June 3, 2004

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

Dear Mr. Chairman:

Pursuant to 31 U.S.C. 720, I am pleased to provide, on behalf of the U.S. Nuclear Regulatory Commission (NRC), our statement of the actions taken and plans in response to the recommendations made by the U.S. General Accounting Office (GAO) in its report entitled "INFORMATION TECHNOLOGY MANAGEMENT: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved" (GAO-04-49). GAO released this report to the public in February 2004.

We have reviewed GAO-04-49 and agree with GAO's recommendations for improving NRC's information technology management. We have already taken steps to implement the recommendations and believe our plans and actions meet the intent of the GAO recommendations. The enclosure to this letter provides our responses to the specific recommendations.

If you have any questions or comments on our written statement, please contact me.

Sincerely,

/RA/

Nils J. Diaz

Enclosure:
Actions and Comments on Report
Recommendations GAO-04-49

cc: Representative Henry A. Waxman
L. Lambert, GAO
D. Powner, GAO

Identical letter sent to:

The Honorable Thomas Davis
Chairman, Committee on Government Reform
United States House of Representatives
Washington, D.C. 20515
cc: Representative Henry A. Waxman
L. Lambert, GAO
D. Powner, GAO

The Honorable Susan M. Collins
Chair, Committee on Governmental Affairs
United States Senate
Washington, D.C. 20510
cc: Senator Joseph I. Lieberman
L. Lambert, GAO
D. Powner, GAO

ACTIONS AND COMMENTS ON GAO REPORT RECOMMENDATIONS
Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved
January 2004
(GAO-04-49)

The General Accounting Office (GAO), in its report, "Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved," made several recommendations with respect to improving the Nuclear Regulatory Commission's (NRC's) Information Technology (IT) strategic planning and performance measurement processes. The recommendations and the NRC's responses are provided below.

Recommendation 1

To improve the agency's IT strategic planning/performance measurement processes, we recommend that the Commissioners of the Nuclear Regulatory Commission:

! document the agency's roles and responsibilities for its IT strategic management processes and how IT planning is integrated with its budget and human resources planning;

Response:

The U.S. Nuclear Regulatory Commission (NRC) has developed a process for establishing an NRC Strategic Plan which is on a 3-year cycle. The Commissioners are actively engaged in the development of the Strategic Plan, including the development of strategic goals and objectives. In response to the strategic plan goals and performance objectives, offices develop their individual plans for IT investments that support their goals and performance objectives.

Additionally, the NRC's Office of the Chief Information Officer (OCIO) has published management directives which establish the IT investment planning and decisionmaking policies and processes, including roles and responsibilities at the agency. NRC Management Directive 2.2, "Capital Planning and Investment Control" describes the process, roles, and responsibilities for justification and approval of IT investments. Approved IT investments are managed using the OCIO's System Development Life Cycle Management Methodology (SDLCMM), which is described in NRC Management Directive 2.5 and will be issued in FY 2004.

Table 1 summarizes the roles and responsibilities described in these management directives. The NRC has established special governance committees, councils, and groups with specific roles and responsibilities in the capital planning and investment control (CPIC) and SDLCMM processes–the NRC IT Governance Framework (Table 2).

The Agency IT Governance Framework is a four-tiered approach to planning and managing agency IT investments. The framework documents the roles, responsibilities, and authorities of its IT investment management boards. The first tier, the IT Focus

Group, draws its membership from program office staff and is chaired by an OCIO manager. This group is responsible for identifying business areas where technology can be used to solve business problems and more effectively and efficiently accomplish business objectives. The second tier, the agencywide IT Business Council (ITBC), consisting of division-level managers, is focused on the business needs of the agency. It is chaired by a group member. The ITBC provides input on the alignment of new IT investments with current applications, practices, and business needs. The third tier, the IT Senior Advisory Council, consisting of office-director-level membership, provides strategic direction on major IT initiatives and prioritizes the agency IT investments to more effectively manage the agency IT investment portfolio. It is chaired by the Chief Information Officer (CIO). The top tier, the Program Review Committee (PRC), reviews office budget submissions for consistency with agency performance goals, measures, policy guidance, and planning assumptions. The CIO briefs the PRC on the agencywide IT budget.

