United States Government Accountability Office

Report to Congressional Committees

May 2018

NASA INFORMATION TECHNOLOGY

Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses

GAO-18-337

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.

Contents

Abbreviations

CIO	Chief Information Officer
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute for Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SAISO	Senior Agency Information Security Officer

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 22, 2018

The Honorable John Thune
Chairman
The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Lamar Smith
Chairman
The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The National Aeronautics and Space Administration (NASA) exercises control over aeronautical and space activities sponsored by the United States and also seeks to encourage the fullest commercial use of space. NASA's current and planned activities span a broad range of complex and technical endeavors, including developing new capabilities to send future missions to Mars, improving the air transportation experience, and developing new space transportation systems. These activities may rely on partnerships with academic, private sector, and international organizations, including foreign space agencies.[1] In recent years, NASA also has increasingly relied on other countries and agreements with private companies to support its missions.[2]

NASA depends heavily upon information technology (IT) to conduct its work. Since fiscal year 2016, the agency has planned to spend about $1.5 billion annually on IT investments that support its missions, including ground control systems for the International Space Station and other space exploration programs. In addition, the agency has invested in cloud

[1]These include the European Space Agency as well as the space agencies of Argentina, Brazil, China, Germany, India, Israel, Japan, Russia, South Korea, and Ukraine.

[2]For example, since the Space Shuttle was retired in 2011, the United States has been relying on Russia to carry astronauts to and from the International Space Station. NASA's Commercial Crew Program is facilitating private development of a domestic system to meet that need safely, reliably, and cost-effectively before the seats it has contracted for on a Russian spacecraft run out in 2019.

computing, data center optimization, and IT security capabilities to support its business operations.

However, we and the NASA Office of Inspector General have reported that the agency has struggled for more than two decades to overcome its decentralized operations and culture of autonomy at its major organizational units, in an attempt to provide effective oversight and management of its IT environment. Moreover, we and others have reported on information security concerns. NASA systems are highly interconnected.[3] The agency is also affected by geopolitics and is targeted by cybercriminals, including those that may be sponsored by foreign intelligence services.[4] In addition, entities with whom NASA collaborates may also be targets of cybercriminals.

The National Aeronautics and Space Administration Transition Authorization Act of 2017 included a provision for us 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.[5] Our objective for this review was to address 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, we compared NASA's IT management policies, procedures, and documentation to criteria established by federal law and leading practices.

- For our work regarding IT strategic planning, we obtained and evaluated NASA's documentation on IT strategic planning, including its related planning guidance, agency-wide strategic plan, and IT-specific strategic plans. We analyzed its strategic planning guidance and assessed the contents of the previous and current IT strategic

[3]The Office of Inspector General has reported that the agency faces unique security challenges because of its connectivity with educational institutions, research facilities, and other organizations.

[4]During 2016 and 2017, NASA reported more than 3,000 computer security incidents related to malicious software on or unauthorized access to agency computers. These incidents included criminal enterprises seeking profit and intrusions that may have been sponsored by foreign intelligence services seeking to further their countries' objectives.

[5]National Aeronautics and Space Administration Transition Authorization Act of 2017, Pub. L. No. 115-10, §811(b), 131 Stat. 18, 59 (2017).

plans by comparing them to leading practices that we and the Office of Management and Budget (OMB) have previously identified.[6] These practices include documenting the IT strategic planning process and developing a strategic plan that defines the agency's vision and provides a road map to help align information resources with business strategies and investment decisions.

- For IT workforce planning, we reviewed documentation, including NASA's 2015 draft IT workforce plan, competencies, reported staffing data, and a workforce gap assessment. We compared this documentation to eight key IT workforce planning activities that we previously identified and that were derived from federal law and guidance, including OMB memorandums, GAO reports, and the Office of Personnel Management's (OPM) Human Capital Framework.[7]
- Our review of IT governance involved analyzing NASA's governance board meeting minutes and briefings, charters, and policies and procedures, and comparing them to criteria as identified by GAO in the IT investment management framework.[8] Specifically, we focused on policies and procedures related to instituting investment boards, selecting investments, overseeing investments, and developing investment portfolios.
- Regarding cybersecurity, we obtained and analyzed available NASA documentation to determine the extent to which the agency had established an effective approach for managing cybersecurity risk. This documentation included information security policies and

[6]Leading practices were identified related to strategic planning from the Office of Management and Budget, Circular No. A-11: *Preparation, Submission, and Execution of the Budget*, July 2017; OMB Circular No. A-130: *Managing Information as a Strategic Resource*, (Washington, D.C.: July 28, 2016); and OMB Memorandum M-13-09 Fiscal Year 2013 PortfolioStat Guidance: *Strengthening Federal IT Portfolio Management* (Washington, D.C.: Mar. 27, 2013). Further, our prior work related to IT strategic planning practices includes, for example, GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, GAO-12-495 (Washington, D.C.: Apr. 26, 2012); and *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*, GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

[7]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

[8]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004) and OMB, *Memorandum M-13-09 Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* (Washington, D.C.: Mar. 27, 2013).

procedures, management briefings and reports, and a draft information security program plan. We then assessed whether NASA's approach addressed foundational cybersecurity risk management components identified in the National Institute for Standards and Technology's (NIST) guidance.[9] These components included the establishment of a risk executive function, a cybersecurity risk management strategy, an information security program plan, and current policies and procedures for relevant security controls.

In addition to assessing IT management at NASA headquarters, we reviewed such management practices at two of the agency's centers and one mission directorate, focusing on those with the largest fiscal year 2017 IT budgets.[10] In addition, we visited and reviewed IT management practices for the Goddard Space Flight Center because of the center's proximity to GAO. We also interviewed cognizant officials with responsibilities for IT management at NASA. The results of our work at the selected NASA centers and mission directorate are not generalizable to other NASA centers and mission directorates. Additional details on our objective, scope, and methodology can be found in appendix I.

We conducted this performance audit from May 2017 to May 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

NASA's mission is to drive advances in science, technology, aeronautics, and space exploration to enhance knowledge, education, innovation, economic vitality, and stewardship of Earth. The NASA Administrator is responsible for leading the agency and is accountable for all aspects of its mission, including establishing and articulating its vision and strategic

[9]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

[10]We conducted work at three of NASA's nine centers (two centers with the largest fiscal year 2017 IT budgets—Johnson Space Center in Houston, Texas and Marshall Space Flight Center in Huntsville, Alabama) and Goddard Space Flight Center, in Greenbelt, Maryland. We also reviewed IT management practices at one of NASA's four mission directorates (the Human Explorations and Operations Mission Directorate).

priorities and ensuring successful implementation of supporting policies, programs, and performance assessments.

Within NASA headquarters, the agency has four mission directorates that define its major core mission work: (1) *Aeronautics Research* conducts cutting-edge research to enable revolutionary advances in future aircraft, as well as in the airspace in which they will fly; (2) *Human Exploration and Operations* is responsible for NASA space operations, developing new exploration and transportation systems, and performing scientific research; (3) *Science* carries out the scientific exploration of Earth and space to expand the frontiers of Earth science, planetary science, and astrophysics, and (4) *Space Technology* develops revolutionary technologies through transparent, collaborative partnerships that expand the boundaries of aerospace. The agency also has a mission support directorate to manage its business needs and administrative functions, such as human capital management.

In addition to NASA headquarters in Washington, D.C., the agency is composed of nine field centers managed by NASA employees, and one federally funded research and development center that are responsible for executing programs and projects.[11] NASA centers are located throughout the country and manage projects or programs for multiple mission directorates. For example, the Goddard Space Flight Center supports various IT programs within the *Science* mission directorate, while the Johnson Space Center supports multiple programs in the *Human Exploration and Operations* mission directorate.

According to NASA documents, the agency planned to spend $1.6 billion of its fiscal year 2018 budget authority on IT.[12] Of this total, $888 million was to be used for business IT and $672.8 million was to be used for mission IT. Business IT includes the infrastructure and systems needed to support internal agency operations, such as commodity IT (e.g., e-mail

[11]The nine field centers are (1) Glenn Research Center in Ohio, (2) the Goddard Space Flight Center in Maryland, (3) the Langley Research Center in Virginia, (4) the Kennedy Space Center in Florida, (5) the Marshall Space Flight Center in Alabama, (6) Stennis Space Center in Mississippi, (7) Johnson Space Center in Texas, (8) Armstrong Flight Research Center in California, and (9) Ames Research Center in California. In addition, the Jet Propulsion Laboratory is a federally funded research center managed for NASA by the California Institute of Technology.

[12]The planned $1.6 billion in IT budget authority represented about 8 percent of NASA's $19.1 billion total budget request for fiscal year 2018.

and communications systems), infrastructure, IT management, administrative services, and support systems, whereas mission IT includes the technology needed to support space programs and research for the agency's mission programs. The technology that the agency uses to support its mission programs includes highly-specialized IT, defined by NASA as any equipment, system, and/or software that is used to acquire, store, retrieve, manipulate, and/or transmit data or information when the IT is embedded in a mission platform or provides a platform required for simulating, executing, or operating a mission.

Historically, NASA and its Inspector General have reported that funding for and oversight of highly-specialized IT has been decentralized among mission directorates and embedded within launch programs and other mission activities instead of being identified as IT to be managed as part of the agency's IT portfolio.[13] According to the Inspector General, the agency's decentralized funding for and oversight of IT has minimized agency-wide visibility into and oversight of NASA's spending on these systems.

NASA's IT Management and Governance Structure

The agency's Chief Information Officer (CIO) reports directly to the NASA Administrator and serves as the principal advisor to the NASA Administrator and senior officials on all matters pertaining to IT. The CIO is to provide leadership, planning, policy direction, and oversight for the management of NASA's information and systems. Toward this end, the CIO's responsibilities include developing and implementing approaches for executing the goals and outcomes in the NASA strategic plan; ensuring that the agency's human resources possess the requisite knowledge and skills in IT and information resources management; maximizing the value of NASA IT investments through an investment management process; and leading and implementing the agency's IT security program. The CIO also is responsible for developing and implementing agency-wide IT policies and processes.

NASA's CIO also is to direct, manage, and provide policy guidance and oversight of the agency's center CIOs. Each center has a CIO responsible for supporting center leadership and managing IT staff.

[13]NASA, *IT Portfolio Review Tiger Team: Final Report to Information Technology Council*, (Washington, D.C.: Dec. 7, 2016) and National Aeronautics and Space Administration Office of Inspector General, *NASA's Efforts to Improve the Agency's Information Technology Governance*, IG-18-002, (Washington, D.C.: Oct. 19, 2017).

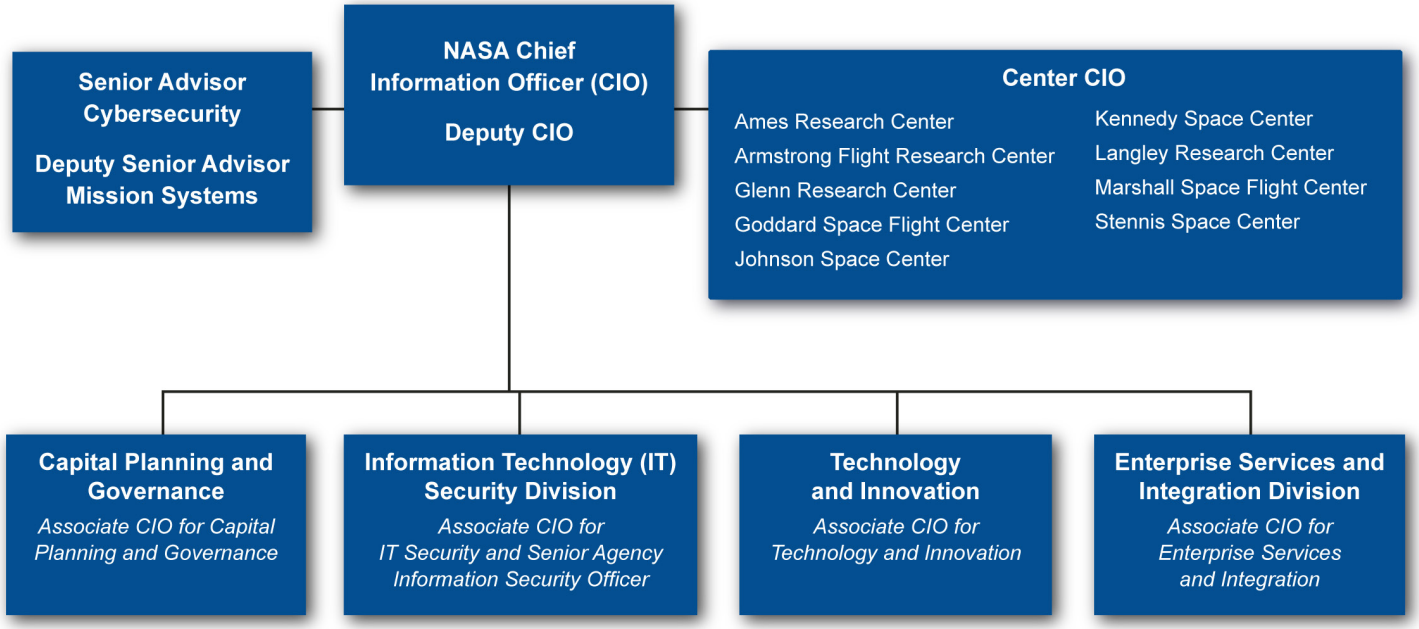
Similarly, each mission directorate has a representative who coordinates with programs on IT-specific issues and, as needed, obtains support from the Office of the CIO. Both center CIOs and mission directorate IT representatives report to the NASA CIO and to the leadership of their respective centers and mission directorates.

