July 28, 2005

The Honorable Tom Davis, Chairman
Committee on Government Reform
United States House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

On behalf of the U.S. Nuclear Regulatory Commission (NRC) and in accordance with 31 U.S.C. 720, I hereby submit our responses to the recommendations made by the U.S. Government Accountability Office (GAO) in its report entitled "Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks" (GAO-05-0471). Specific responses to the GAO recommendations are enclosed.

Sincerely,

/RA/

Nils J. Diaz

Enclosure:
NRC Responses to GAO Recommendations

cc: Representative Henry Waxman

Identical letter sent to:

The Honorable Tom Davis, Chairman
Committee on Government Reform
United States House of Representatives
Washington, D.C. 20515
cc: Representative Henry Waxman

The Honorable Susan Collins, Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510
cc: Senator Joseph I. Lieberman

The Honorable George V. Voinovich, Chairman
Subcommittee on Clean Air, Climate Change,
and Nuclear Safety
Committee on Environment and Public Works
United States Senate
Washington, D.C. 20510
cc: Senator Thomas Carper

The Honorable Ralph M. Hall, Chairman
Subcommittee on Energy and Air Quality
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515
cc: Representative Rick Boucher

The Honorable Joe Barton, Chairman
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515
cc: Representative John D. Dingell

The Honorable James M. Inhofe, Chairman
Committee on Environment and Public Works
United States Senate
Washington, D.C. 20510
cc: Senator James M. Jeffords

The Honorable David M. Walker
Comptroller General of the United States
Government Accountability Office
Washington, D.C. 20548

The Honorable Joshua B. Bolten, Director
Office of Management and Budget
Washington, D.C. 20503

NRC Responses to GAO Recommendations, GAO-05-0471,
Internet Protocol Version 6: Federal Agencies Need to Plan
for Transition and Manage Security Risks

Background

On May 24, 2005, the Government Accountability Office (GAO) issued a report on Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks (GAO-05-0471). This report discusses the key issues surrounding Internet Protocol Version 6 (IPv6) and the security considerations for the transition to IPv6 for federal agencies. GAO expressed concern about poorly configured and unmanaged IPv6 capabilities within federal agencies. GAO recommends in the report that agency heads take action to address near term security risks, including determining what IPv6 capabilities they may have and initiate steps to ensure they can control and monitor IPv6 traffic.

Recommendations and Responses

Nuclear Regulatory Commission's (NRC's) responses to GAO's recommendations to Office of Management and Budget (OMB) appear below.

Recommendation 1 to OMB

Instruct Federal agencies to begin addressing key IPv6 planning considerations, including:

- developing inventories and assessing risks,
- creating business cases for the IPv6 transition,
- establishing policies and enforcement mechanisms,
- determining costs, and
- identifying time lines and methods for transition, as appropriate.

Response

NRC has a three phase approach to planning for and implementing IPv6. Phase one, which has already begun, emphasizes the agency's business drivers and goals for the IPv6 transition. This phase will identify the risks and benefits as a result of the transition to IPv6. From this development process, the agency's strategy will be refined to determine the alignment of the technology with the NRC business goals. The expected completion of phase one is September 2005.

Phase two of the agency's strategy will include a readiness assessment to identify the existing NRC technology baseline for IPv6. This baseline assessment will include a careful review of all planned and scheduled information technology (IT) acquisitions. The baseline will also be used to determine the IPv6 transition prioritization criteria for existing investments at various stages of their life cycle. Phase two of NRC's strategy is expected to start in September 2005 and be completed in November 2005.

Phase three is the implementation phase of the IPv6 strategy. It will provide a transition plan that will take into account specific agency enterprise-wide and individual IT investments. This phase is expected to start in October 2007 and be completed in September 2009.

NRC's three-phased strategy for the implementation, management, and investment in IPv6 technologies will address the development of inventories for current IT investments and planned acquisitions as part of the second phase. Based upon the inventory baseline, the risks associated with the implementation of the technology will be assessed.

With respect to the creation of business cases for the IPv6 transition, the agency's strategy is to identify the business drivers for migration from the current Internet Protocol Version 4 (IPv4) to IPv6, to ensure the transition provides value in achieving the agency's business goals, and to ensure that the technology will integrate with the agency's EA.

In phase three of the agency's strategy, the NRC will identify any specific IT, procurement, or other policy documents requiring modification to provide the necessary IPv6 transition support to effectively promulgate the OMB IPv6 guidance within the agency. The agency will include an appropriate clause enforcing IPv6 compatibility in agency IT acquisitions and has factored into agency resource planning the need to transition to IPv6.

IPv6 Framework Phase	Estimated Start Date	Estimated Completion Date
I - Strategic Planning	1/05	9/05
II - IPv6 Readiness Assessment	9/05	11/05
III - Implementation	10/07	9/09

Recommendation 2 to OMB

Agency heads take immediate actions to address the near-term security risks, including determining what IPv6 capabilities they may have, and initiate steps to ensure that they can control and monitor IPv6 traffic.

Response

The agency's current IT infrastructure is only configured to support IPv4-formatted traffic. Consequently, there are no current IPv6 capabilities and no near term security risks. The agency will address the management and monitoring of IPv6 traffic in the development of agency policy and governance as IPv6 is incorporated into NRC's infrastructure.