NRC's FY 2015 Privacy Program Memorandum

It is the policy of the Nuclear Regulatory Commission (NRC) to ensure that Systems of Records are established and maintained to protect the rights of individuals from unnecessary invasion of personal privacy in accordance with the Federal Privacy Act of 1974, as amended (5 U.S.C. 552a). The processing of initial requests or appeals is consistent with the requirements and the time limits of the Privacy Act and Title 10 of the *Code of Federal Regulations* (CFR) Part 9, Subpart B, "Privacy Act Regulations."

The NRC's privacy program is described in Management Directive 3.2, Privacy Act, July 10, 2014. The Agency's Chief Information Officer (CIO) is designated as the Senior Official for Privacy Policy (SAOP) responsible for ensuring that a program to administer the Privacy Act is established and effectively implemented within the NRC. The NRC General Counsel is responsible for advising and assisting with the development of regulations, procedures and other matters related to the Privacy Act. Placing the SAOP function at a senior management position within the Office of the CIO, with the participation of the General Counsel, ensures that the SAOP has the authority, independence, access to agency leadership, subject matter expertise, and resources to effectively manage and oversee all privacy-related functions across the agency. At NRC, the CIO may delegate the authorities and responsibilities of the SAOP, as necessary. The CIO makes the final determinations, on behalf of the Executive Director for Operations (EDO), on appeals of initial denials of Privacy Act requests, corrections or amendments of Privacy Act records held by an office reporting to the EDO, and on appeals of denials of fee waivers or reductions and denials of expedited processing requests.

Pursuant to MD 3.2, the Chief Information Officer has delegated authorities and responsibilities of the Senior Agency Official for Privacy (SAOP) to the Deputy Director for OCIO. The Deputy Director of OCIO, as SAOP, has the overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with Federal laws, regulations, and policies relating to information privacy. The SAOP designates the Privacy Act (PA) Officer, the official responsible for implementing and administering the Privacy Act program, in accordance with NRC regulations. The SAOP also approves and issues *Federal Register* notices (FRN) establishing new and amending existing Systems of Records in accordance with the delegated authority. The SAOP is also responsible for proposing needed amendments to NRC regulations (10 CFR Part 9) implementing the Privacy Act. In addition, the SAOP provides advice and assistance in the development of technical safeguards for the preservation of data integrity and security for Systems of Records using automated records or processes. Finally, the SAOP implements the program for administering the privacy provisions of Section 208 of the E-Government Act of 2002.

The NRC conducts privacy reviews and provides employees and contractors with privacy-awareness training. Importantly, the NRC has established a process for conducting Privacy Impact Assessments (PIAs) of its information systems containing Personally Identifiable Information (PII) to identify and reduce the privacy impact of the organization's activities, and to notify affected persons about any privacy impacts and steps taken to mitigate them if available. NRC's "Privacy Impact Assessment Manual" (PIA Manual) (Agencywide Documents Access and Management System (ADAMS) Accession No. ML11143A050) explains the processes and procedures required for completing a PIA. NRC has also prepared a privacy threshold analysis (PTA) template that can be used to determine if a PIA is necessary. For additional information, please see the "Privacy Impact Assessment" (ADAMS Accession No. ML050460335) or the "Privacy Threshold Analysis" (ADAMS Accession No. ML091970114). NRC's PIA process is

consistent with relevant privacy-related policy, guidance, and standards and Privacy Act System of Records Notices (SORN's)

Pursuant to OMB memorandum (M-07-16), NRC also has developed a PII Breach Notification Policy (included in FY15 NRC FISMA submission) and has implemented procedures for responding to PII breaches. NRC designates a Core Management Group (CMG) consisting of the General Counsel, the Inspector General, the CIO, and the SAOP, the Deputy Director of OCIO. CMG membership may be supplemented by the Chief Human Capital Officer, the Director of the Office of Administration, or the Chief Financial Officer, as appropriate. For breaches resulting in a CMG decision to notify affected individuals, the Directors of the Office of Public Affairs and the Office of Congressional Affairs, will also participate in the CMG. Similarly, for breaches involving information technology systems, the Director of the Information Security Directorate in OCIO will also be included in the CMG. The Breach Notification Policy provides for assessment of the breach, and depending on the risk to individuals, notification of Credit-Monitoring Remedy.

The NRC continues to develop and implement measures to ensure that the proper use and protection of personally identifiable information (PII) is accomplished in accordance with statutory mandates and to properly safeguard the privacy of individuals.