U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. NW
Washington, DC 20548

Accessible Version

January 15, 2026

Mr. Sean Gallagher
Acting Chief Information Officer
National Aeronautics and Space Administration
300 E Street Southwest
Washington, DC 20546

Chief Information Officer Open Recommendations: National Aeronautics and Space Administration

Dear Mr. Gallagher:

I am writing to you with respect to your role as the Acting Chief Information Officer (CIO) for the National Aeronautics and Space Administration (NASA). 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 and evaluating programs and activities of the U.S. Government at the request of congressional committees and subcommittees, 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 NASA 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, NASA has 30 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 NASA'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 GAO recommendations.

Ensuring the Cybersecurity of the Nation. NASA 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, including improving its risk management program. For example, we recommended that the agency prepare and approve an organization-wide cybersecurity risk assessment. Implementing this recommendation would help improve NASA's ability to identify and mitigate the highest priority cybersecurity threats across the agency.

Further, we recommended that the agency fully implement all event logging requirements as directed by the Office of Management and Budget. Until NASA implements this recommendation, there is increased risk that the agency will not have sufficient and complete information to detect, investigate, and remediate cyber threats.

In addition, we recommended that the agency develop an implementation plan with time frames to update its spacecraft acquisition policies and standards to incorporate essential controls required to protect against cyber threats. Until NASA implements this recommendation, the agency risks inconsistent implementation of cybersecurity controls and lacks assurance that spacecraft have a layered and comprehensive defense.

Improving IT Acquisitions and Management. NASA needs to better manage and track its IT resources. Specifically, we recommended that the agency complete annual reviews of its IT portfolio consistent with federal requirements. Until NASA implements this recommendation, it may miss opportunities to identify areas of duplication within its IT portfolio and to develop strategies to streamline operations and optimize resource allocation.

We also recommended that the agency complete its covered Internet of Things (IoT) inventory within the revised time frame it had proposed.[3] Given the enormous array of disparate devices that may be considered part of IoT, it is important that NASA identifies and documents the devices connected to its information systems. Until NASA implements this recommendation, the agency will lack visibility into the IoT devices in its enterprise environment and the ability to mitigate IoT cybersecurity risks.

In addition to GAO's recommendations, the NASA Inspector General also has multiple open recommendations in the area of cybersecurity. These include cybersecurity recommendations that relate to the agency's requirements under the Federal Information Security Modernization Act of 2014.[4] It will be important to address both GAO and Inspector General recommendations.

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 agencywide priority recommendations[5] to the then-Acting Administrator of NASA.[6]

---

[3]Internet of Things generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices that interact with the physical world, or "things", through such places as buildings, vehicles, transportation infrastructure, or homes.

[4]The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[5]Priority recommendations are those that GAO believes warrant priority attention from heads of key departments or agencies. They are highlighted because, upon implementation, they may significantly improve government operations, for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a high-risk or duplication issue. Since 2015, GAO has sent letters to selected agencies to highlight the importance of implementing such recommendations.

[6]GAO, *Priority Open Recommendations: National Aeronautics and Space Administration*, GAO-25-108199 (Washington, D.C.: Aug. 28, 2025).

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 30 open recommendations that call for the attention of the CIO. I appreciate NASA'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. Gregory Barbaccia, Federal CIO, Office of Management and Budget

Enclosure

Chief Information Officer Open Recommendations to the National Aeronautics and Space Administration

This enclosure includes the open, publicly available GAO recommendations to the National Aeronautics and Space Administration (NASA) 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 recommendations relevant to the NASA CIO.

Table 1: Open Chief Information Officer (CIO)-related Cybersecurity Recommendations for the National Aeronautics and Space Administration (NASA)

GAO report number	GAO report title	Recommendation
GAO-22-105065	Privacy: Dedicated Leadership Can Improve Programs and Address Challenges	The Administrator of NASA should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 48)
GAO-24-105658	Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements	The Administrator of NASA should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 17)
GAO-24-106624	NASA Cybersecurity: Plan Needed to Update Spacecraft Acquisition Policies and Standards	The NASA Administrator should ensure that the Chief Engineer, the CIO, and the Principal Advisor for Enterprise Protection develop an implementation plan with time frames to update its spacecraft acquisition policies and standards to incorporate essential controls required to protect against cyber threats. (Recommendation 1)

