human capital goals, strategies, initiatives, and processes, ensuring that human capital programs and policies effectively integrate and align with the agency’s mission. This includes, but is not limited to, workforce planning, recruiting, hiring, benefits administration, performance management, training and development, and organizational development. The HCC focuses its attention at the strategic level and on those high-level operational issues that have significant impact on the agency’s workforce and resources.

The SAOP is also an advisory member of the Information Technology/Information Management Portfolio Executive Council (IPEC). This council was established to determine strategic direction for NRC Information Technology/Information Management (IT/IM). IPEC manages its IT/IM portfolio by setting current fiscal year priorities and determining the funding of IT/IM investments

that effectively integrate into the IT/IM portfolio. IPEC members provide valuable input and advice on the many aspects of the NRC's mission and business needs. The SAOP works in partnership with program managers to ensure the implementation of information privacy protections and serves as senior advisor to the IPEC for information privacy protections and compliance with the Freedom of Information Act and the Privacy Act of 1974.

As a member in both councils, the SAOP provides expert advice, counsel, and recommendations on agenda items under discussion, and makes presentations on items needing a decision, as appropriate. Both councils meet quarterly or as often as needed to accomplish their purposes.

The SAOP's responsibilities include, but are not limited to:

- Serving in a central policy-making role in the NRC's development and evaluation of legislative, regulatory, and other policy proposals that have privacy implications - In this role, the SAOP ensures that the agency considers and addresses the privacy implications of all agency regulations and policies and leads the agency's evaluation of the privacy implications of legislative proposals, congressional testimony, and other materials pursuant to OMB Circular No. A-19.7

- Serving in a central role in overseeing, coordinating, and facilitating the NRC's privacy compliance efforts - In this role, the SAOP ensures that the NRC complies with applicable privacy requirements in law, regulation, and policy. Relevant authorities include, but are not limited to, the Privacy Act of 1974; the Paperwork Reduction Act of 1995; the E-Government Act of 2002; the Health Insurance Portability and Accountability Act of 1996; OMB Circular A-130; Privacy Act Implementation: Guidelines and Responsibilities; OMB Circular A-108; OMB's Final Guidance Interpreting the Provisions of Public Law 100-503; the Computer Matching and Privacy Protection Act of 1988; and OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

- Serving as the NRC's senior policy authority on matters relating to the public disclosure of information, advising on privacy issues related to informed consent, disclosure risks, and data sharing

- Coordinating with the NRC's CUI Senior Agency Official to ensure that personally identifiable information is appropriately safeguarded and disseminated in accordance with 32 CFR Part 2002 and the NRC's CUI policy when implemented

- Communicating the NRC's privacy vision, principles, and policies internally and externally

- Advocating strategies for data and information collection and dissemination, to ensure the NRC's privacy policies and principles are reflected in all operations

- Managing privacy risks associated with NRC activities, which involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems

- Actively involved in the hiring, training, and professional development needs of the NRC with respect to privacy

- Ensuring that NRC employees have the appropriate training and education concerning privacy laws, regulations, policies, and procedures
- Working with NRC staff to ensure that vendors/contractors, with access to PII, who engage in business with the NRC, abide by Federal privacy requirements
- Overseeing NRC's process for reviewing and approving Privacy Impact Assessments (PIA) to ensure compliance with the E-Government Act
- Coordinating with the NRC's CISO to ensure that the FISMA authorization and accreditation process for new and existing systems appropriately addresses privacy-related risks
- Partnering with the CISO to ensure all aspects of the NRC Privacy Program are incorporated into NRC's enterprise infrastructure, information technology (IT), and IT security program
- Coordinating with the Office of the General Counsel on privacy laws, regulations, policies, and procedures
- Reviewing and approving the Breach Notification Plan
- Assessing the overall effectiveness of the Privacy Program

In accordance with OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy, the NRC SAOP has delegated the daily operations of NRC's Privacy Program to the Privacy Officer and the CISO. For additional details on NRC's organizational responsibilities and delegations of authority, see Management Directive 3.2, "Privacy Act."

