NRC'S RESPONSE TO QUESTIONS CONTAINED IN A LETTER FROM THE HONORABLE ADAM H. PUTNAM CHAIRMAN, SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS UNITED STATES HOUSE OF REPRESENTATIVES DATED MARCH 17, 2004

Question 1. **Getting senior program officials to take accountability for the mission systems they control is a recurring theme in OMB's FISMA report. Have you found the certification and accreditation process which requires the program official to sign off on the risk level any help with this?**

Answer: Yes, the certification and accreditation process has helped to get senior program officials to take accountability for the mission systems they control. This is accomplished by providing high level visibility to the risk level associated with mission systems which may not have been identified outside of the certification and accreditation process. This visibility provides senior program officials with an awareness of the risks associated with mission systems, the opportunity to follow up on actions being taken to control risks, and provides senior management with leverage to ensure senior program officials are taking the appropriate steps to control these risks.

Question 2. **How does your agency ensure that the information you report for FISMA accurately reflects the status and quality of information security at your agency?**

Answer: NRC accomplishes this through several mechanisms. The NRC has a dedicated Computer Security staff that performs oversight activities, including an independent review of all security documentation, capital planning information, system penetration testing, and innovative ideas such as independent security control evaluation to ensure accurate and complete information. The agency head and the CIO utilize a central tracking system to track all system information such as the status of security plans, security testing, system weaknesses and corrective actions, and all other security activities associated with systems security certification and accreditation. The agency head and the CIO ensure that new systems cannot be placed into operation, and major system upgrades cannot be completed, until they have completed the security activities and milestones required to attain systems security accreditation. In addition, the NRC's Office of Inspector General performs an independent assessment of the overall computer security program on an annual basis.

Question 3. **Several witnesses testified that moving FISMA reporting to align with financial reporting would be helpful. What are your thoughts on this proposal?**

Answer: NRC believes the date should remain the same to ensure the ability to compare results from year to year.