The CIO is supported by staff in the Office of the CIO. This office is organized into four divisions responsible for (1) IT security, (2) capital planning and governance, (3) technology and innovation, and (4) enterprise services and integration. Collectively, these divisions support NASA's approach to IT strategic and workforce planning, governance boards and practices, and cybersecurity.

In March 2017, the Office of the CIO submitted plans to establish a fifth division focused on new applications, and also to rename existing divisions to better represent the services they provide. For example, the Office of the CIO proposed that the Capital Planning and Governance Division be renamed the IT Business Management Division. As of March 2018, NASA had not yet approved or implemented the planned reorganization.

Figure 1 depicts the organization of the Office of the CIO, including relevant reporting relationships for center CIOs and mission directorate IT representatives, as of March 2018.

Figure 1: Organization of the National Aeronautics and Space Administration's (NASA) Office of the Chief Information Officer, as of March 2018



Source: GAO analysis of NASA data. | GAO-18-337

GAO and NASA's Office of Inspector General Have Reported on Longstanding Weaknesses in IT Management

We and NASA's Office of Inspector General have reported on longstanding IT management weaknesses within the agency. For example, in October 2009, we reported that NASA had made progress in implementing IT security controls and aspects of its information security program, but that it had not always implemented appropriate controls to sufficiently protect the confidentiality, integrity, and availability of information and systems.[14] We also identified control vulnerabilities and program shortfalls, which, collectively, increased the risk of unauthorized access to NASA's sensitive information, as well as inadvertent or deliberate disruption of its system operations and services. We recommended that the NASA Administrator take steps to mitigate control vulnerabilities and fully implement a comprehensive information security program. The agency concurred with our eight recommendations and

[14]GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009).

stated that it was taking actions to mitigate the information security weaknesses identified.

In addition, NASA's Office of Inspector General has issued 24 reports over the last 7 years on IT governance and security weaknesses at the agency. For example, in June 2013, the office reported that the decentralized nature of NASA's operations and its longstanding culture of autonomy had hindered the agency's ability to implement effective IT governance.[15] Specifically, the report stated that the CIO had limited visibility and control over a majority of IT investments, operated in an organizational structure that marginalized the authority of the position, and could not enforce security measures across NASA's computer networks. Moreover, the IT governance structure in place at the time was overly complex, did not function effectively, and operated under a decentralized model that relegated decision making about critical IT issues to numerous individuals across NASA, leaving such decisions outside the purview of the CIO.

The Office of Inspector General made eight recommendations to the NASA Administrator for improving IT governance, including calling for all governance to be consolidated within the Office of the CIO to ensure adequate visibility, accountability, and integration into all mission-related IT assets and activities. The Administrator concurred with six and partially concurred with two of the recommendations and planned actions sufficient for the Office of Inspector General to close all eight recommendations as implemented. However, the Office of Inspector General later reported that the extent to which NASA had implemented the agreed-upon changes was in doubt based on subsequent audit findings that NASA was still struggling with limited agency CIO authority, decentralized IT operations, and ineffective IT governance.

A follow-on report issued in October 2017 described a continued lack of progress in improving IT governance, determined that the CIO's visibility into investments across the agency continued to be limited, and identified flaws in the process developed to improve governance.[16] Specifically, the Office of Inspector General noted that the Office of the CIO had made

[15]National Aeronautics and Space Administration Office of Inspector General, *NASA's Information Technology Governance*, IG-13-015 (Washington, D.C.: Jun. 5, 2013).

[16]National Aeronautics and Space Administration Office of Inspector General, *NASA's Efforts to Improve the Agency's Information Technology Governance*, IG-18-002 (Washington, D.C.: Oct. 19, 2017).

changes to its IT governance boards over the past few years, but the boards had not made strategic decisions to substantively impact how NASA IT would be managed. According to the Office of Inspector General, slow implementation of the revised governance structure had left many IT officials operating under the previous inefficient and ineffective framework.

The report also noted that, as of August 2017, the Office of the CIO had not finalized the roles and responsibilities for IT management and lingering confusion regarding security roles, coupled with poor IT inventory practices, had negatively impacted NASA's security posture. Importantly, the report explained that the Office of the CIO continued to have limited influence over IT management within the mission directorates and at centers.

The Office of Inspector General made five recommendations to the CIO that were intended to improve, among other things, governance and security. As of October 2017, NASA had concurred with three recommendations, partially concurred with two recommendations, and described corrective actions taken or planned. However, the Office of Inspector General found that NASA's original proposed action to address the fourth recommendation was insufficient; thus, in December 2017, the agency established additional proposed actions to address that recommendation.

Key IT Management Disciplines

We have identified a set of essential and complementary management disciplines that provide a sound foundation for IT management. These include the following:

- **Strategic planning:** Strategic planning defines what an organization seeks to accomplish and identifies the strategies it will use to achieve desired results. We have previously reported that a defined strategic planning process allows an agency to clearly articulate its strategic direction and establish linkages among planning practices, such as

goals, objectives, and strategies and identified leading practices for agency planning.[17]

- **Workforce planning:** We have previously reported that it is important for an agency to have a strong IT workforce to help ensure the timely and effective acquisition of IT.[18] In November 2016, we identified eight key workforce planning activities derived from the Clinger-Cohen Act of 1996 and relevant guidance, including memorandums and guidance from OPM and OMB, and prior GAO reports.[19] These laws and guidance focus on the importance of setting the strategic direction for workforce planning, analyzing the workforce to identify skill gaps, developing strategies to address skill gaps, and monitoring and reporting on progress in addressing skill gaps.
- **IT governance:** IT projects can significantly improve an organization's performance, but they can also become costly, risky, and unproductive. In 1996, Congress passed the Clinger-Cohen Act, which requires executive branch agencies to establish a process for selecting, managing, and evaluating investments in order to maximize the value and assess and manage the risks of IT acquisitions.[20] Agencies can maximize the value of their investments and minimize the risks of their acquisitions by having an effective and efficient governance process, as described in GAO's guide to effective IT investment management.[21]

[17]GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, GAO-12-495 (Washington, D.C.: Apr. 26, 2012); *Defense Business Transformation: Status of Department of Defense Efforts to Develop a Management Approach to Guide Business Transformation*, GAO-09-272R (Washington, D.C.: Jan. 9, 2009); GAO-10-846G; and *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses,* GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

[18]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014); *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003); and *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002).

[19]GAO-17-8; GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, D.C.: Nov. 29, 2011); *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003); and *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002).

[20]*Clinger-Cohen Act of 1996*, Pub. L. No. 104-106, Div. D and Div. E, § 5125(c)(3) 110 Stat. 642, 684-85 (Feb. 10, 1996), codified at 40 U.S.C. § 11315(c)(3).

[21]GAO-04-394G.

- **Cybersecurity:** Federal systems and networks are often interconnected with other internal and external systems and networks, including the Internet. When systems are interconnected, the number of avenues of attack increases and the attack surface expands. Effective security for agency systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information, including personal information entrusted to the government by members of the American public.[22] Taking action to assure that an agency's contractors and partners are adequately protecting the agency's information and systems is one way an agency can address cybersecurity risks.

  NIST has issued a suite of information security standards and guidelines that, collectively, provide comprehensive guidance on managing cybersecurity risk to agencies and any entities performing work on the agencies' behalf.[23] NIST's cybersecurity framework was issued in February 2014 in response to Executive Order 13636.[24] The framework outlines a risk-based approach to managing cybersecurity risk and protecting an organization's critical information assets. Subsequent to the issuance of the cybersecurity framework, a May 2017 executive order required agencies to use the framework to manage cybersecurity risks.[25] The order outlined actions to enhance cybersecurity across federal agencies and critical infrastructure to improve the nation's cyber posture and capabilities against cybersecurity threats to digital and physical security.

[22]GAO, *Social Security Administration: Effective Planning and Management Practices Are Key to Overcoming IT Modernization Challenges*, GAO-16-815T (Washington, D.C.: July 14, 2016).

[23]These documents include NIST, *Managing Information Security Risk: Organization, Mission, and Information System View* (Gaithersburg, Md.: March 2011); *Security and Privacy Controls for Federal Information Systems and Organizations* (Gaithersburg, Md.: April 2013), *and the Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: February 2014).

[24]Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, issued in February 2013, outlines an action plan for improving security for critical cyber infrastructure. This includes, among other things, requirements for NIST to develop a voluntary critical infrastructure cybersecurity framework and performance measures.

[25]Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22, 391, May 16, 2017.

NASA Has Not Yet Effectively Established and Implemented Leading IT Management Practices

NASA has not yet effectively established and implemented leading IT management practices for strategic planning, workforce planning, governance, and cybersecurity. Specifically,

- The agency's IT strategic planning process is not yet fully documented and its IT strategic plan lacks key elements called for by leading practices.
- NASA has not yet established an IT workforce planning process consistent with leading practices.
- The agency has taken recent action to improve its IT governance structure; however, it has not yet fully established that structure, documented improvements to its investment selection process, fully implemented investment oversight leading practices, or fully defined its policies and procedures for IT portfolio management.
- NASA has not fully established an effective approach to managing agency-wide cybersecurity risk. While it has designated a risk executive, the agency lacks a dedicated office to provide comprehensive executive oversight of risks. In addition, the agency-wide cybersecurity risk management strategy is currently in development, and the agency's information security program plan does not address all leading practices and has not been finalized. Further, policies and procedures for protecting NASA's information systems are in place, but the agency has not ensured that they are always current or integrated.

NASA Has Not Fully Documented Its IT Strategic Planning Process

Leading practices of IT strategic planning established in OMB guidance call for an agency to document its IT strategic planning process, including, at a minimum, documenting the responsibilities and accountability for IT resources across the agency. It also calls for

documenting the method by which the agency defines its IT needs and develops strategies, systems, and capabilities to meet those needs.[26]

NASA's documented IT strategic planning process describes the responsibilities and accountability for IT resources across the agency. For example, NASA has assigned specific governance bodies with responsibility for developing and overseeing the implementation of the IT strategy. Also, in its IT strategic plan, NASA described key stakeholders across the agency that are responsible for the development of the plan. These stakeholders include the Associate CIOs, representatives from mission directorates, mission support organizations, and the centers.

On the other hand, the methods by which the agency defines its IT needs and develops strategies, systems, and capabilities to meet those needs are not documented. For example, according to the IT strategic plan, the Office of the CIO is to perform a gap analysis to inform the development of NASA's roadmap that translates its IT needs and the strategies identified for meeting those needs into tactical plans. The tactical plans are to define how the strategic plan will be incrementally executed to achieve the longer term goals.

However, the Office of the CIO has not documented in its strategic planning policies and procedures how the CIO will perform the gap analysis or the methods for developing these tactical plans and roadmaps. This is particularly important since, according to officials in NASA's Office of the CIO, the centers vary as to whether they have developed their own IT strategic plans or tactical plans, and the office does not oversee or review any center-level plans to ensure they align with the NASA IT strategic plan.

