**UNITED STATES
NUCLEAR REGULATORY COMMISSION**
WASHINGTON, D.C. 20555-0001

September 28, 2018

Ms. Carol C. Harris, Director
Information Technology Acquisition
   Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am writing to provide the agency's response to the U.S. Government Accountability Office's (GAO's) report "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93." Having reviewed the final report, the NRC maintains that the requirements in the agency's organizational legislation and established agency policies support our approach to information technology leadership and accountability, workforce, and investment management. A detailed response to the report is enclosed.

If you have any questions or need additional information, please contact Mr. John Jolicoeur by telephone at (301) 415-1642 or by e-mail at John.Jolicoeur@nrc.gov.

Sincerely,

Kristine L. Svinicki

Enclosure:
NRC Response to GAO-18-93

Response to the U.S. Government Accountability Office's Final Report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93," Recommendation 23

Recommendation 23 in this GAO report states: "The Chairman of the Nuclear Regulatory Commission should ensure that the agency's IT management policies address the role of the CIO for key responsibilities in the five areas we identified."

The NRC's comments on each of the five areas are as follows:

Information Technology (IT) Leadership and Accountability

- **Report directly to the agency head or that official's deputy.** The U.S. Nuclear Regulatory Commission (NRC) is fully compliant with this requirement. NRC-specific organizational legislation (Reorganization Plan No. 1 of 1980) assigns the agency's "administrative functions" to the Chairman and then requires the Chairman to delegate them to the Executive Director for Operations (EDO). The NRC's Chief Information Officer (CIO) reports directly to the EDO, who serves as the Chief Operating Officer (COO). The CIO also has direct access to the Chairman. This is consistent with the requirements in Element Q1 of the Federal Information Technology Acquisition Reform Act Common Baseline.

IT Strategic Planning

- **Benchmark agency processes against private and public sector performance.** The NRC performance management process adheres to the agency's policies:

  - Management Directive (MD) 6.9, "Performance Management," dated August 15, 2016

  - MD 6.10, "Strategic Planning," dated August 15, 2016

  The NRC has leveraged private and public sector resources provided by the Project Management Institute to inform process improvements. In addition, the NRC has identified benchmarks for analysis to inform the agency's fiscal year (FY) 2020 IT/information management (IM) performance plan. The NRC also plans to describe the CIO roles and responsibilities for benchmarking in the next revision of the agency IT/IM Strategic Plan, due in the first quarter of FY 2019, in order to bring NRC into full compliance.

- **Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments.** The NRC is fully compliant with this requirement. Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview, Version 2.1, issued December 2017 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML17346A193), includes the following among the responsibilities of the CIO:

  > Develop and implement an agencywide framework that includes policies, processes, and procedures for IT investment management, strategic planning and EA [Enterprise Architecture], information and records management, and information security that supports the NRC's mission, meets the requirements of Federal statutes and regulations and guidance

from OMB [Office of Management and Budget] and GAO [Government Accountability Office], and is consistent with the NRC's overall PBPM [Planning, Budgeting, and Performance Management] programs.

Jointly with the CFO [Chief Financial Officer] and executive-level IRB [Investment Review Board], provide an executive IT investment review function as required by OMB, make decisions on the IT portfolio, and recommend the IT budget to the EDO for consideration in the NRC's overall budget.

IT Workforce

- **Assess annually the requirements established for agency personnel regarding IT management knowledge and skills.** The NRC is partially compliant with this requirement. Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML17346A193) includes the following among the responsibilities of the CIO:

  > Jointly with the CHCO [Chief Human Capital Officer], develop a set of competency requirements for IT and IT acquisition staff (including IT and IT acquisition leadership positions) and develop and maintain a current workforce planning process to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.

  The NRC also recently reissued MD 12.5, "NRC Cybersecurity Program," dated November 2, 2017 (ADAMS Accession No. ML17278B085), to specifically define these CIO responsibilities.

  The NRC has initiated an enhanced Strategic Workforce Planning (SWP) process to develop strategies and action plans that enable the NRC to recruit, retain, and develop a skilled and diverse workforce with the competencies and agility to address emerging needs and workload fluctuations. The SWP process takes place on an annual cycle and results in strategies to address workforce needs in both budget execution year +1 and budget execution year +5.

  The enhanced SWP process leverages existing agency processes for strategic planning, staffing, budget formulation, performance management, and training and development. Implementation of the SWP process also addresses the agency requirement for IT management knowledge and skills.

  The NRC will update applicable guidance to include IT workforce CIO authorities by the end of the second quarter of FY 2020 in order to bring NRC into full compliance.

- **Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements.** The NRC is partially compliant with this requirement. Page 24 of the NRC's Capital Planning and Investment Control Policy (ADAMS Accession No. ML17346A193) states that it is the responsibility of the CIO to:

  > Jointly with the CHCO, develop a set of competency requirements for IT and IT acquisition staff (including IT and IT acquisition leadership

positions) and develop and maintain a current workforce planning process to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.

