November 13, 2015

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 fiscal year (FY) 2015 Federal Information Security Management Act (FISMA) Report. The enclosed FY 2015 NRC FISMA and Privacy Management reports consist of the following eight documents:

- Chief Information Officer (CIO) Section Report
- Information Security Continuous Monitoring (ISCM) Process
- Process Towards Meeting the FISMA Metrics and Cybersecurity Cross Agency Priority (CAP) Goals
- Senior Agency Official for Privacy (SAOP) Section Report
- Progress Update on Actions Taken to Protect Personally Identifiable Information (PII) Social Security Numbers (SSN), including reviews conducted to identify and reduce the unnecessary collection and use of PII
- Breach Notification Policy
- Personally Identifiable Information and Privacy Act Responsibilities Awareness Course
- NRC's FY 2015 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 2015, the agency completed security assessments and approved change authorizations for each system. Subsequently, the NRC's Office of Inspector General identified weaknesses and program issues related to the effective management of plans of action and milestones, authorizations to operate, and the fulfillment of important risk management activities. The NRC has initiatives underway, overseen by senior leadership, to address these findings.

The NRC had no major security incidents since last year's report. The total number of security incidents reported to the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team was 411. These security incidents were all found to be social engineering attack attempts on NRC staff in headquarters and regional offices. These incidents were all detected or reported to our agency computer security incident response team and resolved; none of them resulted in any compromise of sensitive agency information or information systems. In preparation for the FY 2016 reporting requirements, the NRC revised and updated the centralized agency incident response database to conform to the threat/

impact/ vector based reporting requirements. The NRC also updated its XML feed to maintain automated, secure transmission of reportable agency cybersecurity incidents prior to the September 30, 2015, deadline set by DHS.

The NRC participated in the recent Cyber Sprint Activities. While work continues with the high-value asset area, the NRC significantly reduced its number of privileged users and increased its strong authentication program for both privileged and non-privileged users.

The NRC continues to make progress towards meeting the Cybersecurity CAP 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, reduction of 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 towards addressing these initiatives.

If you have any questions about the FY 2015 NRC FISMA and Privacy Management reports, please contact me or Mr. Darren B. Ash, Chief Information Officer, at (301) 415-7443.

Sincerely,

/RA/

Stephen G. Burns

Enclosures:
As stated