According to officials in the Office of the CIO, NASA used a new model in formulating its IT strategy for fiscal years 2018 to 2021, such as including

[26]OMB, *Circular No. A-11: Preparation, Submission, and Execution of the Budget*, July 2017; *Circular No. A-130: Managing Information as a Strategic Resource,* (Washington, D.C.: July 28, 2016) and *Memorandum M-13-09 Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* (Washington, D.C.: Mar. 27, 2013); GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, GAO-12-495 (Washington, D.C.: Apr. 26, 2012); *Defense Business Transformation: Status of Department of Defense Efforts to Develop a Management Approach to Guide Business Transformation*, GAO-09-272R (Washington, D.C.: Jan. 9, 2009); GAO-10-846G; and *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses,* GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

a broader set of stakeholders in the strategic planning cycle before documenting the strategic planning process. The officials stated that they intend to identify lessons learned from using this new model and formally document a complete and repeatable IT strategic planning process in the future. However, the agency has not established time frames for when the Office of the CIO will fully document its strategic planning process. Without a fully documented strategic planning process, NASA risks not being able to clearly articulate what it seeks to accomplish and identify the IT resources needed to achieve desired results in a way that is consistent and complete.

NASA Has Improved Its IT Strategic Plan, but Has Not Yet Established a Comprehensive Plan

In addition to calling for agencies to fully document the strategic planning process, leading practices from OMB guidance and our prior research and experience at federal agencies have shown that an agency should develop a comprehensive and effective IT strategic plan that (1) is aligned with the agency's overall strategy; (2) identifies the mission of the agency, results-oriented goals, and performance measures that permit the agency to determine whether implementation of the plan is succeeding; (3) includes strategies, with resources and time frames, that the governing IT organization intends to use to achieve desired results; and (4) provides descriptions of interdependencies within and across projects so that they can be understood and managed.[27] The resulting plan is to serve as an agency's vision, or road map, and help align information resources with business strategies and investment decisions.

NASA has taken steps to improve its IT strategic plan, but the updated plan is not comprehensive in that it does not fully address all four elements of a comprehensive and effective plan outlined above. In this regard, the agency had a prior strategic plan covering the time frame of March 2014 to November 2017. More recently, in December 2017, the CIO and Associate Administrator approved an updated plan for

[27]OMB, *Circular No. A-11: Preparation, Submission, and Execution of the Budget*, July 2017; *Circular No. A-130: Managing Information as a Strategic Resource,* (Washington, D.C.: July 28, 2016) and *Memorandum M-13-09 Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* (Washington, D.C.: Mar. 27, 2013); GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, GAO-12-495 (Washington, D.C.: Apr. 26, 2012); *Defense Business Transformation: Status of Department of Defense Efforts to Develop a Management Approach to Guide Business Transformation*, GAO-09-272R (Washington, D.C.: Jan. 9, 2009); GAO-10-846G; and *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses,* GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

implementation. The updated plan is intended for use from the date it was approved through fiscal year 2021.

Regarding the four elements of a comprehensive IT strategic plan, NASA's prior plan addressed one element, partially addressed two elements, and did not address one element. The updated plan was slightly improved in that it addressed two elements, partially met one element, and did not meet one element of a comprehensive strategic plan. Table 1 provides a summary of the extent to which NASA's prior IT strategic plan (covering the time frame of March 2014 to November 2017) and recently updated IT strategic plan (covering the time frame of December 2017 to fiscal year 2021) addressed key elements of a comprehensive strategic plan.

Table 1: Extent to Which the National Aeronautics and Space Administration's (NASA) Prior and Updated Information Technology (IT) Strategic Plans Addressed Key Elements of a Comprehensive Strategic Plan

Key element	GAO assessment of NASA's prior IT strategic plan	GAO assessment of NASA's updated IT strategic plan
Aligns with the agency's overall strategy	●	●
Identifies the mission of the agency, results-oriented goals, and performance measures	◐	●
Includes strategies to achieve desired results	◐	◐
Provides descriptions of interdependencies among projects	○	○

Legend: ● NASA's IT strategic plan addressed the key element.
◐ NASA's IT strategic plan partially addressed the key element
○ NASA's IT strategic plan did not address the key element

Source: GAO analysis of National Aeronautics and Space Administration (NASA) data. | GAO-18-337

NASA's prior IT strategic plan was aligned with the agency's overall strategic plan and identified the mission of the agency and results-oriented goals. However, these goals were not linked to specific performance measures that were needed to track progress and did not always describe strategies to achieve desired results. Additionally, this plan lacked descriptions of interdependencies within and across projects.

NASA's updated IT strategic plan is aligned with the agency's overall strategic plan and identifies the mission of the agency and results-

oriented goals.[28] For example, the plan describes the agency's IT vision, mission, principles, and objectives of five strategic goals—excellence, data, cybersecurity, value, and people. To support these goals, the plan defines 14 objectives to be accomplished over 4 years. For example, the plan defines objectives for increasing the effectiveness of NASA's IT strategy execution through disciplined program and project management.

In addition, NASA has improved upon the prior plan by identifying performance measures that allow the agency to determine whether it is succeeding in the implementation of its goals. For example, in order to increase the effectiveness of its IT strategy execution, the Office of the CIO expects 85 percent of projects to be in conformance with approved project plans by the end of fiscal year 2018. As another example, to prepare its employees to achieve NASA's IT vision, the Office of the CIO plans to, by the end of fiscal year 2020, identify skills gaps and ways to close the gaps based on the workforce strategy.

However, similar to the prior plan, the updated plan does not fully describe strategies NASA intends to use to achieve the desired results or descriptions of interdependencies within and across projects. Specifically, the plan discusses how the agency intends to achieve its strategic goals and objectives through various activities. For example, according to the plan, to increase the effectiveness of investment analysis and prioritization, NASA intends to implement a financial management process that integrates Office of the CIO, center, and mission directorate IT spending. The plan states that this process will map IT investments to NASA's vision and strategy, as well as enable high-quality internal and external investment insight and reporting.

However, the updated plan does not further describe the strategies NASA intends to use to accomplish these activities, including a schedule for significant actions and the resources needed to achieve this objective. For instance, the plan states that the Office of the CIO will define clear lines of authority and accountability for IT between the agency and NASA's centers, but does not describe a strategy, including time frames and resources, for accomplishing this. Additionally, the plan does not describe interdependencies between projects, which is essential to help define the relationships within and across projects and major initiatives.

[28]NASA's 2018 agency-wide strategic plan was finalized on February 12, 2018.

According to NASA's CIO, the updated strategic plan was kept at a higher level with the expectation that more detailed implementation plans (e.g., tactical plans and roadmaps) would define the necessary projects and interdependencies. However, NASA has not defined guidance for developing the implementation plans to ensure that any plans developed will fully describe strategies and interdependencies, or time frames for when these plans will be completed. Until NASA incorporates the key elements of a comprehensive IT strategic plan, it will lack critical information needed to align information resources with business strategies and investment decisions.

NASA Has Gaps in Its IT Workforce Planning Efforts

Key to an agency's success in managing its IT investments is sustaining a workforce with the necessary knowledge, skills, and abilities to execute a range of management functions that support the agency's mission and goals. Achieving such a workforce depends on having effective human capital management consistent with workforce planning activities pursuant to federal laws[29] and guidance.[30]

[29]Federal Cybersecurity Workforce Assessment Act of 2015, Pub. L. No. 114-113, Div. N, Title III, 129 Stat. 2242, 2975-77 (Dec. 18, 2015); Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Div. A, Title VIII, Subtitle D—Federal Information Technology Acquisition Reform, Pub. L. No. 113-291, § 835, 128 Stat. 3292, 3449 (Dec. 19, 2014), codified at 41 U.S.C. § 1704 note; E-Government Act of 2002, Pub. L. No. 107-347, § 209 (Dec. 17, 2002), 44 U.S.C. § 3501 note; and Pub. L. No. 104-106, Div. D and Div. E, § 5125(c)(3) (Feb. 10, 1996), codified at 40 U.S.C. § 11315(c)(3).

[30]In 2002, OPM released a *Human Capital Assessment and Accountability Framework*—developed jointly with GAO and OMB—that identifies five human capital systems that together provide a consistent, comprehensive representation of human capital management for the federal government (http://www.opm.gov/hcaaf_resource_center/, accessed July 1, 2016). In addition, GAO, OPM, and OMB have established subsequent guidance on key principles and steps associated with workforce planning that agencies can utilize in their efforts to assess and address IT skill gaps. GAO-17-8 and OPM, *Workforce Planning Model*, https://www.opm.gov/policy-data-oversight/human-capital-management/reference-materials/ (accessed June 7, 2016). OPM, *IT Program Management Career Path Guide*, Nov. 18, 2011 and, for example, OMB, Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 27, 2016); *Federal Cybersecurity Workforce Strategy*, Memorandum M-16-15 (Washington, D.C.: July 12, 2016); *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, Memorandum M-16-04 (Washington, D.C.: Oct. 30, 2015); *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015);); and *Guidance for Specialized Information Technology Acquisition Cadres* (Washington, D.C.: July 13, 2011); and *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

Specifically, OMB requires agencies to develop and maintain a current workforce planning process.[31] In addition, we reported in 2016 on the importance of setting a strategic direction for IT workforce planning, identifying skills gaps and implementing strategies to address them, and monitoring and reporting on progress in addressing the identified skills gaps.[32] We identified eight key IT workforce planning activities that are essential to agency efforts to establish an effective IT workforce:

1. establish and maintain a workforce planning process;
2. develop competency and staffing requirements;
3. assess competency and staffing needs regularly;
4. assess gaps in competencies and staffing;
5. develop strategies and plans to address gaps in competencies and staffing;
6. implement activities that address gaps (including IT acquisition cadres, cross-functional training of acquisition and program personnel, career paths for program managers, plans to strengthen program management, and use of special hiring authorities);
7. monitor the agency's progress in addressing competency and staffing gaps; and
8. report to agency leadership on progress in addressing competency and staffing gaps.[33]

The Office of the CIO has had IT workforce planning efforts underway since 2015 that are intended to address the workforce planning activities listed above; however, the office has not finalized or implemented any of the planned actions. The office recently began working to establish a more comprehensive workforce strategy for fiscal year 2019 to align with the agency's increased emphasis on improving the overall workforce. Specifically, in the draft NASA Strategic Plan, the agency established a workforce development goal and two strategic objectives that relate to its IT workforce and call for, among other things, workforce training and efforts to increase cybersecurity awareness to reduce cybersecurity risks.

[31]OMB, *Circular A-130, Managing Information as a Strategic Resource* (Washington, D.C.: July 27, 2016).

[32]GAO-17-8; and GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[33]GAO-17-8 and GAO-04-39.

Nevertheless, NASA has gaps in its IT workforce planning efforts. Of the eight key IT workforce planning activities that we previously outlined, NASA partially implemented five and did not implement three. Table 2 shows the extent to which NASA has implemented each IT workforce planning activity and provides examples of workforce practices planned or implemented, as well as those not yet undertaken.

Table 2: Evaluation of the National Aeronautics and Space Administration's (NASA) Implementation of Key Information Technology (IT) Workforce Planning Activities

Key activities	Rating	Examples of NASA's efforts to address relevant practices
Establish and maintain a workforce planning process	Partially implemented	NASA's Chief Information Officer (CIO) has taken steps to establish elements of a workforce planning process. Specifically, the CIO is responsible for IT workforce planning and requires center CIOs to implement workforce processes, hire appropriate IT skill sets, and offer training and development opportunities. In addition, the agency has established elements of the workforce planning process for how to respond to changing mission priorities and IT. Further, through its annual budget guidance, NASA's Office of Human Capital Management provides maximum annual staffing limits and offers strategic planning and budget development guidance for workforce planning, and its Office of the CIO identifies recruiting and training activities for high-priority positions and for retaining staff through IT professional career tracks. However, the process is not complete because NASA lacks procedures for how the process will be implemented. For example, NASA's desk guide for workforce planning provides only a general description of workforce practices and lacks details about how the practices are to be implemented. NASA also has not established how it will maintain a current IT workforce planning process. Further, the agency has not yet finalized or implemented a human capital operating plan.
Develop competency and staffing requirements	Partially implemented	To address this key activity, the Office of the CIO identified 15 mission-critical IT workforce competencies and skills. The Office of the CIO also assessed staffing requirements by reviewing staffing for business IT, analyzing mission staffing data submitted by centers, and identifying current and future IT staffing estimates. However, the agency has not formally established competencies or staffing requirements in an approved IT workforce plan that could be linked directly to strategic and annual performance plans.
Assess competency and staffing needs regularly	Not implemented	NASA did not implement this key activity. According to agency officials, including the Associate CIO for Capital Planning and Governance, the Office of the CIO does not yet assess competencies or staffing needs regularly. Further, we determined that the agency has not projected staffing needs far enough into the future (i.e., 3 to 5 years) to ensure that estimates remain aligned with the agency's long-term goals and objectives.
Assess gaps in competencies and staffing	Partially implemented	While the agency has taken action to assess gaps in competencies and staffing, the IT workforce gap assessments are outdated and not regularly updated. NASA's CIO is responsible for working with the Office of Human Capital Management to analyze gaps in competencies and staffing, and an assessment was performed in 2015. However, NASA has not since updated its assessment and its policy does not require the CIO to conduct gap analyses on a regular basis. According to the agency's new IT strategic plan, the Office of the CIO plans to identify skills gaps based upon a new workforce strategy by fiscal year 2020.

