CHAIRMAN

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

January 15, 2026

The Honorable Russell Vought
Director, Office of Management
and Budget
725 17th Street, NW
Washington, DC 20503

Dear Director Vought:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am pleased to report that the agency has submitted its Federal Information Security Modernization Act (FISMA) and Privacy Management Program documents for fiscal year (FY) 2025 through CyberScope, in accordance with Office of Management and Budget (OMB) Memorandum M-25-04, "Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements," dated January 15, 2025. The NRC submitted the following nine documents:

(1) Chief Information Officer/FY 2025 Quarter 4 Annual FISMA Report
(2) Senior Agency Official for Privacy/FY 2025 Annual FISMA Report
(3) Agency Privacy Program Plan
(4) Agency Privacy Program Changes
(5) Agency Breach Response Plan
(6) Agency Privacy Continuous Monitoring Strategy
(7) Agency Privacy Program—Uniform Resource Locator
(8) Social Security Numbers Eliminated and Progress Report
(9) CASES Act Implementation

The NRC's Office of the Inspector General will submit the Inspector General section of the FY 2025 Annual FISMA Report separately through CyberScope.

The NRC continues its efforts to enhance compliance with FISMA requirements and mature the agency's Privacy Program. To date, the NRC has 15 reportable systems. In FY 2025, the agency introduced new technology and cloud services and completed security assessments and approved change authorizations for each related system. The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) performed a "Red Team" assessment of the NRC's information technology infrastructure to evaluate the effectiveness of the agency's cybersecurity protections and identify any areas for improvement. Overall, the NRC demonstrated its cybersecurity maturity as evidenced by achieving a managed and measurable ("effective") rating during the annual FISMA audit.

The NRC had no major security incidents during FY 2025. However, the agency had a total of six confirmed reportable incidents. The NRC's Computer Security Incident Response Team reported these six incidents to CISA with the following threat vectors: three Improper

Usage, one Email, and two categorized as Other. The agency fully investigated, mitigated, and remediated all reportable incidents.

In an environment focused on efficiency, accountability, and outcomes, the NRC is continually assessing its workforce's IT needs and competencies, and adjusting as necessary to align with the administration's priorities and deliver at the highest level. The NRC is incorporating advanced technologies, such as artificial intelligence, to support its regulatory mission while concurrently evaluating the security implications of these technologies, including expanded monitoring and controls. From an enterprise visibility perspective, the NRC has improved its investigative and remediation capabilities by achieving advanced log management maturity and full compliance with OMB Memorandum M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," dated August 27, 2021 (event logging level 3). The agency has also made significant strides in automating cybersecurity governance processes and activities through a governance, risk, and compliance platform, and it continues to enhance support for continuous system authorizations.

In the upcoming FY, the NRC will prioritize adopting new measures as outlined by the administration's cybersecurity strategy. The agency will continue to enhance the ongoing authorization program by incorporating additional control parameters for cloud services based on the recently revised Federal Risk and Authorization Management Program guidance. This includes implementing additional personal identity verification, reducing the risk of unauthorized or end-of-life software, mitigating supply chain risks, and addressing any audit findings. Additionally, the NRC will continue working to implement a zero-trust architecture, adopt quantum readiness strategies, and expand the deployment of endpoint detection and response.

In accordance with OMB and DHS instructions, the NRC will continue to inform your staff of its progress on these initiatives.

If you have any questions about the NRC's FY 2025 FISMA and Privacy Management Program documents, please contact me or have your staff contact Mr. Scott Flanders, Chief Information Officer, at (301) 415-6717.

Sincerely,

Ho K. Nieh