2.1 Privacy Workforce Management

The NRC SAOP collaborates with members of NRC's Executive Leadership to maintain and enhance the workforce planning process, maintain workforce skills, recruit and retain privacy professionals, and develop a set of competency requirements for staff in the NRC's Privacy Program. NRC's SAOP facilitates and oversees training for NRC's workforce to ensure NRC personnel have the appropriate knowledge and skill to embed privacy into their respective business processes. Finally, NRC's SAOP ensures that managers take advantage of flexible hiring authorities for specialized positions where necessary.

2.2 Budget and Acquisition

The SAOP ensures that the agency identifies and plans for the resources needed to implement its Privacy Program each year. The SAOP collaborates with members of NRC's Executive Leadership, to review IT capital investment plans and budgetary requests to ensure that privacy requirements and associated privacy controls are identified and collaborates with key stakeholders to ensure privacy risks are addressed to the maximum extent possible.

3 Strategic Goals and Objectives for the NRC Privacy Program

GOAL 1

- Maintain compliance with Federal privacy laws, regulations, and best practices

  Adhering to privacy laws and implementing best practices is critical to the success of both the Privacy Program as well as the agency.

  Objective 1.1 – Increase accountability and transparency by enhancing NRC's foundational privacy documents to comply with the Privacy Act, the E-Government Act of 2002, OMB requirements, and best practices. These documents include NRC's System of Records Notices (SORN), Privacy Threshold Analyses (PTAs), and PIAs.

  Objective 1.2 – Provide sound and consistent guidance to NRC's offices concerning the implementation of Federal privacy laws, regulations, and other best practices, supported by legal advice from OGC.

  Objective 1.3 – Review, assess, and advise business owners throughout the NRC about NRC programs, projects, information sharing arrangements, systems, and other initiatives to comply with FIPPs. This includes limiting the collection, maintenance, use, and dissemination of PII whenever possible.

  Objective 1.4 – Ensure that privacy-related complaints and incidents at the NRC are reported systematically, efficiently processed, and appropriately mitigated in accordance with legal requirements and NRC policies and procedures.

GOAL 2

- Foster a culture of privacy and demonstrate leadership through policy and strategic partnership

  The Privacy Program's core mission is to preserve and enhance privacy protections for all individuals who entrust their personal information to the agency, and fostering a culture of privacy at the agency is a necessary component for achieving this mission. Consistent with the FIPPs, it is the NRC's policy to collect PII only as necessary to carry out its mission and to use that information only in ways that are compatible with the stated purpose for which it was originally collected.

  Objective 2.1 – Provide guidance and issue policies related to privacy by partnering with leaders in each of NRC's offices to embed and enhance privacy protections throughout the life cycle of NRC initiatives, programs, projects, and systems.

  Objective 2.2 – Leverage the expertise of the Federal Privacy Council, as well as experts from professional privacy associations, to foster dialogue and learn about emerging issues.

  Objective 2.3 – Provide guidance by leveraging the expertise of the Privacy Officer and the CISO.

GOAL 3

- Provide outreach, training, and education to promote and enhance privacy, agency-wide

  The NRC Privacy Program ensures that all NRC personnel have a baseline understanding of Federal privacy requirements, by providing training for new employees and annually thereafter. NRC's Privacy Program also develops and provides targeted, role-based training to employees with specialized roles on a periodic basis.

  Objective 3.1 – Ensure consistent application of privacy requirements across the agency.

  Objective 3.2 – Develop and deliver targeted, role-based training for employees with specialized roles and other key stakeholders across the agency.

  Objective 3.3 – Educate NRC personnel about the importance of adhering to the FIPPs and partner with key stakeholders to embed the FIPPs into NRC's business practices.

GOAL 4

- Develop and maintain top privacy professionals in the Federal Government

  The NRC Privacy Program continues to mature. Attracting and retaining specialized talent is critical to the Privacy Program's continued success. Providing support, opportunities for professional growth and development, and maintaining a workplace environment in which they are valued, are all crucial to recruiting and maintaining a high-performing workforce.

  Objective 4.1 – Support employee development and emphasize the importance of training and professional development in performance planning.

  Objective 4.2 – Reward exceptional employee performance and recognize individual contributions which enhance the Privacy Program's mission.

GOAL 5

- Develop metrics to evaluate the effectiveness of the privacy program and ensuring compliance with privacy laws and regulations,

  Metrics are established and approved by the SAOP and reviewed annually. They are adjusted accordingly based on program needs and any new requirements. Privacy metrics are available at: Privacy Program Metrics.xlsx

  Objective 5.1 – Identify areas of improvement based on operational experience and external requirements.