Key activities	Rating	Examples of NASA's efforts to address relevant practices
Develop strategies and plans to address gaps in competencies and staffing	Partially implemented	NASA's CIO has taken specific actions to address this key activity. Specifically, the CIO has delegated certain tasks associated with strategies and plans for addressing gaps in competencies and staffing to staff within the Office of the CIO or center CIOs. In so doing, the CIO and her designees identify, recruit, hire, train, and provide annual performance reviews for officials leading major IT programs. In addition, staffing and skills requirements are identified via program reviews. Staff for major IT programs are recruited and hired through NASA's recruiting and hiring process. Annual performance reviews are conducted and training needs are assessed between the direct supervisor and the employee. Center CIOs are responsible for training and expertise of enterprise programs assigned to that center. However, NASA has not yet fully developed strategies or plans to address identified gaps. Specifically, NASA has not yet established a talent management plan to close staffing and competency gaps, manage staffing surpluses, maintain the strengths of the existing workforce, or mitigate risks. The chief of the Office of Human Capital Management reported that the agency is currently developing a talent management program intended to consolidate competencies, staffing requirements, talent management, and recruitment; however, the program is not expected to be complete until fiscal year 2019.
Implement activities that address gaps (including IT acquisition cadres, cross-functional training of acquisition and program personnel, career paths for program managers, plans to strengthen program management, and use of special hiring authorities)	Not implemented	NASA has not yet implemented activities to address gaps identified. NASA's CIO and other officials from the Office of the CIO reported that they have not developed the required acquisition human capital plan. As a result, they have not yet performed the critical prerequisites for the plan, including analyzing current IT acquisition staffing challenges; determining if developing or expanding the use of cadres would improve IT program results; outlining a plan to pilot or expand cadres for an especially high-risk IT area; or addressing how the agency is meeting its human capital requirements to support timely and effective acquisitions.
Monitor the agency's progress in addressing competency and staffing gaps	Partially implemented	NASA has begun to address this key activity by developing policies calling for the agency to monitor progress in addressing competency and staffing gaps and requiring the CIO to approve the selection of center CIOs and provide input into their performance evaluations. Specifically, *NASA Policy Document 2800.1B – Managing Information Technology* directs the CIO, in coordination with the Office of Human Capital Management, to regularly conduct a gap analysis and develop and execute a strategy for matching NASA's needs with the required IT workforce skills. However, NASA has not established procedures for how progress will be measured or required the CIO to assess progress annually. The agency also developed criteria it planned to use to determine if efforts to monitor progress had been successful but never incorporated the criteria in approved plans. Officials in the Office of the CIO stated that NASA policy is currently being updated to add a requirement to annually conduct these key activities, but time frames for when this will be completed have not been established.

Key activities	Rating	Examples of NASA's efforts to address relevant practices
Report to agency leadership on progress in addressing competency and staffing gaps	Not implemented	NASA has not implemented this activity. The Office of the CIO does not yet report to agency leadership on progress in addressing competency and staffing gaps. According to the Associate CIO for Technology and Innovation, reports are not made to agency leadership on IT workforce gaps. Officials in the Office of the CIO stated that NASA intends to update its policy in the future to add an annual requirement to report to head of agency on progress made in improving IT personnel.

Legend: Partially implemented - NASA's IT workforce policies, procedures and planning documents addressed some, but not all of the practices for the leading activity

Not implemented - NASA's IT workforce policies, procedures and planning documents did not address any of the practices for the leading activity

Source: GAO analysis of National Aeronautics and Space Administration (NASA) data. | GAO-18-337

According to NASA's CIO, the Office of the CIO put IT workforce planning activities on hold in 2015 pending the outcome of more comprehensive, agency-wide efforts. Specifically, the agency began planning and developing a new phased program—the Mission Support Future Architecture Program—designed to deliver workforce and other mission support services, including a talent management program.[34] Phase 1 of the new phased Mission Support Future Architecture Program began in May 2017.

According to the NASA CIO, the Office of the CIO is expected to be part of a future phase and to renew its IT workforce planning as part of that effort. However, the CIO did not have an estimate for when the Office of the CIO would join the program. Until NASA implements all of the key IT workforce planning activities discussed in this report, the agency will have difficulty anticipating and responding to changing staffing needs. Further, NASA will face challenges in controlling human capital risks when developing, implementing, and operating IT systems.

NASA's IT Governance Approach Does Not Fully Address Leading Practices

Leading practices for governing IT, such as those identified by GAO in its IT investment management framework, call for agencies to establish and follow a systematic and organized approach to investment management to help lay a foundation for successful, predictable, and repeatable

[34]NASA's Executive Council took action in May 2017 to improve the agency's efficiency and effectiveness by establishing the Mission Support Future Architecture Program for, among other things, workforce planning. The program engaged a team to develop an overall implementation plan, a management structure, and an approach for executing a phased enterprise architecture for mission support services.

decisions.[35] Critical elements of such an approach include instituting an IT investment board (or boards), developing and documenting a governance process for investment selection and for investment oversight, and establishing governance policies and procedures for managing the agency's overall IT investment portfolio.

NASA Has Not Fully Instituted an Effective Governance Structure

Instituting an effective IT governance structure involves establishing one or more governance boards, clearly defining the boards' roles and responsibilities, and ensuring that they operate as intended. Moreover, Section 811(a) of the National Aeronautics and Space Administration Transition Authorization Act of 2017 directs the agency to ensure that the NASA CIO, mission directorates, and centers have appropriate roles in governance processes. The act also calls on the Administrator to provide, among other things, an IT program management framework to increase the efficiency and effectiveness of IT investments, including relying on metrics for identifying and reducing potential duplication, waste, and cost.

NASA has established three boards focused specifically on IT governance—an IT Council which is its executive-level IT board, a CIO Leadership Team, and an IT Program Management Board which provides oversight of programs and projects. Meeting minutes for the three IT-specific governance bodies identified above revealed that these groups are meeting as required by their charters.

Further, two of NASA's agency-wide councils (whose governance responsibilities extend beyond IT) also play a role in IT governance. Specifically, the Mission Support Council is the governance body to which the IT Council escalates unresolved decisions, and the Agency Program Management Council is responsible for reviewing and approving highly-specialized IT. In addition, NASA centers have the option to create center-specific IT governance boards to make decisions about center-level IT investments under the authority of center CIOs.

Table 3 describes the roles of the IT-specific governance boards, the agency-wide councils with roles in IT governance, and the center-level IT governance boards. The table also includes additional details on how frequently the councils and boards meet, the dollar thresholds NASA has established to determine which investments each council or board reviews, and which officials serve as members of the boards.

[35] GAO-04-394G.

Table 3: National Aeronautics and Space Administration (NASA) Information Technology (IT) Governance Councils and Boards

Council or board	Role in IT governance	Minimum frequency of meetings	Thresholds	Member(s)
Mission Support Council (agency-wide body with responsibility beyond IT)	Senior NASA decision-making body responsible for managing mission support issues, including those that require a high degree of integration or are highly visible. Its scope of authority includes the agency's mission support investments in facilities, workforce, infrastructure, and IT. For IT, this council is to review the IT strategy, enterprise architecture, and IT policy changes. The council chartered the IT Council to govern IT. When the IT Council cannot resolve governance decisions, they are escalated to this council.	Monthly	Not applicable	• Deputy Associate Administrator (chair) • Associate Administrator • Associate Administrator for Mission Support • Chief Information Officer (CIO) • Chief Financial Officer • Chief, Safety and Mission Assurance
Agency Program Management Council (agency-wide body with responsibility beyond IT)	Senior decision-making body that is responsible for baselining and assessing the performance of NASA projects, programs, and investments by mission directorates and across the agency. It is intended to ensure successful outcomes supporting the achievement of NASA strategic goals. This council is responsible for approving highly-specialized IT, regardless of the size of the investment.	Monthly	Not applicable	• Associate Administrator (Chair) • Deputy Associate Administrator • Chief Engineer • Chief, Safety and Mission Assurance • Associate Administrators for the Directorates • CIO • Chief Financial Officer • General Counsel • Chief Health and Medical Officer • Chief Scientist • Chief Technologist
IT Council	IT-specific governance board and also NASA's executive-level IT governance board. According to its charter, this council sets policy for all of NASA's IT, including highly-specialized IT. However, its program management authority is limited to IT services delivered and managed by the CIO (i.e., IT that is not highly-specialized).	Monthly[a]	Above $10 million	• CIO (chair) • Senior executive leadership from mission directorates • Senior executive leadership from field centers • Senior executive leadership from NASA mission support offices

Council or board	Role in IT governance	Minimum frequency of meetings	Thresholds	Member(s)
CIO Leadership Team	Advisory board for the CIO intended to serve as a change agent and sounding board by providing visibility into the IT requirements, operations, performance, risk management strategies, and stakeholder issues for the centers and mission directorates. According to its charter, the team's responsibilities include (1) overseeing the implementation of agency IT strategy and policy; (2) identifying opportunities and investment recommendations; (3) assessing the impact of and providing recommendations on proposed center and mission directorate investments; and (4) reviewing or recommending decisions before they are submitted to the IT Council.	Every other week[b]	$1-10 million	• Deputy CIO (chair—formally delegated by NASA CIO) • Associate CIO for Capital Planning and Governance • Associate CIO for IT Security • Associate CIO for Technology and Innovation • Associate CIO for Enterprise Services and Integration • Senior Advisor, Cybersecurity • A representative from NASA's Shared Services Center • Nine field center CIOs as well as the CIO from the Jet Propulsion Laboratory • IT representatives from NASA's four mission directorates
IT Program Management Board	This board is to provide a forum for high-level agency participation in the oversight and evaluation of NASA's IT programs and projects. Specifically, the board is to oversee IT programs and projects from development through implementation. It is to conduct key decision point reviews to ensure that programs and projects meet their cost, schedule, and scope commitments.	Bimonthly	Less than $1 million	• Deputy CIO (chair—formally delegated by NASA CIO) • Division Chief, Office of the CIO Capital Planning and Governance Division • Representative from the CIO Leadership Team • Representative from the Office of the Chief Engineer • Center representative (two) • Mission support directorate representative (two) • Enterprise Architecture Lead (non-voting member) • IT Security representative (non-voting member)

Council or board	Role in IT governance	Minimum frequency of meetings	Thresholds	Member(s)
Center-specific IT governance boards	Responsible for approving center-specific IT investments.	Varies by center[c]	Less than $1 million	• Center CIOs (chair) • At the Goddard Space Flight Center, the tactical planning group responsible for IT investment management consists of staff appointed by the directors of the center's directorates • Johnson Space Center's governance council also includes the representatives from the center's directorates, but it also includes a center Chief Financial Officer representative and representatives from the procurement office and certain mission programs

Source: GAO analysis of National Aeronautics and Space Administration (NASA) information. | GAO-18-337

[a]After the IT Council began meeting, members decided to meet monthly instead of quarterly and updated the charter in February 2018 to reflect this change.

[b]As of April 2018, NASA's IT governance lead stated that the agency intended to update the team's charter to call for more frequent meetings. Our review of documentation provided by NASA showed that the agency had scheduled the team to meet during 2018 on every week except for the one week per month when the IT Council is scheduled to meet.

[c]The NASA documentation we reviewed did not identify an established minimum frequency for center board meetings. As such, if NASA centers establish center-specific IT governance boards, the centers are to determine how frequently each board should meet.

Although it has established and assigned responsibilities for the aforementioned governance councils and boards, NASA has not yet fully instituted an effective investment board governance structure for several reasons.

- ***Planned improvements to the IT governance structure are not yet complete.*** NASA has established new governance boards in addition to the boards listed above, but has not yet approved charters to guide their operations. Specifically, the Office of the CIO has revised its governance structure to establish six new boards, one for each of its IT programs. Agency officials, including the IT governance lead, reported that the boards had been established; however, as of December 2017, NASA had not yet approved charters defining the new governance bodies' membership, functions, and interactions with other governance boards.[36]

[36]The NASA Inspector General reported in October 2017 that the program boards had not been implemented. See National Aeronautics and Space Administration Office of Inspector General, *NASA's Efforts to Improve the Agency's Information Technology Governance*, IG-18-002, (Washington, D.C.: Oct. 19, 2017).