GAO-25-108138	Cybersecurity: NASA Needs to Fully Implement Risk Management	The NASA Administrator should ensure that NASA's CIO prepares and approves an organization-wide cybersecurity risk assessment. (Recommendation 1) The NASA Administrator should direct NASA's CIO to ensure that the documented impact levels for confidentiality, integrity, and availability for all systems match the risk of the system, and that any changes to the provisional impact levels are fully justified in accordance with NASA policy. (Recommendation 2) The NASA Administrator should direct NASA's CIO to update its guidance to include oversight responsibilities for ensuring NASA-defined control baselines are properly applied when baselines are updated. (Recommendation 3) The NASA Administrator should direct NASA's CIO to update its policies to provide more specific guidance about how to document assessment results for all types of critical controls including inherited controls. (Recommendation 4) The NASA Administrator should direct NASA's CIO to ensure that all critical controls for the first system found to be unsatisfied during security control assessments include recommendations and a residual risk level. (Recommendation 5) The NASA Administrator should direct NASA's CIO to ensure that all critical controls for the second system found to be unsatisfied during security control assessments include recommendations and a residual risk level. (Recommendation 6) The NASA Administrator should direct NASA's CIO to ensure that all critical controls for the third system found to be unsatisfied during security control assessments include recommendations and a residual risk level. (Recommendation 7) The NASA Administrator should direct NASA's CIO to ensure that all critical controls for the fourth system found to be unsatisfied during security control assessments include recommendations and a residual risk level. (Recommendation 8) The NASA Administrator should direct NASA's CIO to ensure that Plans of Action and Milestones (POA&Ms) related to critical controls for the first system include all key information outlined by its policies and procedures, including risk levels. (Recommendation 9) The NASA Administrator should direct NASA's CIO to ensure that POA&Ms related to critical controls for the second system include all key information outlined by its policies and procedures, including risk levels. (Recommendation 10) The NASA Administrator should direct the information system owner for the first system to ensure that estimated completion dates for POA&Ms related to all critical controls for the system are reasonable (e.g. less susceptible to extensions) and that POA&Ms related to all critical controls are completed in a timely manner. (Recommendation 11) The NASA Administrator should direct the information system owner for the second system to ensure that estimated completion dates for POA&Ms related to all critical controls for the system are reasonable (e.g. less susceptible to extensions) and that POA&Ms related to all critical controls are completed in a timely manner. (Recommendation 12) The NASA Administrator should direct the information system owner for the third system to ensure that estimated completion dates for POA&Ms related to all critical controls

	for the system are reasonable (e.g. less susceptible to extensions) and that POA&Ms related to all critical controls are completed in a timely manner. (Recommendation 13)
	The NASA Administrator should direct the information system owner for the fourth system to ensure that estimated completion dates for POA&Ms related to all critical controls for the system are reasonable (e.g. less susceptible to extensions) and that POA&Ms related to all critical controls are completed in a timely manner. (Recommendation 14)
	The NASA Administrator should direct NASA's CIO to update its policies for the authorize step to include quality control activities to ensure that the information developed for authorization packages is appropriate, current, complete, and accurate. (Recommendation 15)
	The NASA Administrator should direct NASA's CIO to update NASA's continuous monitoring guidance to provide sufficient information to allow systems to develop clearly defined and understood continuous monitoring strategies, and ensure that selected systems develop continuous monitoring strategies in alignment with the updated guidance. (Recommendation 16)

Source: GAO summary based on previously issued reports. | GAO-26-108705

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 NASA CIO.

Table 2: Open Chief Information Officer (CIO)-related IT Acquisition and Management Recommendations for the National Aeronautics and Space Administration (NASA)

GAO report number	GAO report title	Recommendation
GAO-15-431	Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services	To help the agency effectively manage spending on mobile devices and services, the Administrator of NASA should ensure a complete inventory of mobile devices and associated services is established. (Recommendation 29) To help the agency effectively manage spending on mobile devices and services, the Administrator of NASA should ensure a reliable inventory of mobile service contracts is developed and maintained. (Recommendation 30) To help the agency effectively manage spending on mobile devices and services, the Administrator of NASA should ensure procedures to monitor and control spending are established agencywide. Specifically, ensure that (1) procedures include assessing devices for zero, under, and over usage; (2) personnel with authority and responsibility for performing the procedures are identified; and (3) the specific steps to be taken to perform the process are documented. (Recommendation 31)
GAO-18-337	NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses	The Administrator should direct the CIO to address, in conjunction with the Chief Human Capital Officer, gaps in IT workforce planning by fully implementing the eight key IT workforce planning activities noted in this report. (Recommendation 3)
GAO-20-155	Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays	The Administrator of NASA should ensure that the agency's CIO updates the telecommunications inventory to include all telecommunications assets and services in use at the agency, and updates NASA's process for ongoing maintenance of the inventory to include the complete inventory. (Recommendation 21) The Administrator of NASA should ensure that the agency's CIO completes efforts to identify the agency's future telecommunications needs using a complete inventory of existing telecommunications services. (Recommendation 22) The Administrator of NASA should ensure that the agency's CIO conducts an analysis to support the anticipated cost savings identified as part of the agency's justification for its resource requests related to hardware and software upgrades for the telecommunications transition, and justifies its resource requests for transition program management staff; conducts an analysis to identify staff resources needed for the entire transition effort; and analyzes training needs for staff assisting with the transition. (Recommendation 24)

GAO report number	GAO report title	Recommendation
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Administrator of NASA should direct its agency CIO to work with the Office of Management and Budget (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 37)
GAO-25-107114	Cloud Computing: Selected Agencies Need to Implement Updated Guidance for Managing Restrictive Licenses	The Administrator of NASA should update and implement guidance to fully address identifying, analyzing, and mitigating the impacts of restrictive software licensing practices on cloud computing efforts. (Recommendation 7) The Administrator of NASA should assign and document responsibility for identifying and managing potential impacts of restrictive software licensing practices across the agency. (Recommendation 8)
GAO-25-107179	Internet of Things: Federal Actions Needed to Address Legislative Requirements	The Administrator of NASA should direct the CIO to establish a plan and time frame for completing the covered Internet of Things inventory, as directed by OMB. (Recommendation 8)

Source: GAO summary based on previously issued reports. | GAO-26-108705