U.S. NUCLEAR REGULATORY COMMISSION

PRIVACY PROGRAM PLAN

September 2020

U.S. Nuclear Regulatory Commission Privacy Program Plan

Table of Contents

U.S. Nuclear Regulatory Commission Privacy Program Plan

1. Introduction

The purpose of the U.S. Nuclear Regulatory Commission (NRC) Privacy Program Plan is to provide an overview of the privacy program. This Plan, which is consistent with the requirements in the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource* includes:

- A description of the structure of NRC's privacy program;
- The resources dedicated to 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 privacy requirements and manage privacy risks; and
- Additional information deemed important by NRC's SAOP to provide an overview of NRC's privacy program requirements.

2. Overview of NRC Privacy Program

2.1 Mission Statement

NRC's program is led by NRC's SAOP. The mission of the 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*; E-Government Act of 2002; and the Federal Information Security Modernization Act (FISMA), as well as policy directives and best practices issued in furtherance of those Acts.

The Privacy Program also implements requirements in 32 *Code of Federal Regulations* (CFR) Part 2002, "Controlled Unclassified Information," because current laws, regulations, or government-wide policies require safeguarding or dissemination 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 Privacy Program adheres to the policy framework embodied in the Fair Information Practice Principle (FIPPs) to ensure that individual privacy is protected throughout the collection, maintenance, use, and dissemination of all PII maintained by the NRC. The FIPPs consist of

the following five core principles: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. The 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), Cyber Security Branch and Network and Security Operations Branch to implement and operationalize policies to secure the confidentiality, integrity, and availability of 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; and
- Maintains updated privacy artifacts in compliance with legal requirements (e.g., System of Records Notice, Privacy Impact Assessments, Privacy Threshold Analysis, and Privacy Act Notices).

2.2 NRC Privacy Office Organization

NRC's Privacy Program is housed within 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 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 NRC's Deputy Director of OCIO, who has also been formally designated as NRC's SAOP pursuant to OMB Memorandum 16-24, *Role and Designation of Senior Agency Officials for Privacy*.

The SAOP is NRC's key policy advisor on implementing the Privacy Act of 1974; the privacy provisions of the FISMA; the privacy provisions contained in the E-Government Act of 2002; OMB requirements regarding privacy, including those contained in OMB Circular A-130, *Managing Information as a Strategic Resource*; and National Institute of Standards and Technology (NIST) guidance. The SAOP is responsible for:

- Serving as 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;
- Developing and overseeing implementation of Agency-wide policies and procedures relating to the Privacy Act, and assuring that personal information contained in Privacy Act systems of records is handled in compliance with its provisions;
- 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;

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

- Advocating strategies for data and information collection and dissemination, to ensure 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;
- Ensuring that NRC employees have the appropriate training and education concerning privacy laws, regulations, policies, and procedures;
- Working with NRC stakeholders to ensure that vendors/contractors, with access to PII, who engage in business with 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 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 NRC's privacy program are incorporated into NRC's enterprise infrastructure, information technology (IT), an IT security program;
- Coordinating with the Office of the General Counsel on privacy laws, regulations, policies, and procedures;
- Assessing the overall effectiveness of the Privacy Program.

In accordance with OMB Memorandum 16-24, NRC's 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.

2.3 Strategic Goals and Objectives for Privacy

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 Analysis (PTA), 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 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 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. In accordance with the FIPPs, NRC is authorized to only collect PII that is necessary to carry out its mission and must use that information in accordance 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**

NRC's 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**

NRC's 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

❖ **Establish Metrics to track the effectiveness of the NRC's Privacy Program**

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

3. Privacy Workforce Management

NRC's 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 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.

4. Budget and Acquisition

NRC's 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.

5. Fair Information Practice Principles

NRC's privacy program adheres to the FIPPs. 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** – NRC monitors, audits, and documents compliance with the FIPPs through a number of 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** – NRC limits the PII which it creates, collects, uses, processes, stores, maintains, disseminates, and discloses to what is directly relevant and necessary to accomplish the legally authorized purpose. NRC ensures that the appropriate authorities are cited in the appropriate Privacy Act notices.