  Objective 5.2 – Review metrics annually to determine if any modifications are necessary.

  Objective 5.3 – Closely monitor and evaluate metric results and adjust the privacy program as needed.

4 Fair Information Practice Principles

The NRC Privacy Program adheres to the Fair Information Practice Principles (FIPPs). The FIPPs are a collection of widely accepted principles that agencies use when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs are not requirements; rather, they are principles that should be applied by each agency according to the agency's particular mission and Privacy Program requirements.

The agency has incorporated the following principles into several agency-wide processes to evaluate information systems, processes, programs, and activities which affect individual privacy. The FIPPs include:

- **Access and Amendment** – Individuals are provided with appropriate access to PII and the opportunity to correct or amend PII.
- **Accountability** – The NRC monitors, audits, and documents compliance with the FIPPs through several processes, including, but not limited to, the PTA/PIA and SORN processes. Additionally, NRC has incorporated key privacy requirements into the agency's Rules of Behavior, which are enforced through a process, which can include discipline, to strengthen accountability.
- **Authority** – The NRC limits the PII which it creates, collects, uses, processes, stores, maintains, disseminates, and discloses to what is legally authorized. NRC ensures that the appropriate authorities are cited in any appropriate Privacy Act notices.
- **Minimization** – The NRC creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII only when directly relevant and necessary to accomplish a legally authorized purpose. The PII is maintained for only as long as is necessary to accomplish the purpose and/or according to applicable record retention schedules.
- **Quality and Integrity** – The NRC creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII with the accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- **Individual Participation** – Individuals that are involved in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Individuals may address concerns or complaints to NRC's SAOP using NRC form 974.
- **Purpose Specification and Use Limitation** – The NRC provides notice of the specific purposes for which PII is collected and only uses, processes, stores, maintains, disseminates, and discloses PII for the purposes that are explained in the notice and compatible with the purpose for which the PII was collected, or that are otherwise legally authorized.
- **Security** – The NRC ensures that administrative, technical, and physical safeguards are established to protect PII, commensurate with the risk and magnitude of the harm which would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
- **Transparency** – The NRC provides clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

5 Privacy Risk Management Framework

The NRC adheres to the process described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Risk Management Framework, to incorporate information security and privacy risk management activities into the system development life cycle. The SAOP collaborates with NRC's CISO to:

- analyze data elements used by each of the NRC's information systems, including the information processed, maintained, and transmitted by each system, based on an impact analysis compliant with NIST FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- overseeing NRC's process for reviewing and approving PIAs to ensure compliance with the E-Government Act.
- reviews privacy control assessments for possible weaknesses and risk determinations.
    - discuss any privacy risks identified to determine best course of action with appropriate stakeholders and require CIO/SAOP approval of mitigation plans and any risks accepted.
    - develop, monitor, and track mitigation efforts to ensure privacy risks are addressed.
    - track and manage continuous monitoring activities as required in NIST SP 800-53R5 to maintain ongoing awareness of any weaknesses/risk.

6 Privacy Control Requirements

The NRC Privacy Program complies with NIST 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations which addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that NRC IT products and systems that rely on those products are trustworthy.

In addition, FISMA, the Privacy Act, and OMB A-130 require Federal agencies to develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of Federal information processed, stored, and transmitted by Federal information systems and to protect individual privacy. The NRC Privacy Program provides the solutions for the following Program Management Controls:

- PM-13 Security and Privacy Workforce
- PM-14-Testing, Training, and Monitoring
- PM-15-Security and Privacy Groups and Associations
- PM-18-Privacy Program Plan
- PM-19-Privacy Program Leadership Role

- PM-20-Dissmenination of Privacy Program Information
- PM-20 (1)-Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services
- PM-21-Accounting of Disclosures
- PM-22-Personally Identifiable Information Quality Management
- PM-23-Data Governance Body
- PM-24-Data Integrity Board
- PM-25-Minimization of Personally Identifiable Information Used in Testing, Training, and Research
- PM-26-Complaint Management
- PM-27-Privacy Reporting

For more information on how these Program Management controls are implemented, contact the NRC Privacy Office at Privacy.Resource@NRC.gov.

