March 28, 2008

The Honorable Norm Coleman
Ranking Member, Permanent Subcommittee
on Investigations
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Senator Coleman:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to your request for the status of the NRC's compliance with government-wide initiatives to protect Personally Identifiable Information (PII). Specifically, your questions focus on NRC compliance with the recommendations in the Office of Management and Budget (OMB) memoranda M-05-08, M-06-15, M-06-19, M-06-20, and M-07-16, as well as a timeline within which the NRC will have policies in place to implement the recommendations of OMB memorandum M-06-16. As detailed in the enclosure, the NRC has taken many significant steps to ensure protection of this sensitive information, has implemented almost all of the OMB recommendations, and is actively addressing the open items.

If you have any further questions, please contact me.

Sincerely,

/RA/

Dale E. Klein

Enclosure:
NRC's Status in Compliance with
Selected OMB Memoranda

Identical letter sent to:

The Honorable Norm Coleman
Ranking Member, Permanent Subcommittee
on Investigations
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

The Honorable Susan Collins
Ranking Member, Committee on
Homeland Security and Governmental Affairs
United States Senate
Washington, D.C. 20510

U.S. NUCLEAR REGULATORY COMMISSION
STATUS IN COMPLIANCE WITH SELECTED
OFFICE OF MANAGEMENT AND BUDGET MEMORANDA

M-05-08, February 11, 2005, Designation of Senior Agency Official for Privacy

This memorandum requested agencies to provide the Office of Management and Budget (OMB) with the name of the senior official who has the overall agency-wide responsibility for information privacy issues.

The U.S. Nuclear Regulatory Commission (NRC) designated the Deputy Chief Information Officer as the Senior Agency Official for Privacy in an email sent to OMB on March 18, 2005.

M-06-15, May 22, 2006, Safeguarding Personally Identifiable Information

This memorandum requested the designated Senior Agency Officials for Privacy to conduct a review of agency policies and processes, and take corrective action, as appropriate, to ensure adequate safeguards are in place to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information (PII). The results of the review were to be provided in the Fiscal Year (FY) 2006 annual Federal Information Security Management Act (FISMA) report. The memorandum also requested agencies to remind employees of their specific responsibilities for safeguarding PII and to ensure prompt and complete reporting of security incidents.

The NRC reminded its employees and contractors of their specific responsibilities for safeguarding PII in a June 22, 2006, agency-wide announcement entitled, "Safeguarding Personal Privacy Information." The NRC also reviewed its policies and processes and made appropriate modifications aimed at preventing misuse of or unauthorized access to PII. On October 6, 2006, in NRC's FY 2006 FISMA report, which included the Privacy Management Report, the NRC notified the Director, OMB, that the NRC had completed a review of NRC's physical and personnel security, and administrative and technical policies and processes related to the prevention of the intentional or negligent misuse of or unauthorized access to PII.

Although the NRC has been reporting security incidents according to OMB memoranda M-06-15, NRC does not have a formal written policy that requires this reporting. The NRC has drafted a new incident response policy that will be issued in the 3rd quarter of FY 2008 that will implement the OMB recommendation.

M-06-16, June 23, 2006, Protection of Sensitive Agency Information

This memorandum requested agencies to implement the National Institute of Standards and Technology (NIST) checklist for protection of PII that is either accessed remotely or physically transported outside of the agency's secured, physical perimeter. The memorandum also recommended encrypting data on all devices removed from agency facilities that contain sensitive information; allowing remote access to sensitive information systems only using two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; using a 30-minute timeout for remote access and mobile devices; logging all computer-readable data extracts from databases holding sensitive information; and verifying that each extract including sensitive data has been erased within 90 days or that its use is still required.

In response to M-06-16, on September 19, 2006, the NRC issued its policy entitled, "Protection of Personally Identifiable Information," that:

- Prohibits the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted;
- Prohibits staff from storing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices;
- Prohibits staff from using personally-owned computers for processing or storing PII of individuals pertaining to NRC official business other than themselves;
- Prohibits staff from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted;
- Restricts remote access to PII information on NRC systems by requiring two-factor authentication and enforcing a 30-minute timeout;
- Prohibits emailing of PII outside of NRC's infrastructure (except when necessary to conduct agency business); and
- Requires identification of extracts or outputs that contain PII and deletion of those not necessary, as well as logging and assessment of retention for future extracts/outputs.