- **Minimization** – NRC creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII, which is directly relevant and necessary to accomplish the legally authorized purpose. The PII is maintained for as long as is necessary to accomplish the purpose and/or according to the retention schedules.

- **Quality and Integrity** – 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 are involved in the process of using PII and, to the extent practicable, individual consent is granted for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Individuals may address concerns or complaints to NRC's SAOP.

- **Purpose Specification and Use Limitation** – 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 explained in the Privacy Act notice, where applicable.

- **Security** – 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, and disclosure.

- **Transparency** – NRC provides clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

6. Privacy Risk Management Framework

NRC adheres to the process described in 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 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

- Reviews privacy impact assessment which assesses the privacy risks for each of NRC's information systems.

7. Privacy Control Requirements

NRC has implemented NIST SP 800-53, Rev. 4 Appendix J to ensure compliance with applicable statutory, regulatory, and policy requirements with respect to information security. NRC also adheres to Section 208 of the E-Government Act of 2002, which requires agencies to conduct PIAs for electronic systems and collections.

7.1 NRC Control Allocation

NRC's Privacy Program has implemented the requirements contained in NIST SP 800-53, Rev. 4 Appendix J. The Privacy Program will designate each control as program management, common, information system-specific, or hybrid. Common controls are controls that are inherited by multiple information systems. Information system-specific controls are controls that are implemented for a particular information system, or the portion of a hybrid control that is implemented for a particular information system. Hybrid controls are controls that are implemented for an information system, in part as a common control and in part as an information system-specific control. The determination as to whether a privacy control is a common, information system-specific, or hybrid control is based on context.

7.2 Privacy Threshold Analysis

A PTA is a questionnaire used to determine if a system contains PII, whether a PIA is required, whether a SORN is required, and if any other privacy requirements apply to the information system. A PTA is completed when procuring a new IT system, when developing or significantly modifying an information system, or when a new collection of information is being developed. While a PTA is not a legally required document, NRC's Privacy Program uses the document to determine whether legally mandated documents are required for each of NRC's information systems. For the status on any PTA's, see our PTA status listing.

7.3 Privacy Impact Assessment

A PIA is legally required by Section 208 of the E-Government Act of 2002 and analyzes how information in an identifiable form is collected, maintained, stored, and disseminated. The PIA analyzes the privacy risks as well as the protections and process for handling information to mitigate the privacy risks. PIAs are conducted when:

1. Developing or procuring information systems or projects that collect, maintain, or disseminate information in identifiable form; or

2. Initiating a new electronic collection of information in identifiable form from 10 or more persons

NRC's PIAs describe: (1) what information is to be collected; (2) why the information is being collected; (3) the intended use of the information; (4) with whom will the information be shared; (5) what opportunities individuals have to decline or consent to provide information or the particular uses of the information; (6) how the information will be secured (7) whether a system of records is being created under the Privacy Act.

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 complete, the Cyber Security 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, NRC requires PIA's and PTA's to be reviewed annually. For additional details, see our Privacy Impact Assessment Manual and our PIA Status Listing.

7.4 Contractors and Third Parties

NRC ensures contractors and third parties who: (1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the Agency; or (2) operate or use information systems on behalf of the Agency, comply with the mandated privacy requirements. NRC's Privacy Program 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.

7.5 System of Records Notices

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*. A system of records is a group of any records, under the control of any agency, from which information about individuals is retrieved by a unique identifier associated with 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.

All NRC SORNs include a variety of elements, such as: (1) the categories of individuals covered by the system; (2) the legal authority under which the agency collects and maintains individuals' information; (3) the purpose for which the agency may use the information; (4) the categories of records contained in the system; (5) the physical, administrative, and technical safeguards used to secure the information; (6) a description of how an individual may request access to or amend their information; and (7) 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.

