U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. NW **Washington, DC 20548**

Accessible Version

June 26, 2025

Mr. Scott Flanders
Chief Information Officer
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Chief Information Officer Open Recommendations: Nuclear Regulatory Commission

Dear Mr. Flanders:

I am writing to you with respect to your role as the Chief Information Officer (CIO) for the Nuclear Regulatory Commission (NRC). As an independent, non-partisan agency that works for Congress, GAO's mission is to support Congress in meeting its constitutional responsibilities and help improve the performance and ensure the accountability of the federal government. Our work includes investigating matters related to the use of public funds, evaluating programs and activities of the U.S. Government at the request of congressional committees and subcommittees or on the initiative of the Comptroller General, and as required by public laws or committee reports. Our duties include reporting our findings and recommending ways to increase economy and efficiency in government spending. The purpose of this letter is to provide an overview of the open, publicly available GAO recommendations to NRC that call for the attention of the CIO.

We identified recommendations that relate to the CIO's roles and responsibilities in effectively managing IT. They include strategic planning, investment management, and information security. We have previously reported on the significance of the CIO's role in improving the government's performance in IT and related information management functions.[1] Your attention to these recommendations will help ensure the secure and effective use of IT at the agency.

Currently, NRC has six open recommendations that call for the attention of the CIO. Each of these recommendations relates to a GAO High-Risk area: (1) Ensuring the Cybersecurity of the Nation or (2) Improving IT Acquisitions and Management.[2] Fully implementing these open recommendations could significantly improve NRC's ability to deter threats and manage its critical systems, operations, and information. I have summarized selected recommendations here. See the enclosure for a full list, and additional details on the recommendations.

Ensuring the Cybersecurity of the Nation. NRC needs to take additional steps to secure the

[1]See for example, GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

[2]GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

information systems it uses to carry out its mission. Specifically, we recommended that the agency fully implement all event logging requirements as directed by the Office of Management and Budget. Until NRC implements this recommendation, there is increased risk that the agency will not have complete information from logs on its systems to detect, investigate, and remediate cyber threats.

Improving IT Acquisitions and Management. NRC needs to take steps to address key cloud procurement and portfolio review requirements. For example, we recommended that the CIO develop guidance regarding standardizing cloud service level agreements. Implementing this recommendation would help ensure that the agency is consistently holding its cloud service providers accountable for their service performance.

In addition, we recommended that NRC complete annual reviews of its IT portfolio consistent with federal requirements. Until NRC implements this recommendation, investments with substantial cost, schedule, and performance problems may continue unabated without necessary corrective action.

Copies of this letter are being sent to the appropriate congressional committees and the Federal CIO. The letter will also be available at no charge on the GAO website at https://www.gao.gov. In addition, we sent a separate letter, related to agency-wide priority recommendations, which discusses the importance of addressing cybersecurity risks, to the Chairman of NRC.[3]

If you have any questions or would like to discuss any of the recommendations outlined in this letter, please do not hesitate to contact me at marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this letter. Our teams will continue to coordinate with your staff on addressing these six open recommendations that call for the attention of the CIO. I appreciate NRC's continued commitment and thank you for your personal attention to these important recommendations.

Sincerely,

//SIGNED//

Nick Marinos
Managing Director
Information Technology and Cybersecurity
Enclosure

cc: Mr. Greg Barbaccia, Federal CIO, Office of Management and Budget

[3]GAO, *Priority Open Recommendations: Nuclear Regulatory Commission,* GAO-25-108097 (Washington, D.C.: May 5, 2025).

Enclosure

Chief Information Officer Open Recommendations to the Nuclear Regulatory Commission

This enclosure includes the open, publicly available GAO recommendations to the Nuclear Regulatory Commission (NRC) that call for the attention of its Chief Information Officer (CIO). We have divided these recommendations into two categories: (1) ensuring the cybersecurity of the nation and (2) improving IT acquisitions and management.

Ensuring the Cybersecurity of the Nation

Federal agencies depend on IT systems to carry out operations and process, maintain, and report essential information. The security of these systems and data is vital to protecting individual privacy and ensuring national security. Table 1 provides information on the open cybersecurity-related recommendation relevant to the NRC CIO.

Table 1: Open Chief Information Officer-related Cybersecurity Recommendation for the Nuclear Regulatory Commission

GAO report number	GAO report title	Recommendation
GAO-24-105658	Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements	The Chairman of the Nuclear Regulatory Commission should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 18)

Source: GAO summary based on previously issued reports. | GAO-25-108462

Improving IT Acquisitions and Management

Federal IT investments too frequently fail to deliver capabilities in a timely, cost-effective manner. Key management challenges—such as a lack of disciplined project planning and program oversight—continue to hamper effective acquisition and management of the government's IT assets. Table 2 provides information on the open IT acquisition and management-related recommendations relevant to the NRC CIO.

Table 2: Open Chief Information Officer (CIO)-related IT Acquisition and Management Recommendations for the Nuclear Regulatory Commission (NRC)

GAO report number	GAO report title	Recommendation
GAO-24-106137	Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements	The Chairman of NRC should ensure that the CIO of NRC develops guidance to put a cloud service level agreement (SLA) in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses the Office of Management and Budget's (OMB) four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 37) The Chairman of NRC should ensure that the CIO of NRC develops guidance regarding standardizing cloud SLAs. (Recommendation 38) The Chairman of NRC should ensure that the CIO of NRC develops guidance to require that contracts affecting the agency's high value assets that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 39) The Chairman of NRC should ensure that the CIO of NRC updates its existing contracts for high value assets that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 40)
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Chairman of NRC should direct its agency CIO to work with OMB to ensure that annual reviews of their IT portfolio are conducted in conjunction with the Federal CIO and the Chief Operating Officer or Deputy Secretary (or equivalent), as prescribed by the Federal Information Technology Acquisition Reform Act. (Recommendation 39)

Source: GAO summary based on previously issued reports. | GAO-25-108462