The CPIC process is used to establish a portfolio of approved major IT investments. The CPIC process requires identification of the NRC strategic goal(s) addressed by each major investment and the human resource requirements. The CIO reviews each investment submitted through CPIC to ensure that it is aligned with the NRC Strategic Plan goals and objectives and consistent with the agency's draft Information Resources Management (IRM) Plan and Enterprise Architecture Blueprint. The OCIO maintains the enterprise view of the IT investments. The PRC approves the agencywide IT budget as part of the overall budget approval process. The IT budget is reviewed by the Chairman and Commissioners as a part of the overall budget approval process.

Human resource planning is integrated with IT planning through the agency's Human Resources (HR) organization's Strategic Workforce Planning program using the Office of Personnel Management's five steps of workforce planning: 1) set strategic direction; 2) analyze workforce, identify skill gaps; 3) develop action plan; 4) implement action plan; and 5) monitor, evaluate, and revise action plan. In addition, the OCIO has recruited a Senior Program Analyst (Educational Outreach) who will serve as a Human Capital expert for IT human resource needs. The role of the Human Capital expert will be to assist the OCIO in continuing to analyze and address skill gaps between the agency's human resources and its planned IT investments.

! include in the department's annual performance plan the resources and time periods required to implement the information security program plan required by the Federal Information Security Management Act (FISMA);

Response:

The NRC's annual performance plan includes output measures which capture the activities needed for compliance with FISMA. NRC submits OMB Exhibit 53, *Information Technology and E-Government* to the Office of Management and Budget (OMB). The Exhibit 53 provides information on agencywide IT resources, and identifies security resources for each system, which are included in NRC's annual performance plan. The NRC submits OMB Exhibit 300s, *Capital Asset Plan and Business Case* for all major applications. In Section II.B. of the Exhibit 300, IT security is addressed for each major system. Additionally, the NRC's FISMA plan of action and milestones (POA&M) addresses current IT security resources, gaps, and plans to close the gaps.

We consider this part of Recommendation 1 to be closed.

! develop a documented process to assign roles and responsibilities for achieving its enterprisewide IT goals;

Response:

The NRC has an IT Governance Framework (Table 2) which describes the roles and responsibilities for approval of IT programs and projects. The roles and responsibilities are documented in Management Directive 2.2, "Capital Planning and Investment Control," a revision of which was issued in January 2004 and Management Directive 2.5, "System Development Life Cycle Management Methodology," which will be issued in FY 2004.

The agency is continuing to develop an Enterprise Architecture Blueprint and an IRM Strategic Plan that describe our enterprisewide IT goals. It is the OCIO's role to ensure that IT programs that are approved are consistent with these goals. The review process for IT programs required by Management Directive 2.2 includes an Enterprise Architecture review by OCIO to determine whether programs are aligned with the goals in the IRM Strategic Plan and the Enterprise Architecture Blueprint prior to CIO approval.

! develop performance measures related to the effectiveness of controls to prevent software piracy;

Response:

As part of seat management implementation, NRC developed a baseline of licensed software installed on agency computers. This baseline is updated as system configurations change. In January 2003, we began monthly software monitoring to ensure ongoing compliance with licensing requirements. On a monthly basis, the software found on randomly selected computers is compared to the database of software licensed for each computer, and any unlicenced software is removed. Performance measures related to the effectiveness of controls to prevent software piracy will be included in the NRC IRM Strategic Plan in FY 2004.

In addition, our computer security awareness training and educational program include special training to all new employees, and an annual on-line awareness course for all employees and contractors covers piracy, bootlegging, and copyright protection of software. This information is further stressed in our continuous agencywide poster campaign and in annual activities for computer security awareness day.

! develop performance measures for the agency's enterprise goals in its IRM plan, and track actual-versus-expected performance for these measures.

Response:

In 2004, the enterprisewide IRM Strategic Plan for the NRC will be developed, approved, and implemented. In 2005, the IRM Strategic Plan will be aligned with the agency's enterprise goals and will indicate the IT strategies that will be implemented to contribute to achieving the performance measures and the targets for those goals.

Major IT investment cost, schedule, and performance goals will be included, along with plans for major IT investments that deviated from cost, schedule, or performance goals.