- ***Roles and responsibilities of the IT governance boards and agency-wide governance councils are not clearly defined.*** NASA continues to operate a federated governance model with decentralized roles and responsibilities for governance of mission and business IT investments. Business IT is selected and approved by the IT-specific governance boards, but mission IT follows a different path for investment selection in that it is not reviewed and approved by the CIO along with other IT investments proposed for selection. Instead, the Agency Program Management Council's reviews focus on the selection of overall mission programs, and not on selecting IT. As a result, mission IT has historically been reported to the Office of the CIO only if the program has been designated as a major agency IT investment to be reported to OMB.

  NASA has begun making changes to its decentralized governance approach in response to provisions in legislation commonly referred to as the Federal Information Technology Acquisition Reform Act[37] that are intended to ensure that the CIO has visibility into both mission and business IT investments. However, the agency has not yet developed policies and procedures to clarify how these changes will affect the CIO's and governance boards' roles and responsibilities. For example, in January 2017, the IT Council approved an updated definition for highly-specialized IT[38] and established new expectations about the extent to which highly-specialized IT investments would be reviewed by the NASA CIO.

  However, NASA has not clarified roles and responsibilities for identifying such investments and ensuring they are reported by mission directorate programs to the CIO. In addition, the agency has not yet outlined procedures for how these investments that are overseen by the agency-wide Agency Program Management Council are to be reported to the CIO or IT-specific governance boards.

  During a January 2017 IT Council meeting, the NASA CIO acknowledged that roles and responsibilities for IT governance were

[37]Federal Information Technology Acquisition Reform provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, § 831 (Dec. 19, 2014).

[38]NASA clarified that highly-specialized IT is "any equipment, system and/or software that is used in the acquisition, storage, retrieval, manipulation and/or transmission of data or information which comprises or is embedded in a mission platform, or a platform required for mission simulation, execution or operations."

unclear and that it would take 1 to 2 years to clarify them. In July 2017, the Deputy CIO recognized that significant work remained for NASA to achieve a consistent agency-wide governance approach with established roles and responsibilities.

- ***While the IT governance boards are meeting regularly, they are not consistently operating as intended.*** Board charters finalized in 2016 defined the membership for the governance boards and established expectations for the expertise to be made available to support board decisions. However, the boards are not consistently operating with all designated board members in attendance. For example, the Chief Engineer was designated as a member of the IT Council, but the council's meeting minutes indicated that the Deputy Chief Engineer regularly attends the council meetings instead.

  In addition, IT Program Management Board meetings are consistently held with fewer voting members than designated by the board's charter. The board's meeting minutes indicated that fewer than six voting members regularly attend board meetings instead of the eight voting members outlined in the board charter. For example, the minutes showed that each meeting has been held with only one center and mission support directorate representative—instead of the two required by the charter.

NASA officials, including the Associate CIO for Capital Planning and Governance, stated that planned efforts to update the governance structure and develop additional guidance for IT investment management have impacted the agency's time frames for fully establishing its new boards and defining their roles and responsibilities. Specifically, these officials stated that the Office of the CIO is working to develop a comprehensive IT framework intended to update the governance structure, fully establish the new governance boards, and define governance roles and responsibilities. According to the officials, this framework is expected to be finalized in 2018, but the office did not provide a detailed schedule with milestones for completing the framework. Without a detailed schedule for updating the governance structure and establishing a comprehensive IT framework to help ensure that the revised governance boards are fully established and operating as intended, NASA may not be able to improve IT governance in accordance with the requirements in the National Aeronautics and Space Administration Transition Authorization Act of 2017.

NASA Has Not Completed or Updated Governance Selection Process Policies and Procedures and Lacks Established Guidance for Reselecting Investments

According to our IT investment management guide, defining policies and procedures for selecting investments provides investment boards and others with a structured process and a common understanding of how investments will be selected. Selection policies and procedures should, among other things, establish thresholds or criteria (e.g., investment size, technical difficulty, risk, business impact, customer needs, and cost-benefit analysis) for boards to use in identifying, analyzing, prioritizing and selecting new IT proposals.

In addition, outlining a process for reselecting ongoing projects is intended to support board decisions about whether to continue to fund projects not meeting established goals or plans. Using the defined selection process promotes consistency and transparency in IT governance decision making. Further, after the guidance has been developed, organizations must actively maintain it, making sure that it always reflects the board's current structure and the processes that are being used to manage the selection of the organization's IT investments.

NASA's defined selection process policies and procedures designated the CIO with responsibility to ensure that IT governance, investment management, and program/project management processes are integrated to facilitate the selection of appropriate IT investments. The agency has established multiple policies and procedures outlining certain aspects of how both mission programs and business IT investments are to be planned, such as standardized templates for requesting approval to plan investments and direction for teams to use in planning for investments. In addition, the Office of the CIO has established a *Capital Planning and Investment Control Guide* for business IT investments and issues annual budget guidance for requesting funding for IT investments.

The agency's selection process also includes specific IT governance processes developed by centers for the investments they review. For example, Goddard Space Flight Center had developed additional center-specific guidance assigning lead responsibility for assessing new and ongoing projects. The center also has established predetermined criteria, such as whether projects conflict, overlap, or are redundant with other projects, and the risk if the investment was not funded.

Nevertheless, NASA's established process does not yet define thresholds or criteria (e.g., qualitative or quantitative data) to be analyzed and compared when governance boards make decisions to select investments. Charters for NASA's governance boards outline the functions these boards are to perform and direct them to be involved in IT

governance. However, the charters do not outline specific thresholds or procedures that the boards are to follow in selecting investments.

For example, NASA's process does not fully define how investment risks are to be evaluated. NASA policy establishes dollar thresholds for IT governance board reviews, but does not define any other parameters for how risk will be evaluated. In addition, NASA has established an expectation that the new capital investment review process is to yield risk-based decisions for all investments and help mitigate IT security risks. However, guidance for capital investment reviews does not address how investment risks are to be evaluated.

Moreover, NASA's selection process policies and procedures have not been updated to reflect efforts to improve governance. Its guidance for selecting investments (and for all aspects of its governance process) is fragmented, and the agency has not updated its policies and procedures to reflect current selection practices. In addition, this guidance does not yet reflect recent efforts to clarify and standardize the definitions of fundamental IT investment terms, such as "information technology" and "major" investments.

Further, while NASA has begun changing its selection process to ensure that the CIO and IT governance boards will be provided data about all IT investments, including mission IT investments such as highly-specialized IT, the agency's selection policies have not been updated to reflect these changes. NASA's *Capital Planning and Investment Control Guide* does not require all investments to be included in the selection process (or other IT governance processes) and the NASA *Space Flight Program and Project Management* procedures for mission program governance do not address whether or how the investments within mission programs are to be reported to the agency's IT-specific governance boards.

In addition, NASA has not yet defined a reselection process for IT investments. Current policies and guidance for selecting investments do not clearly define a consistent approach for how performance is to be considered in reselecting investments. Without a defined reselection process, the agency's boards lack structure and a common understanding about how to make decisions about whether to continue to fund projects not meeting established goals or plans.

NASA officials acknowledged that the current policies and procedures do not establish sufficient content within the business cases and IT plans for proposed investments to support effective governance decision making.

The agency has begun working to update its policy for IT program and project management but did not expect to complete the update until April 2018. Further, even when this key IT investment management policy is updated, the agency will still need to update related policies and procedures to reflect changes it has made but not yet documented in the investment selection process. NASA has not yet established plans for when all needed updates to the policies and procedures will be completed.

Until NASA updates its IT governance policies and procedures to establish thresholds and procedures to guide its boards in decision making and outline a process for reselecting investments, the agency will be limited in its assurance that the investment selection process will provide a consistent and structured method for selecting investments. Further, until all relevant governance policies and procedures are updated to reflect current investment selection practices and proposed changes intended to provide the CIO with data about mission IT, the CIO will not be positioned to minimize investments that present undue risk to the agency and ensure accountability for both business and mission IT.

NASA Lacks Criteria for Assessing Investment Performance and Ensuring Oversight of All Investments

Organizations that provide effective IT investment oversight have documented policies and procedures that, among other things, ensure that data on actual performance (e.g., cost, schedule, benefit, and risk) are provided to the appropriate IT investment board(s). In addition, such organizations establish procedures for escalating or elevating unresolved or significant issues; ensure that appropriate actions are taken to correct or terminate underperforming IT projects based on defined criteria; and regularly track corrective actions until they are completed.

As with investment selection, NASA has established multiple policies and procedures for the oversight of IT investments. In October 2015, the agency added to its oversight processes by establishing a capital investment review process to improve the quality of the information available for investment oversight and established a matrix defining dollar thresholds to delineate oversight among the IT governance boards. The IT Program Management Board is also assigned specific oversight responsibilities for reviewing investment cost, schedule, performance, and risk at key lifecycle decision points for investments submitted for its review. In addition, the IT Program Management Board's charter requires this board to track, among other things, board decisions about investments and action items.

In implementing NASA's oversight practices, the IT Program Management Board consistently reviewed updates on investment performance (i.e., cost, schedule, and benefits) and progress. In addition, the IT Program Management Board's oversight decisions about IT investments are documented in meeting minutes,[39] and the board also records any action items identified for investments in the decision memorandums it submits to the CIO.

Nevertheless, we identified limitations in NASA's established oversight policies and procedures. For example, the agency's policies and procedures require IT investments to report data to the governance boards at key decision points but do not establish specific thresholds or other criteria for the governance boards to use in overseeing the investments' performance or escalating investments to review by other boards. The oversight guidance also does not specify the conditions under which a project would be terminated.

In addition, weaknesses we identified in oversight of specific NASA IT investments highlighted additional limitations of the established oversight process.

- Specifically, NASA did not have a mechanism for alerting the IT Program Management Board to provide oversight if investments were underperforming or overdue for review. For example, significant schedule overruns did not trigger additional oversight for one investment. In March 2015, NASA approved the proposed design for an investment to implement a security tool in June 2015 at an expected cost of $1.3 million. Although the project fell 13 months behind schedule and encountered unforeseen challenges, the IT Program Management Board did not review the investment again until June 2017—2 years later.[40]
- Not all IT investments followed the established oversight process. For example, in our review of governance board meeting minutes and documentation, we identified an investment that was close to completion before the IT Program Management Board reviewed its

[39]Johnson Space Center standardized documentation for all center IT governance decisions in meeting minutes and consistently recorded additional supporting detail about IT decisions.

[40]The CIO was informed only that the investment had been approved; the memorandum did not document the significant concerns of governance board members or the gap between reviews of the investment.

proposed design. Specifically, in February 2016, the board was asked—1 day before the investment was to become operational—to (1) approve the proposed design and (2) grant authority to operate for the investment intended for use by NASA staff and external partners. Although concerns about limited oversight were noted, the investment was approved.[41]

- Further, NASA lacks procedures to ensure that action items identified are tracked. We identified instances in which the IT Program Management Board did not consistently track action items identified for IT investments. NASA's investments typically report back to the IT Program Management Board at future decision point reviews about steps taken to address documented action items. However, the board's meeting minutes and documentation identified multiple examples of investments that were returned to the board at future decision points without reporting on whether identified action items had been addressed.

Moreover, NASA's oversight processes do not encompass highly-specialized or other IT that supports mission programs. After reviewing NASA's fiscal year 2015 budget request, OMB directed NASA to identify unreported IT investments throughout the agency to ensure that all related spending would be documented.[42] NASA established a team in 2016 to explore how to identify such investments so that they could be reported to the CIO. The team initiated efforts to identify such investments in mission directorates and evaluated various mechanisms that NASA could employ to detect unreported IT. However, the agency has not yet finalized decisions about how to implement the team's recommendations, including those for fully identifying investments for all mission directorates or determining which mechanisms to employ to identify unreported IT. According to NASA officials, time frames for completing these activities have not yet been established.

[41]The investment was approved with the condition that the functional cost and risks be reviewed and reassessed by the end of the fiscal year, but there is no evidence the investment was reviewed again by the IT Program Management Board. The CIO Leadership Team was briefed on an exit strategy for this investment in May and July 2016, and the investment may have formally been elevated to that board for discussion, but neither board's meeting minutes documented such a decision.

