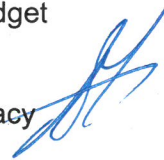




UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

October 17, 2019

MEMORANDUM TO: Mick Mulvaney, Director
Office of Management and Budget

FROM: Scott C. Flanders
Senior Agency Official for Privacy 

SUBJECT: THE U.S. NUCLEAR REGULATORY COMMISSION'S FISCAL
YEAR 2019 PRIVACY PROGRAM MEMORANDUM

It is the policy of the U.S. 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* (10 CFR) Part 9, "Public Records," Subpart B, "Privacy Act Regulations."

The NRC describes its privacy program in [Management Directive \(MD\) 3.2, "Privacy Act,"](#) dated July 10, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML18073A087). The agency's Chief Information Officer (CIO) is designated as the Senior Agency Official for Privacy (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 and procedures and other matters related to the Privacy Act. Placing the SAOP function at a senior management position within the Office of the Chief Information Officer (OCIO), 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 the 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 to or amendments of Privacy Act records held by an office reporting to the EDO and appeals of denials of fee waivers or reductions and denials of expedited processing requests.

Pursuant to MD 3.2, the CIO has delegated the SAOP's authorities and responsibilities to the Deputy Director of 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 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 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. The NRC's "[Privacy Impact Assessment Manual](#)," issued May 2014 (ADAMS Accession No. ML11143A050), explains the processes and procedures required for completing a PIA. The NRC has also prepared a privacy threshold analysis template that can be used to determine whether a PIA is necessary. The NRC's [PIA template](#) (ADAMS Accession No. ML050460335) and [privacy threshold analysis template](#) (ADAMS Accession No. ML091970114) contain additional information. The NRC's PIA process is consistent with relevant privacy-related policy, guidance, and standards and Privacy Act system of records notices.

Pursuant to an Office of Management and Budget memorandum (M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated May 22, 2007), the NRC also has developed a [PII Breach Notification Policy](#), revised February 2014 (ADAMS Accession No. ML14036A058) (included in the Fiscal Year(FY) 2018 NRC Federal Information Security Modernization Act (FISMA) submission), and has implemented procedures for responding to PII breaches. In the event of a breach involving PII, the NRC will designate a Core Management Group (CMG), consisting of the General Counsel, the Inspector General, the CIO, and the SAOP. The Chief Human Capital Officer, the Director of the Office of Administration, or the Chief Financial Officer may supplement CMG membership, 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 CMG will also include the OCIO Chief Information Security Officer. The breach notification policy provides for assessment of the breach and, depending on the risk to individuals, notification of a credit-monitoring remedy.

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

The following provides the current listing of names and titles of all staff supporting the NRC's privacy program, along with the names, titles, and organizational information for the FY 2019 SAOP FISMA reporting metrics:

- OCIO, Deputy Director, SAOP, Scott Flanders
- OCIO, Governance & Enterprise Management Services Division, Director, John Moses
- OCIO, Governance & Enterprise Management Services Division, Deputy Director, Cris Brown

- OCIO, Governance & Enterprise Management Services Division, Information Services Branch Chief, Anna McGowan
- OCIO, Governance & Enterprise Management Services Division, Information Services Branch, Privacy Officer, Sally Hardy
- OCIO, Information Technology Services Development and Operations Division, Security Operations Branch, Information Technology Specialist, Charles Watkins