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

CHAIRMAN

October 30, 2017

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

Dear Mr. Mulvaney:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am providing the fiscal year (FY) 2017 Federal Information Security Modernization Act (FISMA) Report and Privacy Management reports. The reports constitute the following nine enclosures:

- 2017 Quarter 4 / Annual Chief Information Officer (CIO) Report
- 2017 Quarter 4 / Annual Seeking Service Agencies (SSA) Report
- Agency Information Security Continuous Monitoring (ISCM) Strategy
- 2017 Annual Senior Agency Official for Privacy (SAOP) Section Report
- Progress Update on Actions Taken to Protect Personally Identifiable Information (PII) and Social Security Numbers (SSN)
- NRC Plan to Eliminate the Unnecessary Collection and Use of SSN
- Breach Notification Policy
- NRC's Privacy Program Memorandum
- Inspector General (IG) Section Report

Since submitting last year's report, the NRC continues towards full compliance with FISMA targets and with the agency's Privacy Management Program. The current number of reportable systems at the NRC stands at 23. During FY 2017, the agency completed security assessments and approved change authorizations for each system. Subsequently, the NRC's Office of the Inspector General identified weaknesses and program issues related to the inventory and authorization of NRC national security systems. The NRC has initiatives underway, overseen by senior leadership, to address these findings.

NRC had no major security incidents that resulted in significant compromise of Information Security during FY 2017. There have been a total of 27 confirmed incidents reported to the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team. This total is comprised of 23 information spills, 2 attempted attacks against the external perimeter, and 2 lost devices. The confirmed incidents at NRC headquarters and

Enclosures 1, 2, and 4 transmitted herewith contains Official Use Only – Security-Related Information. When separated from these enclosures, this document is decontrolled.

regional locations were all detected and reported to the agency's Computer Security Incident Response Team and have all been mitigated.

In prior years, the NRC has participated in the high-value assets risk and vulnerability assessments led by DHS, and has completed mitigation and remediation activities. 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 towards meeting the cybersecurity cross-agency priority (CAP) goals. Current progress is presented in the "CAP Goals Evaluations" table, embedded as Appendix A of Enclosure 1.

In the upcoming year, the NRC expects to make progress in updating the ongoing authorization program, implementing additional personal identity verification, reducing the risk of malware, and addressing audit findings.

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

If you have any questions about the FY 2017 NRC FISMA and Privacy Management reports, please contact me or have your staff contact Mr. David J. Nelson, Chief Information Officer, at (301) 415-8700.

Sincerely,

Kristine L. Svinicki

Enclosures:
As stated