RESPONSES FOR THE SUBCOMMITTEE

1) To improve our understanding of your agency's current progress, please provide a copy of your agency's plan of action and milestones (POA&M) that you submitted to the Office of Management and Budget (OMB).

NRC Response: OMB requested that agencies provide an updated POA&M with the second quarter report that was submitted on April 1, 2003. A copy of the POA&M that was submitted to OMB with the NRC second quarter report is attached.

2) The Subcommittee is seeking confirmation that individual department CIOs have been assigned the appropriate and necessary authority to ensure effective and accountable information security throughout the agency. Please describe the present authorities assigned to the department CIO regarding the ability to ensure effective information security, including:

- Establishing and enforcing department-wide information system security policies, protocols and procedures;

  NRC Response: The NRC CIO is designated in agency policy as having responsibility and authority to develop, manage, and implement policies and procedures for the agency-wide automated information system security program. As the Designating Accrediting Authority (DAA) for agency information systems, the CIO reviews and approves all system risk assessment results, security plans, and information system contingency plans.

- Approval of IT investments, including proposed investments in information security;

  NRC Response: The NRC CIO has responsibility and authority for implementing the agency-wide information technology (IT) capital planning and investment control (CPIC) policies, processes, and procedures. The CIO reviews and approves all IT investments including proposed investments in information security, referring those IT investments having a project cost greater than $500,000 to the Chairman for approval.

- Managing the activities of component (e.g., bureau) CIOs;

  NRC Response: The NRC does not have any component organizations with their own CIOs.

- Regular monitoring of the security of all department systems and network;

  NRC Response: NRC has an integrated network and security management program to protect NRC information and systems, and to monitor, detect and respond to anomalies that may indicate computer and network intrusions or misuse. Security is ensured by comprehensive controls for access, well-protected network boundaries to prevent intruders, and an ongoing program for monitoring and testing systems for security deficiencies. NRC's access to the Internet is protected by a firewall, and e-mail traffic is screened using anti-virus software. Agency workstations and servers are protected by anti-virus software that is updated periodically. NRC logs and audits network and system activity and uses intrusion detection systems to monitor for intrusions or misuse. The agency has a comprehensive program that uses recognized standards to ensure the security of systems as they are planned, developed and operated; it employs standard security bench marking tools to verify the security of systems on an ongoing basis.

- Establishment and routine updates of department business continuity plans;

  NRC Response: Business continuity plans and IT contingency plans are in place for all agency major applications and general support systems. Agency information security policy requires that these plans be reviewed and tested annually.

- Ensuring appropriate information security staffing and ongoing commitment to training throughout the department;

  NRC Response: NRC has implemented two new online information security training courses. All employees are required to annually complete a computer security awareness course. Individuals in positions with significant security responsibilities, including all of the NRC information systems security officers (ISSOs), are required to complete an ISSO course which provides more in depth technical training. NRC continues to pursue the hiring of information systems security technical professionals in order to supplement our capabilities in this critical area.

- Ensuring the appropriate level of security awareness, including adherence to policies, protocols, and procedures, throughout the department.

  NRC Response: All employees are required to annually complete the new online computer security awareness course. NRC conducts an annual Computer Security Day each November. All new employees receive initial orientation that includes computer security awareness training. The Office of the Chief Information Officer (OCIO) distributes computer security awareness brochures, posters, and other materials.

3) FISMA requires each agency develop, under the CIO, a senior agency information security officer (CISO). Please advise the Subcommittee of the following:

- When the position was established and when it will be filled;

  NRC Response: NRC established an agency Senior Information Technology (IT) Security Officer position in 2002. The position was filled in May 2002.

- Where the position presently is located on the organization chart and to whom the position reports;

  NRC Response: The Senior IT Security Officer (SITSO) is in the Office of the Chief Information Officer and reports directly to the CIO.

- What authority, responsibility, and accountability has been assigned to this position;

  NRC Response: On behalf of the CIO, the SITSO is responsible for the management of the agency-wide automated information security program and policies, ensuring the agency's security program integrates fully into the agency's enterprise architecture and capital planning and investment control processes.

- If the position has not been created or filled, please explain the circumstances and the timeframe for addressing the matter

  NRC Response: The position has been established and was filled in May 2002.

As the Subcommittee is committed to a federal government with secure and protected information systems, we are requiring that you provide the Subcommittee with a quarterly report on your progress in identifying and mitigating your security vulnerabilities, and fulfilling your POA&M. These reports may be filed at the same time as the quarterly reports required by OMB. Please include in the report:

- Actions taken;

- Updated POA&M;

- Explanations and details as to how actions taken correspond to the POA&M;

- Listing and discussion of any current material weaknesses related to information security;

- Discussion of any outstanding impediments to achieving secure information systems.

  NRC Response: The NRC was required to submit the third quarterly FISMA status report to OMB on July 1, 2003. A copy of that report is attached, along with an updated POA&M.

Finally, we are requesting that you provide us with a summary of how you are integrating information security management into your enterprise architecture. Please provide us with a narrative that details your efforts to ensure that managing information security risk is a part of your enterprise architecture.

NRC Response: The NRC has developed new management directives that describe a Full Capital Planning and Investment Control (CPIC) Life Cycle for IT Investments that includes Research, Selection, Control, and Operations / Evaluation phases. Enterprise Architecture includes security as a component of each CPIC phase with greatest emphasis during the evaluation and approval process in the Selection, Control, and Operations / Evaluation phases. Security Risks and Security Plans are reviewed and evaluated during each of these phases broadening agency accountability for security and further ensuring that NRC information security plans are up-to-date and practiced throughout the full life cycle of each agency system.