[42]NASA's Office of the CIO reported that certain mission directorates had begun to have success in identifying previously unreported IT. However, as of the fiscal year 2018 budget, the CIO continued to have greater insight and influence over investments in agency IT services and space communications and navigation than in other mission IT investments.

In July 2017, NASA officials, including the Deputy CIO, acknowledged in governance board meeting minutes describing needed improvements, that the agency had not yet fully identified its IT footprint and needed to establish a comprehensive investment management process to address federal requirements, including those governing processes for selecting, reselecting, and overseeing IT investments. NASA officials explained that important progress had been made in improving oversight practices, but that efforts to implement more thorough capital investment reviews and identify IT investments across the agency had not yet been completed. The officials reported that they anticipated additional improvement to be made by the next annual budget cycle.

However, expanding NASA's oversight of IT will require continued coordination with the mission directorates to work through any needed changes to the longstanding differences in NASA's management of mission and business IT. The scope and complexity of such efforts are likely to be significant and may take time to plan and implement. Clearly defining how IT across the agency is to be identified and reported to the CIO would likely involve changes to policies and processes within and across NASA's IT, engineering, and mission program areas and would involve expertise and collaboration from those same groups. Until such practices are fully established, NASA will continue to operate with limitations in its oversight process and projects that fall short of performance expectations. In addition, the agency will face increased risk that its oversight will fail to (1) prevent duplicative investments, (2) identify opportunities to improve efficiency and effectiveness, and (3) ensure that investment progress and performance meet expectations.

NASA Has Not Yet Fully Defined Policies and Procedures for Managing Investments as a Portfolio

The IT investment management framework developed by GAO notes that, as investment management processes mature, agencies move from project specific processes to managing investments as a portfolio. The shift from investment management to IT portfolio management enables agencies to evaluate potential investments by how well they support the agency's missions, strategies, and goals. According to the framework, the investment board enhances the IT investment management process by developing a complete investment portfolio. As part of the process to develop a complete portfolio, an agency is to establish and implement policies and procedures for developing the portfolio criteria, creating the portfolio, and evaluating the portfolio.

NASA has not yet fully defined its policies and procedures for developing the portfolio criteria, creating the portfolio, and evaluating the portfolio. In its *Annual Capital Investment Review Implementation Plan*, dated

October 2015, NASA began documenting policies for IT portfolio management and procedures for creating and evaluating the portfolio. For example, the procedures state that NASA is to update its IT portfolio annually in conjunction with the agency's planning and budgeting process. Additionally, in its *IT Capital Planning and Investment Control Process* guide, dated October 2006, NASA outlined procedures the agency can use to analyze the portfolio by establishing factors that should be taken into consideration, including the relative benefits, costs, and risks of the investment compared to all other proposals and the strength of the investment's linkage to NASA's strategic business plan.

However, these documents do not constitute a comprehensive IT portfolio management process in that they do not specifically define the procedures for creating and modifying the IT portfolio selection criteria; analyzing, selecting, and maintaining the investment portfolio; or reviewing, evaluating, and improving the performance of its portfolio. Further, the policies and procedures have not been updated to reflect current NASA practices. Specifically, the current policies and procedures have not been updated to reflect changes the agency made to its capital investment review process that are relevant to portfolio management.

According to NASA officials, the reason that the agency has not fully defined its policies and procedures is because they are intended to be part of a new IT portfolio management framework that also requires NASA to make changes to its investment management process. Specifically, the IT portfolio management plan that NASA drafted in January 2017 called for the agency to develop new IT investment criteria, discover currently unreported IT investments, develop an investment review process, and implement an IT investment dashboard and reporting tool, and a communications plan.

Although the IT Council has not yet approved the IT portfolio management plan, NASA has begun work to address elements of the draft plan, including building the requirements for an IT dashboard and reporting tool for implementation in 2018. In addition, according to Office of the CIO officials, the capital planning team is continuing to work with stakeholders to develop a comprehensive IT framework and investment review process. However, no firm dates have been established for the approval and implementation of the final plan or the framework. Until NASA fully defines its policies and procedures for developing the portfolio criteria, creating the portfolio, and evaluating the portfolio, the agency will lack assurance it is identifying and selecting the appropriate mix of IT projects that best meet its mission needs.

NASA Has Not Fully Established an Effective Approach for Managing Cybersecurity Risk

We have previously reported that securing federal government computerized information systems and electronic data is vital to the nation's security, prosperity, and well-being. Yet, the security over these systems is inconsistent and agencies have faced challenges in establishing cybersecurity approaches. Accordingly, we have recommended that federal agencies address control deficiencies and fully implement organization-wide information security programs.

NIST's cybersecurity framework is intended to support federal agencies as they develop, implement, and continuously improve their cybersecurity risk management programs.[43] In this regard, the framework identifies cybersecurity activities for achieving specific outcomes over the lifecycle of an organization's management of cybersecurity risk.[44] According to NIST, the first stage of the cybersecurity risk management lifecycle—which the framework refers to as "identify"—is focused on foundational activities for effective risk management that provide agencies with the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. NIST also provides specific guidance for implementing foundational activities and achieving desired outcomes that calls for, among other things, the following:[45]

- **A risk executive** in the form of an individual or group that provides agency-wide oversight of risk activities and facilitates collaboration among stakeholders and consistent application of the risk management strategy.
- **A cybersecurity risk management strategy** that articulates how an agency intends to assess, respond to, and monitor risk associated with the operation and use of the information systems it relies on to carry out the mission.

[43]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

[44]According NIST's cybersecurity framework, there are five stages in the cybersecurity risk management lifecycle: "identify," "protect," "detect," "respond," and "recover." They are intended to aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

[45]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (SP) 800-53, Revision 4* (Gaithersburg, Md.: April 2013); *Managing Information Security Risk: Organization, Mission, and Information System View, SP 800-39* (Gaithersburg, Md.: March 2011).

- **An information security program plan** that describes the security controls that are in place or planned for addressing an agency's risks and facilitating compliance with applicable federal laws, executive orders, directives, policies, or regulations.[46]
- **Risk-based policies and procedures** that act as the primary mechanisms through which current security requirements are communicated to help reduce the agency's risk of unauthorized access or disruption of services.

However, NASA has not yet fully implemented these foundational activities of effective cybersecurity risk management.

Efforts to Establish Executive Oversight of Cybersecurity Are Underway

According to NIST guidance,[47] federal agencies should establish a risk executive in the form of an individual or group that provides organization-wide oversight of risk activities and facilitates collaboration among stakeholders and consistent application of the risk management strategy. This functional role helps to ensure that risk management is institutionalized into the day-to-day operations of organizations as a priority and integral part of carrying out missions.

NASA has developed a policy regarding the establishment of a risk executive function in accordance with NIST guidance, but it has not fully implemented the policy. Specifically, the agency's policy designates the Senior Agency Information Security Officer (SAISO) as the risk executive. According to the policy, the SAISO is charged with ensuring that cybersecurity is considered and managed consistently across the systems that support the agency and its partnerships—academic, commercial, international, and others that leverage NASA resources and extend scientific results.[48] The policy also calls for the SAISO to establish an office with the mission and resources for information security operations, security governance, and cyber-threat analysis.

In accordance with its policy, NASA has designated an Acting SAISO. Since April 2017, the Acting SAISO has led the IT Security Division within

[46]Security controls are the safeguards and countermeasures (management, operational, and technical) needed to protect the confidentiality, integrity, and availability of an information system and its information.

[47]NIST 800-39.

[48]Systems that support NASA and its partnerships provide, for example, business operations, ground support, publicly accessible web applications, and spacecraft control and communications.

the Office of the CIO—an office that coordinates information security operations, security governance, security architecture and engineering, and cyber-threat analysis.

However, the agency has not yet established a risk executive office with assigned leadership positions and defined roles and responsibilities. According to NASA documentation, the agency had planned for the office to become operational by mid-December 2016. Agency officials, including the Acting Deputy Associate CIO for Information Security, explained that an IT security program office was not established in 2016 because the planned time frame for doing so was not realistic and failed to take into account other risk management efforts competing for available resources. For example, the officials stated that the agency was focused on a priority goal of deploying a centralized tool across its centers that would provide monitoring of implemented security controls to ensure they are functioning adequately.

According to the NASA CIO, the agency planned to establish a comprehensive risk executive function by employing a cybersecurity risk manager in April 2018 and forming a program office—called the Enterprise Security Office—by September 2018. NASA's new cybersecurity risk manager began work on April 2, 2018. The agency's plan to have the new cybersecurity risk manager establish a comprehensive risk executive function should help ensure that current risk management efforts and decisions are appropriate and consistently carried out across the agency and its external partnerships.

NASA Has Not Yet Established an Agency-Wide Cybersecurity Risk Management Strategy

NIST guidance[49] states that federal agencies should establish and implement an organizational strategy for managing cybersecurity risk that guides and informs how the agency assesses, responds to, and monitors risk to the information systems being relied on to carry out its mission. The strategy should, among other things, make explicit an agency's risk tolerance,[50] accepted risk assessment methodologies, a process for consistently evaluating risk across the organization, risk response

[49]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014); SP 800-53, Revision 4; and NIST SP 800-39.

[50]Risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations. It affects the nature and extent of risk management oversight, the extent and rigor of risk assessments performed, and the context of organization strategies for responding to risk.

strategies, approaches for monitoring risk over time, and priorities for investing in risk management.

In 2015, NASA recognized the need to establish and implement an agency-wide strategy for managing its cybersecurity risks to address weaknesses it had identified with the decentralized approach it was using. Specifically, because the agency's centers had independently developed approaches for managing cybersecurity risk, there was little integration regarding risk management and practices across the agency. Further, NASA determined that the decentralized, center-level approach did not provide sufficient transparency regarding risks that could affect mission directorate programs.

To overcome the limitations of its decentralized approach, NASA planned to develop and begin implementing a comprehensive cybersecurity strategy by the end of September 2016 that was expected to include the key elements identified in NIST guidance. For example, it was expected to define the agency's risk tolerance, establish a methodology for identifying and assessing risks, and provide a clear understanding of NASA's risk posture.

However, the strategy was not completed as planned and is currently in development. According to officials in the Office of the CIO, including the Acting Deputy Associate CIO for Information Security, the strategy was not completed as planned due to the complexity and scope of the effort. For example, the officials stated that establishing an effective agency-wide strategy required insight into center-specific practices and significant input from stakeholders at all levels of NASA. In addition, these officials and the NASA CIO explained that the agency's efforts were redirected in order to respond to a new executive order from the President to develop an action plan for adopting NIST's cybersecurity framework in phases.[51]

According to NASA's CIO, the agency plans to move forward with drafting an agency-wide cybersecurity strategy that reflects the agency's approach to using NIST's framework; however, the agency has not yet

[51]Exec. Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22,391 (May 16, 2017). In responding to the executive order, NASA identified key issues that the agency needed to address in order to implement an integrated cybersecurity risk management approach. These issues include the lack of (1) a dedicated cybersecurity team to provide agency-level direction and recommendations, (2) cybersecurity workforce planning, and (3) effective processes for reporting cybersecurity risks.

established time frames for completing this effort. Until NASA establishes and implements a comprehensive strategy for managing its cybersecurity risks using NIST's framework, its ability to make operational decisions that adequately address security risks and prioritize IT security investments will be hindered.

NASA's Information Security Program Plan Does Not Fully Address Relevant Leading Practices and Is Not Finalized

NIST recommends that federal agencies develop and disseminate an information security program plan that describes the organization-wide security controls that are in place or planned for addressing the agency's risks and complying with applicable federal laws, executive orders, directives, policies, or regulations.[52] Specifically, the plan should provide a description of the agency's program management controls and common controls[53] in place or planned for meeting relevant federal, legal, or regulatory requirements; include the identification and assignment of roles, responsibilities, and coordination among organizational entities responsible for different aspects of information security; define the frequency for reviews of the security program plan; and receive approval from a senior official with responsibility and accountability for the risk being incurred.

NASA issued a draft information security program plan in November 2017 that addresses many of the components called for in NIST guidance. For example, the plan discusses

- program management controls that will be established, including the development of an inventory of its information systems, measures to determine information security performance, and an information security workforce development and improvement program;

[52]NIST, SP 800-53, Revision 4. According to NIST, security controls are the safeguards and countermeasures (management, operational, and technical) needed to protect the confidentiality, integrity, and availability of an information system and its information.

[53]Program management controls focus on organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Common controls, also referred to as inherited controls, provide a security capability for multiple information systems within an organization. When common controls are used to support a specific information system, they are referenced by that specific system as an inherited control.

