GAO
Highlights

Highlights of GAO-18-337, a report to congressional committees

May 2018

NASA INFORMATION TECHNOLOGY

Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses

Why GAO Did This Study

NASA depends heavily upon IT to conduct its work. The agency spends at least $1.5 billion annually on IT investments that support its missions, including ground control systems for the International Space Station and space exploration programs.

The National Aeronautics and Space Administration Transition Authorization Act of 2017 included a provision for GAO to review the effectiveness of NASA's approach to overseeing and managing IT, including its ability to ensure that resources are aligned with agency missions and are cost effective and secure. Accordingly, GAO's specific objective for this review was to determine the extent to which NASA has established and implemented leading IT management practices in strategic planning, workforce planning, governance, and cybersecurity. To address this objective, GAO compared NASA IT policies, strategic plans, workforce gap assessments, and governance board documentation to federal law and leading practices. GAO also assessed NASA IT security plans, policies, and procedures against leading cybersecurity risk management practices.

What GAO Recommends

GAO is making 10 recommendations to NASA to address the deficiencies identified in NASA IT strategic planning, workforce planning, governance, and cybersecurity. NASA concurred with seven recommendations, partially concurred with two, and did not concur with one. GAO maintains that all of the recommendations discussed in this report remain valid.

View GAO-18-337. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

The National Aeronautics and Space Administration (NASA) has not yet effectively implemented leading practices for information technology (IT) management. Specifically, GAO identified weaknesses in NASA's IT management practices for strategic planning, workforce planning, governance, and cybersecurity.

- NASA has not documented its IT strategic planning processes in accordance with leading practices. While NASA's updated IT strategic plan represents improvement over its prior plan, the updated plan is not comprehensive because it does not fully describe strategies for achieving desired results or describe interdependencies within and across programs. Until NASA establishes a comprehensive IT strategic plan, it will lack critical information needed to align resources with business strategies and investment decisions.
- Of the eight key IT workforce planning activities, the agency partially implemented five and did not implement three. For example, NASA does not assess competency and staffing needs regularly or report progress to agency leadership. Until NASA implements the key IT workforce planning activities, it will have difficulty anticipating and responding to changing staffing needs.
- NASA's IT governance does not fully address leading practices. While the agency revised its governance boards, updated their charters, and acted to improve governance, it has not fully established the governance structure, documented improvements to its investment selection process, fully implemented investment oversight practices and ensured the Chief Information Officer's visibility into all IT investments, or fully defined policies and procedures for IT portfolio management. Until NASA addresses these weaknesses, it will face increased risk of investing in duplicative investments or may miss opportunities to ensure investments perform as intended.

NASA has not fully established an effective approach to managing agency-wide cybersecurity risk. An effective approach includes establishing executive oversight of risk, a cybersecurity risk management strategy, an information security program plan, and related policies and procedures.

NASA Implementation of Cybersecurity Risk Management Practices

Practice	Status
Executive oversight of risk	While NASA has designated a risk executive, the agency lacks a dedicated office to provide comprehensive executive oversight of risks.
Cybersecurity risk management strategy	NASA lacks an agency-wide cybersecurity risk management strategy; one is currently in development.
Information security program plan	NASA developed a draft agency-wide information security program plan; however, the plan does not yet fully address leading practices.
Policies and procedures	Policies and procedures for protecting NASA's information systems are in place, but the agency has not kept them current or integrated.

Source: GAO analysis of National Aeronautics and Space Administration documentation. | GAO-18-337

As NASA continues to collaborate with other agencies and nations and increasingly relies on agreements with private companies to carry out its missions, the agency's cybersecurity weaknesses make its systems more vulnerable to compromise. Until NASA leadership fully addresses these leading practices, its ability to ensure effective management of IT across the agency and manage cybersecurity risks will remain limited.