6.1 NRC Privacy Continuous Monitoring Program

The NRC has developed a Privacy Continuous Monitoring Program (PCM) that maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks and monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information. The NRC PCM includes the following activities:

- PIAs and PTAs are reviewed annually.
- SORNs are reviewed biennially.
- Privacy control assessments are conducted annually for systems that contain PII.
- Annual PII and Privacy Act training is provided to all NRC employees and contractors.

7 Privacy Impact Assessment

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, requires agencies to conduct a PIA.

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 existing IT 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 Paperwork Reduction Act (PRA), which governs how Federal agencies collect information from the public

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

Part of the NRC's PIA review process is to determine if data collections are adhering to the PRA, if applicable, and complying with Federal requirements for managing the lifecycle of agency records.

Pursuant to NRC's PTA/PIA Policy and Procedures, if the Privacy Officer determines a PIA is required, the sponsoring office, Information System Security Officer and System Owner complete the PIA. The Privacy Officer, Information Collections Officer and Records Officer then review the PIA to ensure it is accurate and complete and analyze whether privacy risks are mitigated to an acceptable level. Once completed, the Cybersecurity Branch Chief signs the PIA document and a copy is provided to the CISO and Director of IT Services Development & Operation Division. Also, to comply with FISMA reporting, the NRC requires PIA's and PTA's to be reviewed annually. For additional details, see the Privacy Impact Assessment Process document located at https://intranet.nrc.gov/ocio/catalog/30684. The PIA template is available in ADAMS at ML050460335.

At the NRC, the PIA is created along with the Security Categorization Report by the system owner/information owner/steward and/or Information System Security Officer (ISSO) during step 2, Categorize, of the NIST Risk Management Framework. This effort is conducted in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business function and/or risk management responsibilities).

8 Privacy Threshold Analysis

If the sponsoring office (program manager/system owner and/or ISSO) anticipates that an IT system or project will not collect, maintain, or disseminate information about individuals, then a 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 template can be found in ADAMS ML091970114.

9 System of Records Notices (SORNS)

A system of records is 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 identifying number, symbol, or other identifier assigned to the individual, including, but not limited to, the individual's name, Social Security number (SSN), or a symbol or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register. This notice is generally referred to as a SORN.

The NRC adheres to the Privacy Act for publishing the SORN in the Federal Register, following requirements identified in OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act.

All NRC SORNs include but are not limited to:

- the categories of individuals covered by the system;
- the legal authority under which the agency collects and maintains individuals' information;
- the purpose for which the agency may use the information;
- the categories of records contained in the system;
- the physical, administrative, and technical safeguards used to secure the information;
- a description of how an individual may request access to or amend their information; and
- listing of permitted "routine uses" of information in the system—that is, the particular types of disclosures an agency is permitted to make to recipients outside the agency without obtaining prior consent of the data subject.

The NRC Privacy Officer works with the appropriate subject matter experts to draft amended or new SORNs, ensuring that the SORNs include the information required by, and meet the format requirements specified in, OMB Circular No. A-108.

9.1 Privacy Act Regulations

NRC has promulgated regulations which implement the requirements contained in the Privacy Act of 1974. The regulations, which are located at *10 CFR Part 9, Subpart B of Title 10 of the CFR*, apply to all records maintained by the NRC that contain identifiable information about individuals and which are included as part of a system of records. NRC's regulations establish procedures that enable individuals to gain access to records maintained about them, provide detailed procedures for how to amend inaccurate information, and limit access such information.

9.2 Privacy Act Statements

The NRC works with forms owners in each of the NRC's offices to ensure that a Privacy Act statement is provided, or otherwise made available, when the agency collects information about individuals that will be maintained in a Privacy Act system of records or when collecting an SSN (irrespective of whether the SSN will be maintained in a Privacy Act system of records). This includes working with the NRC Form's Manager.

NRC's Privacy Act Statements provide individuals with the:

- agency's legal authority to collect the information, such as statutes, executive orders, and/or regulations;

- purpose for collecting the information and how it will be used;
- routine uses of the information, which describe to whom the NRC may disclose information when disclosing it outside the agency and for what purpose;
- if disclosure is mandatory or voluntary, and the effect on the individual of not providing the information; and
- contact information for questions.