The NRC also recently reissued MD 12.5 (ADAMS Accession No. ML17278B085) to specifically define these CIO responsibilities.

The SWP process takes place on an annual cycle and results in strategies to address workforce needs in both budget execution year +1 and budget execution year +5. The enhanced SWP process also requires the monitoring and evaluation of strategies to make course corrections and address new workforce issues, including IT management and skill positions, on an as-needed basis but at least annually. Management will also monitor the environment for internal and external changes that may require revisions to strategies and action plans.

The CIO also identifies IT skill gaps based on short-term (FY 2018–2019) and long-term goals (FY 2020 and beyond) that are developed from documents such as the IT/IM Strategic Plan, enterprise architecture plan, the OMB Cross-Agency Priority goals, and the agency strategic plan. Internal and external training, on-the-job training, rotational opportunities, and internal and external postings serve as effective gap-closure strategies. The internal and external trainings available to the staff allow the CIO to develop staff within the office and acquire skills that are currently lacking in the agency.

The NRC will update applicable guidance to include IT workforce CIO authorities by the end of the second quarter of FY 2020 in order to bring NRC into full compliance.

- **Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies.** The NRC is partially compliant with this requirement. Part III, Section I, of MD 10.1, "Recruitment, Appointments, and Merit Staffing," dated May 5, 2015 (ADAMS Accession No. ML14092A397), and Part III, Section E, of MD 10.77, "Employee Development and Training," dated January 4, 2016 (ADAMS Accession No. ML15341A156), require all NRC Office Directors to work with the CHCO annually to build an annual staffing plan and a prioritized list of training for their staff. The CIO is the Office Director of the Office of the Chief Information Officer (OCIO) and is therefore required to work with the CHCO annually to build an annual staffing plan and a prioritized list of training for OCIO staff.

  Also, the CIO is involved in the NRC's strategic workforce planning, as evident in the NRC Strategic Workforce Plan, dated February 4, 2016 (ADAMS Accession No. ML16032A343), and the enhanced SWP process. The NRC Strategic Workforce Plan ensures that the agency is positioned to have the right number of people with the right competencies at the right time.

  The NRC will update applicable guidance to include IT workforce CIO authorities by the end of the second quarter of FY 2020 in order to bring NRC into full compliance.

- **Report annually to the head of the agency on progress made in improving IT personnel capabilities.** The enhanced SWP process will identify areas of improvement for IT professionals, and the CIO will report the progress to the head of the agency.

IT Investment Management

- **Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT.** The NRC is fully compliant with the requirement. The CIO, in collaborating with the governance bodies, reviews and approves the reallocation of resources into or within the IT/IM product lines, consistent with the Information Technology Budget Guidance, Version 1.0, issued June 2016 (ADAMS Accession No. ML15300A002), and presents remaining activities to the NRC's IT/IM governance bodies for prioritization and approval.

- **Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget.** The NRC is fully compliant with this requirement. Page 24 of the NRC's Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML17346A193) states that it is the responsibility of the CIO to:

  > Jointly with the CAO [Chief Acquisition Officer], share acquisition and procurement responsibilities. The CIO reviews all cost estimates of IT-related costs and ensures all acquisition strategies and acquisition plans that include IT apply adequate incremental development principles (see definitions).

  Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML17346A193) states that it is the responsibility of the CIO to:

  > As a member of the Strategic Sourcing Group, review and approve all acquisitions over $1 million and provide oversight to acquisitions to ensure all acquisition strategies and plans that include IT apply adequate incremental development principles, use appropriate contract types, contain appropriate statements of work for the IT portions, support the mission and business objectives included in the IT strategic plan, and align mission and program objectives in consultation with program leadership.

  Additionally, page 26 of the NRC's Capital Planning and Investment Control Process and Overview (ADAMS Accession No. ML17349A084) states the following:

  > For proposed capabilities or enhancements that include development, the CIO will also confirm and certify the appropriate use of an incremental development approach consistent with the current OMB guidance at the time of the review. The CIO's certification will be recorded by the Capital Planner in the agency's IT Portfolio Management System.

  Lastly, page 36 of the NRC's Capital Planning and Investment Control Process and Overview (ADAMS Accession No. ML17349A084) states the following:

  > The CIO, via the Major IT Business Case approval process, will certify that all software development projects utilize incremental development practices. The CIO may request additional artifacts from the IT PMs [Project Managers] to support the incremental development implementation.

- **Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation.** The NRC is fully compliant with this requirement. Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML17346A193) states that it is the responsibility of the CIO to:

    > Jointly with the CFO and executive-level IRB, provide an executive IT investment review function as required by OMB, make decisions on the IT portfolio, and recommend the IT budget to the EDO for consideration in the NRC's overall budget.

    Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML17346A193) states that it is the responsibility of the CIO to:

    > As a member of the Strategic Sourcing Group, review and approve all acquisitions over $1 million and provide oversight to acquisitions to ensure all acquisition strategies and plans that include IT apply adequate incremental development principles, use appropriate contract types, contain appropriate statements of work for the IT portions, support the mission and business objectives included in the IT strategic plan, and align mission and program objectives in consultation with program leadership.

    Page 14 of the NRC's Capital Planning and Investment Control Process and Overview (ADAMS Accession No. ML17349A084) states that the CIO:

    > Works alongside agency leadership to define the strategic priorities for IT and to formalize assumptions regarding the EA and the availability of financial resources.

    > Serves as the primary approval authority on select decisions and is accountable for the IT portfolio.

    The CIO has a significant role in planning, programming, budgeting, and acquisition decisions. In addition to the documentation mentioned above, MD 4.7, "Budget Formulation," dated August 15, 2016 (ADAMS Accession No. ML13207A234), and MD 4.8, "Budget Execution," dated August 18, 2016 (ADAMS Accession No. ML15256A002), define the CIO's role in such decisions.

- **Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented.** The NRC is fully compliant with this requirement. Page 15 of the NRC's Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML17346A193) states the following:

    > An IT investment shall be classified as a major IT investment if it meets one or more of the following OMB criteria:
    >
    > - importance to the mission or function of the Government;
    > - significant program or policy implications;
    > - high executive visibility;

- high development, operations, or maintenance costs, which the NRC defines as budget planning year costs of $10 million or greater;

- unusual funding mechanism;

- **financial systems with annual cost and spending of $500,000 or more, as dictated by mandates and guidance on financial systems, such as Circular A-127** [emphasis added]; or

- defined as major by the NRC CPIC [Capital Planning and Investment Control] process.

OMB's major IT investment oversight includes all of the NRC's financial systems; therefore, the NRC monitors and submits the financial systems Major IT Business Case to OMB on a monthly basis.

- **Maintain strategy to consolidate and optimize data centers.** The NRC has completed this action. The NRC maintains and posts the Data Center Optimization Initiative Strategic Plan on the NRC public Web site (https://www.nrc.gov/public-involve/open/digital-government.html#data) and has provided a copy of the CIO certification memorandum signed by the NRC CIO to the Federal CIO. The FY 2018 certification memorandum (https://www.nrc.gov/public-involve/open/digital-government/dcoi-strategic-plan-cio-certification-20180501.pdf) is also on the NRC public Web site. The NRC continues to update the strategy as new opportunities to optimize the agency's remaining data centers are realized.

Information Security

- **Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities.** The NRC is fully compliant with this requirement. The NRC has in place policies managed by the CHCO to ensure that the staff carry out the assigned responsibilities. These policies rely on first-line managers and higher-level supervisors to manage staff performance and conduct. This includes responsibilities for sensitive and classified information as well as for the use of and training surrounding information systems.

- **Ensure that all personnel are held accountable for complying with the agency-wide information security program.** The NRC is fully compliant with this requirement. The NRC has in place policies managed by the CHCO to ensure that the staff carry out the assigned responsibilities. These policies rely on first-line managers and higher level supervisors to manage staff performance and conduct. This includes responsibilities for sensitive and classified information as well as for the use of and training surrounding information systems.

- **Report annually to the agency head on the effectiveness of the agency information security program.** The NRC is fully compliant with this requirement. The Chief Information Security Officer and the CIO meet regularly with the EDO and the Deputy EDOs to present the information security program and to outline risks to NRC information and information systems. There are also regular discussions about the CIO metrics required under the Federal Information Security Modernization Act (FISMA)

before their submission to OMB, responses to Binding Operational Directive responses and updates, and the annual FISMA report and metrics.

Identical letter sent to the following recipients, with the exception of the replacement of the point of contact with the Chairman and the Director of the Office of Congressional Affairs:

Ms. Carol C. Harris, Director
Information Technology Acquisition
   Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

The Honorable Trey Gowdy
Chairman, Committee on Oversight
   and Government Reform
United States House of Representatives
Washington, DC 20515
cc: Representative Elijah Cummings

The Honorable John Barrasso
Chairman, Committee on Environment
   and Public Works
United States Senate
Washington, DC 20510
cc: Senator Thomas R. Carper

The Honorable Greg Walden
Chairman, Committee on Energy
   and Commerce
United States House of Representatives
Washington, DC 20515
cc: Representative Frank Pallone, Jr.

The Honorable Fred Upton
Chairman, Subcommittee on Energy
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515
cc: Representative Bobby L. Rush

The Honorable Michael McCaul
Chairman, Committee on Homeland Security
United States House of Representatives
Washington, DC 20515
cc: Representative Bennie Thompson

The Honorable Ron Johnson
Chairman, Committee on Homeland
   Security and Governmental Affairs
United States Senate
Washington, DC 20510
cc: Senator Claire McCaskill