- common controls that are to be implemented agency-wide, including configuration management, contingency planning, and personnel security;[54]
- roles and responsibilities for promoting collaboration and providing consolidated unclassified security operations, and incident response and IT security awareness and training capabilities;[55] and
- responsibility for ensuring that the information security program plan is maintained, approved by the NASA CIO, and reviewed annually.

However, the plan is currently in draft and incomplete. For example, it does not yet describe the majority of the security functions and services that are to be carried out by the agency's IT Security Division to address the relevant federal statutory and regulatory requirements. Specifically, the plan does not identify the agency-wide privacy controls derived from standards promulgated pursuant to federal law and guidance that, according to the agency, are an integral part of its security program.[56]

According to NASA's Acting Deputy Associate CIO for Information Security, the information security program plan has not been finalized because of an upcoming revision to NIST's guidance for implementing security controls. Specifically, a fifth revision of NIST SP 800-53 is planned for release in December 2018. NASA's Acting Deputy Associate CIO for Information Security stated that the agency intends to finalize its draft plan after incorporating the updated NIST guidance.

In the absence of an established information security program plan, NASA's view of the security controls that protect its systems will remain decentralized, and it will lack assurance that it has established oversight over security controls for all of its systems. In addition, the agency will continue to operate its systems without defined and established

[54]Configuration management controls are intended to prevent unauthorized changes to information system resources (for example, software programs and hardware configurations) and to provide reasonable assurance that systems are configured and operating securely and as intended.

[55]Incident response controls are necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

[56]Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of personally identifiable information (for example, an individual's name, social security number, or biometric records).

information security requirements that are essential to agency-wide operations.

NASA's Security Policies and Procedures Are Not Always Current or Integrated

NIST Special Publication 800-53 recommends that agencies create policies and procedures to facilitate the appropriate application of security controls.[57] If properly implemented, these policies and procedures may be able to effectively reduce the risk that could come from cybersecurity threats such as unauthorized access or disruption of services. Because risk-based policies and procedures are the primary mechanisms through which federal agencies communicate views and requirements for protecting their computing environments, it is important that they are established and kept current.

NASA has taken steps to document policies and procedures that address the security controls identified in NIST guidance for protecting information systems. For example, the agency established an overarching security policy that identified roles and responsibilities related to configuration management, contingency planning, and incident response. In addition, the agency issued procedures for implementing each of the NIST controls.

However, NASA does not have current and fully integrated policies and procedures. For example, the agency's overarching policy for implementing security controls expired in May 2017. In addition, approximately one-third of the documents that guide the implementation of these controls remained in effect past their expiration dates instead of being updated before they had expired per NASA policy requirements.

Further, in July 2017, NASA determined that cybersecurity roles and responsibilities were not always clear and sufficiently integrated across policies. For example, responsibilities were not consistently well-defined in the policies for governance, IT security, program and project management, and systems engineering. In addition, although *NASA's Policy Directive 2810.1E, NASA Information Security Policy* provided the SAISO with responsibility for the agency's cybersecurity risk, the policy assigned mission directorates control over risk decisions for their missions and programs and the centers were given the authority to implement any technical changes needed to address risk.

[57]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014) and SP 800-53, Revision 4.

NASA's *Procedural Requirement 2810.1A, Security of Information Technology* states that the agency's SAISO is responsible for ensuring that information security policies and procedures are reviewed and appropriately updated. However, according to officials in the Office of the CIO, including the specialist for IT security, responsibilities for establishing, reviewing, and updating policies and procedures are being shared by two groups: the IT Security Division, led by the SAISO, and the Capital Planning and Governance Division. Specifically, the IT Security Division controls the content of IT-related policies and procedures but does not have control over the established NASA-wide process for reviewing the policies and procedures to determine if any changes are needed to the content. Instead, the Capital Planning and Governance Division is responsible for ensuring formal review and approval of any IT-related policies and procedures through the standard agency process and schedule.

Officials from the Office of the CIO, including the specialist for IT security, also stated that they intend to (1) establish a policy management framework that would provide the SAISO with more control over policies and procedures and include an annual document review, and (2) clarify and update cybersecurity roles and responsibilities in NASA policies. However, the agency has not yet developed a plan and specific time frame for completing these activities.

In addition, the Acting Deputy Associate CIO for Information Security stated that, having expired policies and procedures is not significant because they will remain in use until they are rescinded or superseded by updated versions. However, until NASA fully updates its policies and procedures to govern security over the agency's computing environments, it will have limited assurance that controls over information are appropriately applied to its systems.

Conclusions

NASA continues to pursue efforts to improve IT strategic planning, workforce planning, IT governance, and cybersecurity, but consistently lacks the documented processes needed to ensure that policies and leading practices are fully addressed. Specifically, the agency has taken steps to improve the content of its strategic plan and established an agency-wide goal for improving its workforce. In addition, after analyzing its IT management and governance structure, NASA took action to streamline its governance boards and standardize and strengthen its selection and oversight of investments, including initiating a portfolio

management process. NASA has also moved toward new strategies and plans to bolster cybersecurity.

Nevertheless, while NASA has made progress, the agency has not yet fully addressed many of the leading IT management practices noted in this report or completed efforts to increase the CIO's authority over, and visibility into, agency-wide IT. Among other things, NASA has not fully documented a process for IT strategic planning or addressed all key elements of a comprehensive plan. In addition, it has not yet fully implemented a workforce planning process and has gaps in efforts to address leading practices. Regarding IT governance, its efforts to institute an effective governance structure and update policies and procedures for selecting IT investments are not yet complete. Moreover, NASA has not yet addressed weaknesses in its oversight practices or fully defined policies and procedures for developing an effective portfolio management process.

Similarly, although NASA continues cybersecurity improvement efforts, important elements of an effective cybersecurity approach have not been completed, including establishing a risk management strategy, an information security program plan, and updated policies and procedures. Until NASA leadership fully addresses these leading practices, its ability to overcome its longstanding weaknesses and ensure effective oversight and management of IT across the agency will remain limited. Moreover, NASA may be limited in its ability to strengthen its risk posture, including ensuring effective cybersecurity across partnerships with commercial entities, federal agencies, and other countries.

Recommendations for Executive Action

We are making 10 recommendations to the National Aeronautics and Space Administration:

- The Administrator should direct the Chief Information Officer to develop a fully documented IT strategic planning process, including methods by which the agency defines its IT needs and develops strategies, systems, and capabilities to meet those needs. (Recommendation 1)
- The Administrator should direct the Chief Information Officer to update the IT strategic plan for 2018 to 2021 and develop associated implementation plans to ensure it fully describes strategies the agency will use to achieve the desired results and descriptions of interdependencies within and across programs. (Recommendation 2)

- The Administrator should direct the Chief Information Officer 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)
- The Administrator should direct the Chief Information Officer to institute an effective IT governance structure by completing planned improvement efforts and finalizing charters to fully establish IT governance boards, clearly defining roles and responsibilities for selecting and overseeing IT investments, and ensuring that the governance boards operate as intended. (Recommendation 4)
- The Administrator should direct the Chief Information Officer to update policies and procedures for selecting investments to provide a structured process, including thresholds and criteria needed for, among other things, evaluating investment risks as part of governance board decision making, and outline a process for reselecting investments. (Recommendation 5)
- The Administrator should direct the Chief Information Officer to address weaknesses in oversight practices and ensure routine oversight of all investments by taking action to document criteria for escalating investments among governance boards and establish procedures for tracking corrective actions for underperforming investments. (Recommendation 6)
- The Administrator should ensure that the Chief Information Officer fully defines policies and procedures for developing the portfolio criteria, creating the portfolio, and evaluating the portfolio. (Recommendation 7)
- The Administrator should direct the Chief Information Officer to establish an agency-wide approach to managing cybersecurity risk that includes
    - a cybersecurity strategy that, among other things, makes explicit the agency's risk tolerance, accepted risk assessment methodologies, a process for consistently evaluating risk across the organization, response strategies and approaches for monitoring risk over time, and priorities for risk management investments; (Recommendation 8)
    - an information security program plan that fully reflects the agency's IT security functions and services and agency-wide privacy controls for protecting information; (Recommendation 9) and

- policies and procedures with well-defined roles and responsibilities that are integrated and reflect NASA's current security practices and operating environment. (Recommendation 10)

Agency Comments and Our Evaluation

We provided a draft of this product to NASA for comment. In its comments, which are reproduced in appendix II, NASA concurred with seven of the recommendations, partially concurred with two recommendations, and did not concur with one recommendation.

NASA partially concurred with our first and second recommendations. Specifically, consistent with the first recommendation, NASA agreed to fully document its strategic planning process, including the methods by which the agency defines IT needs and develops outcomes, strategies, major actions, and performance measures to meet those needs.

In addition, our second recommendation called for NASA to update the strategic plan and develop associated implementation plans. With regard to updating the plan, NASA stated that its strategic plan provides the context and parameters to support achievement of the agency's vision and mission through the strategic use of IT. The agency also stated that this plan describes the business outcomes, strategies, major actions, and performance measures to achieve the desired results.

With regard to the implementation plans related to our first and second recommendation, NASA agreed to develop the associated implementation plans for accomplishing the IT strategic plan, including descriptions of the interdependencies within and across programs. Nevertheless, in commenting on both recommendations, as well as the first recommendation, NASA stated that it does not believe that implementation plans, including specific IT capability and system changes, should be part of a strategic plan. The agency also maintained that the implementation plans, including descriptions of interdependencies within and across programs, are at a lower level than the IT strategic plan, since detailed IT implementation plans are more dynamic than the four-year NASA IT Strategic Plan.

However, our first and second recommendations do not call for NASA to incorporate implementation plans within the strategic plan. Rather, as discussed in the report, it is important that NASA document how it intends to accomplish the activities outlined in the strategic plan. Further, we continue to believe that NASA should address the weaknesses we

identified in this report by updating the strategic plan to incorporate strategies on resources and time frames to achieve desired results and descriptions of interdependencies within and across projects so that they can be understood and managed. Thus, we stand by both recommendations (recommendations 1 and 2) that the agency take these actions.

NASA did not concur with our third recommendation to implement the IT workforce planning activities noted in our report. In this regard, the agency stated that its workforce improvement efforts were already underway. Specifically, NASA stated that IT workforce planning is part of the agencywide Mission Support Future Architecture Program. It added that, among other things, this program is intended to ensure that mission support resources, including the IT workforce, are optimally structured to support NASA's mission. In addition, NASA referenced our two additional ongoing audits of the agency's IT workforce, and noted that its activities related to IT workforce planning would be centered on any recommendations resulting from those audits.

In our view, neither of these circumstances should hinder NASA from addressing our recommendation in this report. As of March 2018, the agency's IT workforce plans were out-of-date and incomplete because activities the agency had been planning since 2015 had not been finalized in an approved plan or implemented. Further, NASA had not yet determined when the Office of the CIO would become an active part of the agencywide Mission Support Future Architecture program or developed plans for when that program's assessment of the IT workforce would be completed.

Thus, instead of limiting NASA's ability to address our recommendation, implementing the workforce planning activities discussed in this report could complement the agency's ongoing and future efforts. Specifically, NASA could use the IT workforce leading practices described in this report to strengthen any new workforce plans and assess the implementation of any planned improvements. Until NASA documents an IT workforce planning process and implements all of the key IT workforce planning activities, the agency may not be effectively positioned to anticipate and respond to changing staffing needs. Further, the agency is likely to face challenges in controlling human capital risks when developing, implementing, and operating IT systems.

NASA concurred with our four recommendations aimed at addressing deficiencies in its IT governance (recommendations 4 through 7). In this

regard, the agency described planned actions intended to address each of these recommendations. For example, among other activities, the agency stated that it intended to publish charters for all IT governance boards; have the IT Council review governance board operations annually; document criteria for escalating investments among governance boards; and update policies and procedures for managing its investments as a portfolio.

Similarly, NASA concurred with our three recommendations related to establishing an agency-wide approach to managing cybersecurity risk (recommendations 8, 9, and 10). The agency described actions it had taken or planned to address each of these recommendations. In particular, with regard to establishing a cybersecurity risk management strategy (recommendation 8), NASA asserted that it had already taken actions that met the requirements of our recommendation. Specifically, NASA stated that it had established an approach to developing its cybersecurity risk management strategy by approving a charter for an agency-wide team to address cybersecurity risk management needs and hiring a Chief Cybersecurity Risk Officer to oversee agency-wide risk management initiatives.

