



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

October 26, 2020

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

Dear Mr. Vought:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am pleased to report that the Federal Information Security Modernization Act (FISMA) and Privacy Management Program documents for fiscal year (FY) 2020 have been submitted through CyberScope in accordance with the November 19, 2019, Office of Management and Budget (OMB) Memorandum M-20-04, "Fiscal Year 2019–2020 Guidance on Federal Information Security and Privacy Management Requirements." The NRC's submittal included the following eight documents:

- (1) Chief Information Officer/2020 Quarter 4 Annual FISMA Report
- (2) Senior Agency Official for Privacy/2020 Annual FISMA Report
- (3) Agency Privacy Program Changes
- (4) Agency Privacy Program Plan
- (5) Agency Breach Response Plan
- (6) Agency Privacy Continuous Monitoring Strategy
- (7) Agency Privacy Program – Uniform Resource Locator
- (8) Social Security Number Collection Policy and/or Procedures

The NRC's Office of the Inspector General will separately submit the Inspector General Section Report/2020 Annual FISMA Report through CyberScope.

The NRC continues its efforts towards full compliance with FISMA targets and with the agency's Privacy Management Program. To date, the NRC has reduced its number of reportable systems to 17. During FY 2020, the agency completed security assessments and approved change authorizations for each system.

The NRC had no major security incidents during FY 2020. The NRC had a total of 10 confirmed incidents. The NRC's Computer Security Incident Response Team reported six incidents to the U.S. Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT): five improper usage events and one attempted access event. US-CERT reported four incidents to the NRC. The NRC investigated, mitigated, and remediated all 10 incidents.

As in prior years, the NRC participated in the high-value asset risk and vulnerability assessments led by DHS and has completed mitigation and remediation activities. In accordance with current DHS guidance, the NRC reassessed its high-value assets and reduced the number from nine to five. The NRC will continue to collaborate with DHS in future efforts to assess the NRC's protection of high-value assets.

The NRC continues to make progress toward meeting the cybersecurity cross-agency priority (CAP) goals, as demonstrated by the agency's 100-percent achievement of the FY 2020 metric targets. The "CAP Goal Evaluations" table in Appendix A to the NRC's Chief Information Officer/2020 Quarter 4 Annual FISMA Report details the agency's current progress.

In the upcoming fiscal year, the NRC will continue to make progress in updating the ongoing authorization program, deploying encryption at rest, implementing additional personal identity verification, reducing the risk of unauthorized software, and addressing audit findings.

In accordance with the instructions issued by OMB and DHS, the agency will continue to update your staff on its progress on these initiatives.

If you have any questions about the FY 2020 NRC FISMA and Privacy Management Program documents, please contact me or have your staff contact Mr. David J. Nelson, Chief Information Officer, at (301) 415-8700.

Sincerely,

A handwritten signature in blue ink, appearing to read 'K. Svinicki', is written over a light blue horizontal line.

Kristine L. Svinicki

Identical letter sent to:

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

The Honorable Chad F. Wolf
Secretary of Homeland Security
Washington, DC 20528