December 1, 2016

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

Dear Mr. Donovan:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am providing the agency's fiscal year (FY) 2016 Federal Information Security Management Act (FISMA) and Privacy Management reports. The reports include the following ten enclosures:

- Chief Information Officer Section Report and Crosswalk – Office of Management and Budget (OMB) Memorandum 17-05 to NRC's Annual FISMA Letter/Enclosures
- Information Security Continuous Monitoring Process
- Progress Towards Meeting the FISMA Metrics and Cybersecurity Cross Agency Priority (CAP) Goals
- Senior Agency Official for Privacy Section Report
- Progress Update on Actions Taken To Protect Personally Identifiable Information (PII) and social security numbers (SSNs), including reviews conducted to identify and reduce the unnecessary collection and use of PII
- NRC Plan to Eliminate the Unnecessary Collection and Use of SSNs
- FY16 Efforts to Comply With the Privacy Related Requirements in OMB M-16-04
- PPI and Privacy Act Responsibilities Awareness Course
- NRC's FY 2016 Privacy Program Memorandum
- Inspector General Section Report

Since submitting last year's report, the NRC continues toward full compliance with FISMA targets and with the agency's Privacy Management Program. The current number of reportable systems at the NRC stands at 22. During FY 2016, the agency completed security assessments and approved change authorizations for each system. Subsequently, the NRC's Office of Inspector General (IG) identified weaknesses and program issues related to the inventory and authorization of NRC national security systems. NRC senior leadership is overseeing initiatives to address these findings.

Since submitting last year's FISMA and privacy management reports, the NRC has had

Enclosures 1, 3, and 4 transmitted herewith contains Official Use Only – Security-Related Information. When separated from these enclosures, this document is decontrolled.

no major security incidents. In the last year, the NRC reported 29 minor security incidents to the U.S. Department of Homeland Security's (DHS's) United States Computer Emergency Readiness Team. All of these incidents were attempts to attack NRC staff through social engineering. NRC staff detected these incidents and reported them to the agency's computer security incident response team. None of these attacks resulted in any compromise of PII, sensitive agency information, or information systems.

The NRC has participated in the DHS-led, high-value assets risk, and vulnerability assessments. The agency continues to perform mitigation and remediation activities associated with this effort. On June 29, 2016, the NRC and DHS also agreed to plan for a security architecture assessment. The NRC will continue to collaborate with DHS in meeting the requirements associated with securing high-value assets.

The NRC continues to make progress towards meeting the Cybersecurity Cross Agency Priority Goals. Current progress is represented in the enclosed table, "Progress Towards Meeting the FISMA Metrics and Cybersecurity Cross Agency Priority (CAP) Goals." 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.

If you have any questions about the FY 2016 NRC FISMA and Privacy Management reports, please contact me or Mr. David Nelson, Chief Information Officer, at (301) 415-8700.

Sincerely,

/RA/

Stephen G. Burns

Enclosures:
As stated