

**Responses to Requests for Information
The Honorable Jason Chaffetz
Letter dated July 26, 2016**

1. **The remaining FISMA report elements due from NRC, as described above; or those materials that are complete, if some elements of NRC's FISMA submission are incomplete, and the status of the remaining elements. According to the Committee's records, the Committee has yet to receive the following items from you:**
 - a. **Your letter to OMB with the elements described in Part I.A. above or—if no letter was submitted to OMB—your attestation that no letter was submitted to OMB;**
 - b. **If not included in your letter to OMB accompanying the FISMA report, a document containing the elements described in Part I.A. including information on security incidents at NRC;**
 - c. **NRC's strategy on Information Security and Continuous Monitoring (ISCM);**
 - d. **NRC's data breach response plan;**
 - e. **NRC's plan for reducing holdings of personally identifiable information and social security numbers;**
 - f. **The memorandum describing NRC's privacy program; and**
 - g. **The memorandum describing NRC's privacy training for employees and contractors.**

ANSWER

- a. See: 11-13-15 Letter to The Honorable Shaun Donovan.pdf.
 - b. See: 11-13-15 Letter to The Honorable Shaun Donovan.pdf; PUBLIC ENCL 1 Breach Notification Policy.pdf; PUBLIC ENCL 2 FY15 Progress Update to Protect PII and SSN.pdf; PUBLIC ENCL 3 NRC_ISCM_Strategy.pdf; PUBLIC ENCL 4 Privacy Program.pdf; PUBLIC ENCL 5 PII-Privacy Training_Final for 2015.pdf; NONPUBLIC ENCL 1 FY15 CIO Report.pdf; and NONPUBLIC ENCL 2 FY15 SAOP Report.pdf.
 - c. See: PUBLIC ENCL 3 NRC_ISCM_Strategy.pdf.
 - d. See: PUBLIC ENCL 1 Breach Notification Policy.pdf.
 - e. See: PUBLIC ENCL 2 FY15 Progress Update to Protect PII and SSN.pdf.
 - f. See: PUBLIC ENCL 4 Privacy Program.pdf.
 - g. See: PUBLIC ENCL 5 PII-Privacy Training_Final for 2015.pdf.
-
2. **If you believe NRC is not subject to or is otherwise exempt from FISMA, your legal interpretation of FISMA and your agency's authorizing statutes that exempts NRC from FISMA.**

ANSWER

The NRC does not claim an exemption from FISMA.

Enclosure

- 3. The classified annex for NRC's report submitted under Section 3554(c) for FY 2015, or your attestation that no classified annex to the report exists or was created.**

ANSWER

The NRC attests that no classified annex to the report exists or was created.

- 4. The report of the results of each independent evaluation of information security program as required under Section 3555 for FY 2015.**

ANSWER

See: PUBLIC ENCL 6 OIG Evaluation.pdf.

- 5. The report of the results of each independent evaluation of an information security program involving a national security system or a classified system, as required under Section 3555 for FY 2015, or your attestation that NRC does not have or control any national security systems or classified systems.**

ANSWER

The 2015 Office of the Inspector General (OIG) FISMA audit did not include an evaluation of a national security system, the classified cybersecurity program, or any classified system. I have since designated the OIG as the evaluator of the NRC's national security systems. The OIG will conduct the evaluation as soon as practical. Separately, the OIG is now completing, and will soon deliver to Congress, its FY 2016 review of covered systems under Section 406 of the Cybersecurity Act of 2015, which includes national security systems.

- 6. The report of the results of each penetration test and red team exercise conducted against NRC's information or information systems from FY 2015 to present, or your attestation that no such test or exercise was completed.**

ANSWER

See: NONPUBLIC ENCL 3 ISD_FY15_Red_Team_Penetration_Test_Report_v1 1_20160324-wm.pdf.

- 7. Each certification you submitted to the Director of OMB or any committee of Congress pursuant to Section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015, and your assurance that you will provide the Committee a copy of any such certification you submit to the Director of OMB or any committee of Congress in the future.**

ANSWER

No such certifications currently exist or are expected in the future.

- 8. A list of major incidents, as identified in FISMA, at NRC—including any of its subordinate offices, components, and agencies—from October 30, 2015, to the date of your response, or your attestation that no major incidents occurred at NRC during that period.**

ANSWER

The NRC attests that no major incidents have occurred at the agency during the period identified.