Recommendation 2

To improve the agency's IT investment management processes, we recommend that the Commissioners of the Nuclear Regulatory Commission:

! include a description of the relationship between the IT investment management process and the department's other organizational plans and processes and its enterprise architecture, and identify external and environmental factors that influence the process in the agency's IT capital planning and investment control policy;

Response:

The IT investment management process uses information derived from NRC's Planning, Budgeting, and Performance Management Process and the agency strategic planning process. Performance measures that support the information technology and investment management goals in the NRC Strategic Plan have been developed and are used internally for both focused program evaluations and ongoing organizational monitoring. Specific metrics address the factors most appropriate to each program and investment. The IT investment management process employs broad overall "value" performance measures. Investment value measures relate to strategic alignment, financial management goals, productivity and efficiency, quality, enterprise architecture and security, timeliness, and customer or programmatic benefit. Investment project managers perform a risk analysis for each potential major IT investment. Specific risk concerns that cut across all IT investments, such as level of definitional risk, external or environmental risk, and use of iterative project development procedures, are beginning to be addressed through a standardized methodology. NRC is currently acquiring contract support to formalize and refine these broad measures into a portfolio management program that will be utilized for all IT investments and is expected to be operational in FY 2006. NRC is also supplementing existing practices by using the Federal Enterprise Architecture (FEA) Performance Reference Model metrics to help measure the performance of major IT initiatives and assess their contribution to NRC program performance. NRC conducts annual performance reviews and performance evaluations and assessments and summarizes results in the annual Budget/ Performance Plan.

NRC Management Directive 2.2, "Capital Planning and Investment Control," requires that major IT investments comply with the NRC enterprise architecture. Compliance with the NRC enterprise architecture is also mandated in Management Directive 2.1, "Information Technology Architecture." NRC is taking the steps necessary to improve its current management directives and fully integrate its IT investment management processes. NRC capital planning and investment control, enterprise architecture, the infrastructure development process, the systems development life cycle management methodology, and security processes are central IT investment processes. These processes are now being integrated into a single, documented IT investment management process that will provide standard operating procedures with significant events and decision points outlined throughout an IT initiative's life cycle. This new methodology will be called the Project Management Methodology (PMM). Current plans

are to make the PMM available to all NRC staff as a new management directive with accompanying handbook during FY 2006.

External and environmental factors such as new legislation may impact the IT investment management process by requiring the addition of new controls or compliance checks, but we do not believe such changes will impact NRC's IT Governance Framework or the IT strategic management planning process.

! develop work processes and procedures for the agency's investment management boards;

Response:

We are in the process of developing work processes and procedures for our investment management boards. We will continue to refine roles and responsibilities for our IT strategic management processes as we gain more experience. Specific details of these procedures will be defined in conjunction with the board members as we refine our proposed Project Management Methodology (PMM), which will integrate capital planning and investment control, enterprise architecture, security, the infrastructure development process, and the systems development life cycle management methodology. The PMM will be completed during FY 2006 and will serve as a new, integrated policy, with accompanying handbook supplemented by web-based standard operating procedures, which will document our processes for aligning and coordinating NRC IT investment decision making.

To date, the NRC has developed the Agency Information Technology Governance Framework, which provides a high-level outline of our board processes. See Table 2. The Agency IT Governance Framework is a four-tiered approach to planning and managing agency IT investments. The framework is described in our response to recommendation 1, bullet 1.

! implement a standard, documented procedure to maintain its IT asset inventory, and develop a mechanism to use the inventory as part of managerial decision making;

Response:

The NRC is currently developing a standard, documented procedure to ensure the update and maintenance of its IT asset inventory. The procedure to be followed will be documented in the Project Management Methodology (PMM) standard operating procedures, which will delineate specific processes to be followed to ensure that timely and repeatable updates occur. We currently have a baseline IT applications inventory that has been migrated to the System Architect toolset. We have made selected asset inventory reports available on our Intranet. We currently maintain an on-line inventory database of IT infrastructure hardware and commercial off-the-shelf software. This database will feed into the System Architect tool that maintains the applications layer of our enterprise architecture. The information in our IT asset inventory is now used in IT investment decision making. However, we expect to leverage this information within our portfolio management program that will become operational during FY 2006, thus establishing better linkage to managerial decision making. We plan to utilize reports from this toolset to better enable IT investment duplication checks and better support the managerial selection of IT investments.