10 Overview of Handling and Protecting Personally Identifiable Information

Handling and safeguarding PII maintained and used by NRC personnel is necessary to ensure the trust of NRC stakeholders. PII refers to information which can be used to distinguish or trace an individual's identity, either alone or when combined with other information, and which is linked or linkable to a specific individual, such as information relating to NRC stakeholders or individual NRC employees or contractors. Sensitive PII is PII which, if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. It is always important to consider the context in which the information is used when determining the level of sensitivity. The same types of information can be sensitive or non-sensitive depending on the context. For example, a list of employee names and phone numbers maintained for emergency contact purposes is far less sensitive than a list of employee names and phone numbers who are being treated for a particular disease.

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

10.1 Minimizing the Collection of PII

Consistent with the Privacy Act and NRC PII policies, the NRC limits the collection of PII from individuals. The NRC maintains only relevant and necessary information about individuals, in accordance with a legally authorized purpose. The NRC also complies with the OMB Circular A-130, Managing Information as a Strategic Resource, which directs agencies to eliminate unnecessary collections, maintenance, and uses of SSN.

NRC's Privacy Program maintains an inventory of PII holdings and uses the PTA, PIA, and SORN processes to identify methods to further reduce the PII data the agency collects and to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Additionally, NRC's SAOP ensures that the NRC minimizes the collection and use of PII in the context of NRC forms and correspondence.

10.2 Handling and Transmitting PII

The NRC provides guidelines for employees and contractors who handle PII. Methods for handling PII include, but are not limited to the following, and must be done in accordance with NRC's approved records schedules:

- You must NOT store PII in a shared electronic location (e.g., shared drives, SharePoint,

Power Apps, or Teams location) unless access is restricted to those with a need-to-know by permissions settings or passwords.

- Secure paper records must be in a locked file drawer.
- Do not leave PII in open view of others, either on your desk or computer screen.
- Destroy paper records containing PII by shredding.
- Use an opaque envelope when transmitting PII through the mail.
- Do not collect or maintain PII unless you are authorized to do so as part of your official duties.
- Remove or delete PII when no longer needed.
- Emails containing PII that are sent outside the agency must be encrypted.

PII may be distributed or released to other individuals only if:

- it is within the scope of the recipient's official duties;
- the recipient has an official, job-based need-to-know;
- the distribution is done in accordance with a legitimate underlying authority (e.g., a routine use specified in a SORN); and
- sharing information is done in a secure manner. When in doubt, NRC employees must treat PII as sensitive and must keep the transmission of sensitive PII to a minimum, even when transmission would occur by secure means.

Secure means for communicating, sending, and receiving PII include the following:

- **Email** – When emailing PII to external users, NRC personnel should ensure the information is appropriately encrypted.
- **Facsimile** – When faxing PII, NRC personnel should notify the recipient before and after transmission.
- **Mail** – NRC personnel should physically secure PII when in transit by sealing it in an opaque envelope or container, and mail it using First-Class or Priority Mail, or a comparable commercial service. NRC personnel should not mail or send PII by courier on any media unless the data is encrypted.
- **Hard Copy** – NRC personnel should hand-deliver documents containing PII whenever needed. NRC personnel should not leave PII unattended on printers, facsimile machines, copiers, or in other common places.

10.3 Contractors and Third Parties

The NRC ensures contractors and third parties comply with privacy requirements when they:

- Create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the agency
- Operate or use information systems on behalf of the agency

NRC's Privacy Program has coordinated with NRC's Acquisition Management Division to ensure that the applicable privacy clauses are included in the terms and conditions of contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of NRC information.

11 Breach Response and Management

The NRC has an obligation to protect the personal information individuals entrust to the agency. The NRC Privacy Office takes this obligation very seriously and has developed a *Breach Notification Plan* that defines NRC policies and procedures for reporting, investigating, and managing a PII breach.