This policy implements the NIST checklist for protection of PII that is either accessed remotely or physically transported outside of the NRC's secured, physical perimeter. This policy also implements the other recommendations contained in M-06-16 for protection of PII.

The NRC adopted an additional policy on February 7, 2008, to further protect sensitive information. This policy prohibits employees from processing sensitive information on home personal computers unless the employee is using NRC's CITRIX Broadband Remote Access System. Employees are also prohibited from storing sensitive information on a home computer. Employees may process sensitive information at home on an NRC-issued laptop that is encrypted using NRC-approved encryption software.

Although the NRC currently implements 30-minute or less timeouts for remote access sessions and mobile device access, NRC has not issued a formal written policy addressing this issue. The NRC will issue a written timeout policy in the 3rd quarter of FY 2008.

The NRC is currently examining methods to enable encryption of certain sensitive information transmitted outside of NRC's infrastructure prior to transmission and decryption by the recipient to ensure adequate protection of sensitive information transmissions. After completion of the technology examination, the NRC will develop a policy and implementation timeline that is consistent with government-wide efforts in this area.

The NRC is developing a written policy requiring encryption of NRC sensitive information removed from NRC facilities on mobile devices and expects to implement this policy in the 1st quarter of FY 2009.

The NRC is developing a written policy requiring logging all computer-readable data extracts from databases holding sensitive information and erasure of the information within 90 days or documentation of the need to retain the data extract for a longer period of time. The policy is expected to be issued in the 4th quarter of FY 2008; however, full implementation will be delayed until October 2011 to enable implementation of technological aids to assist in complying with this requirement.

New systems that provide for remote access to information with a sensitivity of "high," such as the National Source Tracking System, are being deployed requiring that the user have an NRC issued digital certificate on a separate hard token to gain access to the system.

The NRC is scheduled to implement HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, for physical access to NRC facilities in October 2010. Logical access to NRC systems and sensitive information will be incorporated into the identity cards by October 2011. Accordingly, NRC plans to require that all remote access to NRC sensitive information employ two-factor authentication where one of the factors is a device separate from the computer gaining access by October 2011.

M-06-19, July 12, 2006, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

This memorandum requests agencies to report all incidents (either electronic or physical form) involving PII to US-CERT within one hour of discovering the incident and should not distinguish between suspected and confirmed breaches. This memorandum also reminded agencies that security and privacy requirements should be included within agency information technology investments and that steady-state system operations meet existing security requirements before new funds are spent on system development, modernization, or enhancement. In addition, the memorandum requested agencies to identify the specific funds being requested for proposed development, modernization, or enhancement efforts to correct security significant isolated or wide-spread weaknesses identified by the agency Inspector General or the Government Accountability Office (GAO) and weaknesses identified during privacy program reviews.

The NRC has drafted a new incident response policy that will be issued in the 3rd quarter of FY 2008 which will codify our current practice and require the reporting of incidents (either electronic or physical form) involving PII to US-CERT within one hour of discovering the incident, regardless of whether the breach is suspected or confirmed.

The NRC currently requires identification of security and privacy requirements as part of NRC's Capital Planning and Investment Control process. NRC will issue a written policy addressing this process in the 3rd quarter of FY 2008.

The NRC is ensuring that operational systems meet applicable security requirements for security-significant isolated or wide-spread weaknesses identified by the agency Inspector General or the GAO. NRC will issue a written policy on these issues in the 3rd quarter of FY 2008.

M-06-20, July 17, 2006, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.

This memorandum requested agencies to include in their FY 2006 annual FISMA report: the results of the Senior Agency Official for Privacy's review per OMB memorandum M-06-15; the

agency's Inspector General's list of systems missing from the agency's inventory of major systems; quarterly updates of privacy updates to be submitted with the President's Management Agenda scorecard; and identification of physical or electronic loss of PII.
The NRC's submission of the NRC FY 2006 annual FISMA report included this information with the exception of scorecard information. The NRC is not a scorecard agency and does not provide quarterly scorecard updates.

M-07-16, May 22, 2007, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

This memorandum requested agencies to develop and implement a PII breach notification policy and to establish a plan in which agencies would eliminate the unnecessary collection and use of social security numbers.

The NRC issued on September 19, 2007, "U.S. Nuclear Regulatory Commission Personally Identifiable Information Breach Notification Policy," and the "U.S. Nuclear Regulatory Commission Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers." NRC employees were notified of these policies via an agency wide announcement on that date. These policies are publicly available on the NRC's Web site at: http://www.nrc.gov/site-help/privacy.html#ssn.