! develop a structured IT investment management selection process that includes project selection criteria, a scoring model, and prioritization of proposed investments; and

Response:

The recent update to NRC Management Directive 2.2 on CPIC has a structured IT investment management selection process that includes project selection criteria based on a three-tier investment model. Tier 3 payments are approved by the sponsoring office director (less than $500,000). Tier 2 payments are approved by the CIO ($500,000 to $1,500,000). Tier 1 payments are approved by the EDO (greater than $1,500,000). We are further refining the CPIC management directive and related processes to include standard operating procedures specifying an investment scoring model that will address different measures at each stage of the life cycle. As we move forward and complete our PMM and implement our IT investment portfolio management program, we will have developed an IT selection and prioritization process, integrated with our financial and program management processes, which will better address all appropriate scoring criteria at each stage and investment tier. Within our portfolio management program, we will identify and evaluate IT investment measurement, review, and improvement processes, compare investment performance to targets and benchmarks and conduct reviews. We will categorize and prioritize our investments and continue to execute improvement plans when our managerial oversight processes indicate that an ongoing project is not realizing desired cost, benefit, or schedule results. We expect to have the early phases of both PMM and portfolio management operational during FY 2006.

! document the role, responsibility, and authority of its IT investment management boards, including work processes and control, and evaluate processes that address the oversight of IT investments, such as what is outlined in practices 2.15, 2.16, 2.17, and 2.18.

Response:

We are currently developing a streamlined and integrated set of instructions for managing the design, development, operation, maintenance, and decommissioning of information technology investments. The process is tentatively called “Project Management Methodology” (PMM), and it will provide a framework for improving agency IT investment management processes. PMM will address policies and procedures heretofore separately covered in agency policies and procedures for capital planning and investment control, enterprise architecture, security, infrastructure development process model, and systems development life cycle management methodology. Both the PMM and our IT investment portfolio management program will provide the foundation and information necessary to provide better managerial oversight of our IT investments. We are already working to fully establish and document our Agency IT Governance Framework (Table 2) that delineates roles and responsibilities.

As we develop this new integrated set of instructions and establish improved policies, NRC intends to adopt the most applicable IT investment management best practices made available through GAO/AIMD-10.1.23, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, as well as other sources. Best practices that best fit the agency will be utilized in conjunction with our existing Planning, Budgeting, and Performance Management Process to better

address the oversight of IT investments, such as what is outlined in practices 2.15, 2.16, 2.17, and 2.18. The new PMM instructions will fully address information technology investments throughout the life cycle with appropriate evaluations taking place at each stage. Our portfolio management program will provide a much improved oversight mechanism that will better enable managerial decision making, corrective actions, verification and validation of projects, etc. Our goal is to have the first phases of our improved IT investment management policies and processes operational during FY 2006.

Roles and Responsibilities for IT Strategic Management Processes

	Program Review Committee	IT Senior Advisory Council	IT Business Council	IT Focus Group	Com-mis-sion	EDO	CIO	CFO	OHR	Other Offices
Develop NRC Strategic Plan					X	X	X	X	X	X
Review office (IT) budget submission for consistency with Agency performance goals, metrics, policy guidance, and planning assumption.	Deputy Executive Director, CIO, Deputy CFO, and one Regional Administrator									
Provide strategic direction on major IT initiatives and prioritize agency IT investments to more effectively manage the Agency IT investment portfolio.		Office Directors				X	X	X	X	X
Provide input on the alignment of new IT investments with current applications, practices, and business needs.			Division Level				X	X	X	X
Identify Business areas where technology can be used to solve business problems and more effectively and efficiently accomplish business objectives.				Branch/ Staff			X	X	X	X
CPIC	X	X	X			X	X	X	X	X
EA: IRM Strategic Plan			XX				X	XX	XX	XX

XX = Future process

Table 1

Agency IT Governance Framework

	Program Review Committee (PRC)	IT Senior Advisory Council Chair: CIO	IT Business Council Chair: Member	IT Focus Group Chair: Business Process Improvement And Application Division
Members	Deputy Executive Director, CIO, Deputy CFO, and one Regional Administrator	Office Director	Division Level	Branch/Staff
Meeting Frequency	Annually	Semi Annual	Monthly [As Needed]	Quarterly
Purpose	Review office budget submissions for consistency with Agency performance goals, metrics, policy guidance, and planning assumptions. Recommend funding levels to the EDO, CFO, and Commission.	Provide strategic direction on major IT initiatives and prioritize agency IT investments to more effectively manage the Agency IT investment portfolio.	Provide input on the alignment of new IT investments with current applications, practices and business needs.	Identify business areas where technology can be used to solve business problems and more effectively and efficiently accomplish business objectives.
				
Level	Agency Budget	Executive	Business	Customer

Prioritization:

1-essential to day-to-day operations

2-Nice to have

3-Discretionary

Table 2