It is NRC policy that all NRC staff and contractors immediately report any suspected or confirmed breach of PII to the Computer Security Incident Response Team (CSIRT) at CSIRT@nrc.gov or 301-415-6666 along with their direct supervisory chain of command. This includes but is not limited to:

- Email spills that may contain PII
- PII spills on Shared Drives, ADAMS, OneDrive, Teams, SharePoint Online, Power Apps
- Stolen/lost/missing NRC laptops or mobile devices that may contain PII

CSIRT conducts initial forensics to confirm the sensitivity of the information and contacts the NRC Privacy Officer to validate that the information is in fact PII. Once CSIRT is made aware of a possible spill, CSIRT requests the Customer Service Center (CSC) to lockdown the file, if applicable and grant access only to the CSIRT Team and the NRC Privacy Officer to confirm whether it is a PII spill.

Note: Non-electronic PII incidents such as the improper handling or storage of hardcopy documents containing PII must be reported immediately to the Office of Administration (ADM) Division of Facilities & Security (DFS).

Within one (1) hour of discovery or detection, CSIRT will notify the Cybersecurity and Infrastructure Security Agency (CISA) United States Computer Emergency Readiness Team if the confirmed spill compromised the confidentiality, integrity, or availability of NRC systems.

If the NRC determines that a breach constitutes a "major incident," the SAOP will notify the appropriate Congressional Committees no later than seven days after the date of determination. In addition, NRC will supplement their initial seven-day notification to Congress with a report no later than 30 days after the agency discovers the breach.

As defined in OMB-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements, a breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American

people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII automatically constitutes a "major incident."

11.1 Privacy Program's Role in Incident Response Process

These procedures describe the Privacy Program's role in the incident response process. In accordance with NRC's Incident Response Policy and Procedures, there are additional steps the CISO is required to take to detect, contain, respond to, and prevent incidents, in accordance with NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide. The process includes the following:

- All NRC employees and contractors must immediately report any potential or actual incidents to NRC's CSIRT as soon as they become aware that an incident may have occurred.
- CSIRT must investigate the facts and circumstances surrounding the potential incident and, if PII may have been involved, obtain a determination by the SAOP or designee as to whether PII was potentially compromised.
- The SAOP and Core Management Group (CMG) must determine which remediation methods should be used in the event of an actual compromise of PII based on the type of harm caused to the individual(s).
- CSIRT develops after action reports for high and moderate risk incidents, which document the details of the incidents and the steps taken to remediate the gaps which caused the incident to occur.
- CSIRT conducts an annual table-top exercise, which consists of a structured, readiness-testing activity, which simulates an actual incident involving PII designed to prepare key stakeholders and decision-makers for an emergency situation involving a data breach.

12 Awareness and Training

The NRC requires all employees and contractors to complete privacy training when first beginning work with the agency and annually thereafter. The NRC conducts its annual training through the agency's Talent Management System (TMS). The training provides an overview of important statutory, regulatory, and other Federal privacy requirements, including the Privacy Act, Freedom of Information Act and the E-Government Act of 2002.

12.1 New Employee Orientation Training

NRC's Office of Chief Human Capital Officer provides privacy training to all new employees which must be completed within 30 days from their first day of work with the agency. New employee orientation sessions provide an overview about the importance of privacy at the NRC, how to handle privacy-protected information, and the penalties for violating the Privacy Act.

12.2 Role-Based Training

In addition to new employee and annual privacy training requirements, NRC's Privacy Program provides role-based training to employees with specialized roles on a periodic basis as part of their official duties. The NRC includes privacy training in other continuing education venues such as the "Lunch Byte" series and the ISSO/Auditor Training Course.

13 Privacy Reporting

FISMA requires Federal agencies to develop, document, and implement agency-wide information security programs, which include plans and procedures to ensure the security of operations for information systems which support the operations of the agencies. All Federal agencies are required to submit an annual report to OMB; the United States Department of Homeland Security; and specific Committees in the United States House of Representatives and Senate.

NRC's SAOP completes the SAOP report, which is submitted as part of the NRC's annual FISMA report.

14 Conclusion

The NRC is committed to safeguarding PII that individuals entrust to the agency. The NRC's Privacy Program uses regulations, policies, guidance, and principles to further its objective across the agency. Privacy considerations are embedded in all levels of decision-making and operations to continue to build a culture of trust and privacy at the NRC.

Signed by Flanders, Scott
on 09/27/23

Scott C. Flanders
Senior Agency Official for Privacy
U.S. Nuclear Regulatory Commission