7.6 Privacy Act Statements

NRC works with forms owners in each of 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 statute, executive order, and/or regulation;
- Purpose for collecting the information and how it will be used;
- Routine uses of the information, which describes to whom NRC may disclose information and for what purpose; and
- Whether providing the information is mandatory or voluntary, along with the effects, if any, on the individual for not providing all or any part of the information requested.

7.7 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 NRC that contain identifiable information about individuals and which are included as part of a system of records. NRC's regulations establish procedures, which enable individuals to gain access to records maintained about them; provide detailed procedures for how to amend inaccurate information; and limit individuals who may access such information.

8. 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.

8.1 Recognizing PII

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.

The following types of PII are considered sensitive when associated with an individual:

- SSN (including in truncated form);
- Personal Account numbers (included in truncated form);
- Place of birth;
- Date of birth;
- Mother's maiden name;
- Biometric information; (e.g., physiological measurement that uniquely identifies a specific individual, such as fingerprints, palm veins, iris prints, or DNA);
- Medical information;
- Personal banking/investment account information (including bank routing numbers);
- Credit card/purchase card account numbers;
- Passport numbers;
- Potentially sensitive employment information (e.g., performance ratings, disciplinary actions, results of background investigations);
- Criminal history; or
- Information which may stigmatize or may adversely affect an individual.

8.2 Minimizing the Collection of PII

NRC complies with the Privacy Act's requirement to limit the collection of PII from individuals. NRC maintains only relevant and necessary information about individuals, in accordance with a legally authorized purpose. 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 data the Agency collects and to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Moreover, NRC's SAOP ensures NRC minimizes the collection and use of PII contained on NRC forms and correspondence.

8.3 Handling and Transmitting PII

NRC provides guidelines for employees and contractors who handle PII due to the nature of the data and the risk to an individual if data were to be compromised. Methods for handling PII include, but are not limited to, the following, and must be done in accordance with NRC's approved records schedules:

- Store sensitive PII on secure NRC networks, systems, and NRC-approved media;

- Secure sensitive paper PII data by locking it in desks and filing cabinets;

- Remove visible PII from desks and office spaces when not in use;
- Destroy sensitive PII by shredding;
- Delete sensitive electronic PII by emptying computer "recycle bin";
- Only use NRC-provided e-mail addresses for conducting official business; and
- Encrypt sensitive PII on computers, media, and other devices, especially when sending data outside of NRC's network.

Sensitive PII may be distributed or released to other individuals only if: (1) it is within the scope of the recipient's official duties; (2) the recipient has an official, job-based need to know; (3) the distribution is done in accordance with a legitimate underlying authority (e.g., a routine use specified in a SORN); and (4) 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 sensitive PII include:

- **Facsimile** – When faxing information, 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 by courier, sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.
- **Hard Copy** – NRC personnel should hand-deliver documents containing sensitive PII whenever needed. NRC personnel should not leave sensitive PII unattended on printers, facsimile machines, copiers, or in other common places.

9. Breach Response and Management

NRC has an obligation to protect the personal information individuals entrust to the Agency. The Privacy Program takes this obligation very seriously and has developed a policy and procedures to inform NRC employees and contractors of their obligation to protect PII and to instruct them in specific steps they must take in the event there is an actual or potential compromise of PII. NRC's process for responding to a breach of PII is part of the Agency's formal Incident Response Policy and Procedures and is based on OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

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 Incident Response Team (IRT) as soon as they become aware that an incident may have occurred;

- The IRT 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);

- The IRT 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; and

- The IRT 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.

10. Awareness and Training

NRC requires all employees and contractors to complete privacy training when first beginning work with the Agency and annually thereafter. 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.

10.1 New Employee Orientation Training

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

10.2 Talent Management System

NRC delivers privacy-specific annual training, through the Agency's centralized training system, called TMS. The annual privacy training is required to be completed by all NRC employees and contractors.

10.3 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.

11. 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 to specific Committees in the United States House of Representatives and Senate.

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

12. Conclusion

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

Signed by Flanders, Scott
on 09/16/20

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