While these actions constitute steps toward addressing the recommendation, we disagree that establishing a charter for a team and hiring a Chief Cybersecurity Risk Officer fully addresses the recommendation. As previously noted in this report, the agency does not have a cybersecurity risk management strategy that includes elements of NIST guidance. The strategy should, among other things, make explicit the agency's risk tolerance, accepted risk assessment methodologies, a process for consistently evaluating risk across the organization, risk response strategies, approaches for monitoring risk over time, and priorities for investing in risk management. Ensuring that the established agency-wide team and the Chief Cybersecurity Risk Officer develop a cybersecurity risk management strategy that aligns with the NIST guidance will be essential to fully address our recommendation.

NASA also provided technical comments on the draft report, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Administrator of the National Aeronautics and Space Administration, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

Should you or your staffs have any questions on information discussed in this report, please contact Carol Harris at (202) 512-4456 or harriscc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Carol C. Harris
Director
Information Technology Acquisition Management Issues

Appendix I: Objective, Scope, and Methodology

The National Aeronautics and Space Administration Transition Authorization Act of 2017 included a provision for us to review the effectiveness of the agency's approach to overseeing and managing information technology (IT), including its ability to ensure that resources are aligned with agency missions, cost effective, and secure.[1] Our specific objective for this review was to address the extent to which the National Aeronautics and Space Administration (NASA) has established and implemented leading IT management practices in strategic planning, workforce planning, governance, and cybersecurity.

To address this objective, we compared NASA's IT management policies, procedures, and other documentation to criteria established by federal laws and leading practices.[2] This documentation included the agency's strategic plans, workforce gap assessments, governance board meeting minutes and briefings, charters, policies and procedures, and other documentation of the Chief Information Officer's (CIO) authority. We also reviewed relevant reports by GAO and the NASA Office of Inspector General.[3]

[1]National Aeronautics and Space Administration Transition Authorization Act of 2017, Pub. L. No. 115-10, §811(b), 131 Stat. 18, 59 (March 21, 2017).

[2]Federal Cybersecurity Workforce Assessment Act of 2015, Pub. L. No. 114-113, Div. N, Title III, 129 Stat. 2242, 2975-77 (Dec. 18, 2015); Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Div. A, Title VIII, Subtitle D—Federal Information Technology Acquisition Reform, Pub. L. No. 113-291, § 835 128 Stat. 3292, 3449 (Dec. 19, 2014), codified at 41 U.S.C. § 1704 note; E-Government Act of 2002, Pub. L. No. 107-347, § 209, 116 Stat.2899, 2923-32 (Dec. 17, 2002), codified at 44 U.S.C. § 3501 note; and Clinger-Cohen Act of 1996, Pub. L. No. 104-106, Div. D and Div. E, § 5125(c)(3), 110 Stat. 642, 684-85 (Feb. 10, 1996), codified at 40 U.S.C. § 11315(c)(3). Office of Management and Budget, *Circular No. A-11: Preparation, Submission, and Execution of the Budget*, July 2017; OMB *Circular No. A-130: Managing Information as a Strategic Resource,* (Washington, D.C.: July 28, 2016); and OMB *Memorandum M-13-09 Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* (Washington, D.C.: Mar. 27, 2013); Office of Personnel Management, *The Human Capital Framework* (https://www.opm.gov/policy-data-oversight/human-capital-management/); and GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003), and *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004).

[3]GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009) and National Aeronautics and Space Administration Office of Inspector General, *NASA's Efforts to Improve the Agency's Information Technology Governance*, IG-18-002 Washington, D.C.: Oct. 19, 2017) and *NASA's Information Technology Governance*, IG-13-015 (Washington, D.C.: Jun. 5, 2013).

With regard to IT strategic planning, we identified the strategic plans and related planning guidance issued by NASA and the Office of the CIO, including *NASA's Governance and Strategic Management Handbook*, dated November 26, 2014; *NASA's Information Resources Management Strategic Plan*, dated March 2014; and NASA's updated *Information Technology Strategic Plan* for fiscal years 2018 to 2021. We then reviewed the agency's overall strategic plan, and evaluated its previous and current IT strategic plans against key practices for IT strategic planning that we have previously identified.[4] These practices call for documenting the agency's IT strategic planning processes and developing an IT strategic plan that

- aligns with the agency's overall strategy;
- identifies the mission of the agency, results-oriented goals, and performance measures that permit the agency to determine whether implementation of the plan is succeeding;
- includes strategies the governing IT organization will use to achieve desired results; and
- provides descriptions of interdependencies within and across projects so that they can be understood and managed.

To determine the extent to which NASA has established and implemented leading IT workforce planning practices, we conducted a comparative analysis of NASA's IT workforce planning policies and documents. Specifically, we compared agency documents, such as NASA policy directives, the desk guide, and documentation of efforts to establish IT workforce competencies and staffing requirements and conduct gap

[4]Leading practices were identified related to strategic planning from the Office of Management and Budget, *Circular No. A-11: Preparation, Submission, and Execution of the Budget*, July 2017; OMB *Circular No. A-130: Managing Information as a Strategic Resource,* (Washington, D.C.: July 28, 2016); and OMB *Memorandum M-13-09 Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* (Washington, D.C.: Mar. 27, 2013). Further, prior GAO work related to IT strategic planning and management practices includes, for example, GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, GAO-12-495 (Washington, D.C.: Apr. 26, 2012); and *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*, GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

assessments, to GAO's IT workforce framework.[5] GAO's framework consists of four IT workforce planning steps and eight key activities. The eight key activities were identified in federal law, regulations, and guidance, including the Clinger-Cohen Act of 1996,[6] the legislation referred to as the Federal Information Technology Acquisition Reform Act,[7] Office of Management and Budget (OMB) guidance,[8] the Office of Personnel Management's Human Capital Framework,[9] and GAO reports.[10]

Based on our assessment of the documentation and discussions with agency officials, we assessed the extent to which the agency implemented, partially implemented, or did not implement the activities. We considered an activity to be fully implemented if NASA addressed all of the underlying practices for the activity; partially implemented if it addressed some but not all of the underlying practices for the activity; and not implemented if it did not address any of the underlying practices for the activity.

We assessed IT governance practices by comparing NASA documentation to critical processes identified by GAO in the IT investment management framework.[11] To align our work with the

[5]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

[6]Pub. L. No. 104-106, Div. D and Div. E, § 5125(c)(3) (Feb. 10, 1996), codified at 40 U.S.C. § 11315(c)(3).

[7]Federal Information Technology Acquisition Reform provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

[8]OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015); *Chief Information Officer Authorities*, Memorandum M-11-29 (Washington, D.C.: August 8, 2011); *Guidance for Specialized Information Technology Acquisition Cadres* (Washington, D.C.: July 13, 2011).

[9]OPM, *Human Capital Framework*, (Washington, D.C.: Dec. 2016). The framework is accessible at https://www.opm.gov/policy-data-oversight/human-capital-management/.

[10]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016); *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[11]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004).

provision in Section 811(a) of the National Aeronautics and Space Administration Transition Authorization Act of 2017 calling for NASA to take actions regarding IT governance,[12] we selected critical processes from Stage 2 of the framework:

- instituting the investment board;
- selecting and reselecting investments that meet business needs; and
- providing investment oversight.

For each critical process, we compared key practices outlined in the framework to NASA documentation. The documentation we reviewed included NASA's IT governance policies and procedures, and charters and other guidance. We also reviewed governance board meeting minutes and briefings from each board's first meeting in 2016 through meetings held in August 2017.

In addition, we selected key practices for effective governance from Stage 3 of the IT investment management framework regarding establishing and implementing policies and procedures for developing the portfolio criteria, creating the portfolio, and evaluating the portfolio. We then compared documentation, including NASA's *IT Capital Planning and Investment Control Process* guide dated October 2006, and *Annual Capital Investment Review Implementation Plan* dated October 2015, and draft IT portfolio management plans, against these practices.

Using standards and guidance from the National Institute of Standards and Technology (NIST),[13] which identify foundational elements of effective cybersecurity risk management, we evaluated NASA's cybersecurity risk management approach by

- analyzing policies and plans for establishing a comprehensive risk executive function;
- evaluating documents and plans for establishing a cybersecurity risk management strategy;
- comparing a draft Information Security Program Plan to determine if it was consistent with NIST guidance; and

[12]National Aeronautics and Space Administration Transition Authorization Act of 2017, Pub. L. No. 115-10, §811(a), 131 Stat. 18, 58 (2017).

[13]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

- analyzing policies and procedures to determine if they address relevant NIST security controls and are current.

In addition to assessing NASA headquarters, we reviewed IT management practices at two of the agency's nine centers (Marshall Space Flight Center in Huntsville, Alabama; and Johnson Space Center in Houston, Texas) and at one of NASA's four mission directorates (the Human Exploration and Operations Mission Directorate). The two centers and one mission directorate were selected because they had the largest fiscal year 2017 IT budgets, respectively, as reported on the federal IT dashboard.[14] We also visited the Goddard Space Flight Center in Greenbelt, Maryland, because of the center's proximity to GAO. The results of our work at the selected NASA centers and mission directorate are not generalizable to other NASA centers and mission directorates.

To assess the reliability of these data, we compared them to budgetary data obtained directly from NASA's Office of the CIO. We found the data to be sufficiently reliable for the purpose of identifying the NASA centers and mission directorate with the largest IT budgets. We also interviewed cognizant officials with responsibilities for IT management at NASA headquarters and for the selected centers and mission directorate.

We conducted this performance audit from May 2017 to May 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[14]GAO, *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to Be More Accurate and Available*, GAO-14-64 (Washington, D.C.: Dec 12, 2013). The dashboard is OMB's public website that reports performance and supporting data for major IT investments.

Appendix II: Comments from the National Aeronautics and Space Administration

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-001

May 1, 2018

Reply to Attn of: Office of the Chief Information Officer

Ms. Carol C. Harris
Director
Information Technology Acquisition Management Issues
United States Government Accountability Office
Washington, DC 20548

Dear Ms. Harris:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses" (GAO-18-337), dated March 21, 2018.

In 2014, NASA acknowledged the need to change its culture and management of information technology (IT) and established the Business Services Assessment (BSA) for IT. We continue to implement recommendations resulting from the BSA assessment, establishing a strong foundation to manage IT as a strategic resource. NASA's efforts have resulted in many successes, including consolidation of network operations and operational funding, a more effective IT investment review process integrated with the Agency budget process, and fully embracing the intent of Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Systems Infrastructure."

NASA recognizes the importance of cyber risk management and increasing insight into NASA's IT systems and assets to enable adequate identification, mitigation planning, and risk reduction of potential cybersecurity vulnerabilities. To support these efforts, NASA recently hired a Cyber Risk Manager to advance cybersecurity efforts and is establishing an Enterprise Cybersecurity Services Office. At this time, NASA has completed 90 percent of Phase I continuous diagnostics and mitigation (CDM) tool deployment, expecting completion of Phase I by December 2018. NASA has also started CDM Phase II. NASA's work to develop its response to EO 13800 provided an additional foundational piece for improving NASA's cybersecurity posture. In response to the EO, the NASA Acting Administrator charted the Cybersecurity Executive order Tiger Team (CEOTT), who designed and conducted NASA's first-ever Agency-wide cybersecurity capability gap assessment. As a result, the CEOTT identified key cybersecurity risk management priorities, redefined the way leadership conceptualizes cybersecurity, and

laid the groundwork for incorporating cyber risks into the enterprise risk management framework to provide stronger insights to NASA's senior leadership.

Significant progress has been made in transforming the Agency's IT governance model to become more effective and efficient. The IT Council (ITC), with executive members from each mission directorate, Center, and functional area was established. The ITC approved the recent NASA IT Strategic Plan, providing first ever cross-Agency stakeholder and customer ownership. Although effective until fiscal year 2021, the IT strategic plan is a living document that NASA will amend to meet changing needs. In addition, NASA continues our work in formalizing IT programs, managing and provisioning more IT services at the enterprise level, and identifying legacy IT and determining approaches to prioritize modernization efforts.

In the draft report, GAO makes ten recommendations to the NASA Administrator intended to address the deficiencies identified in IT strategic planning, workforce planning, governance, and cybersecurity.

Specifically, GAO recommends the following:

Recommendation 1: The Administrator should direct the Chief Information Officer to develop a fully documented IT strategic planning process, including methods by which the agency defines its IT needs and develops strategies, systems, and capabilities to meet those needs.

Management's Response: NASA partially concurs with this recommendation. The Agency will fully document its IT strategic planning process, including methods by which NASA defines its IT needs and develops outcomes, strategies, major actions, and performance measures to meet those needs. NASA does not believe that implementation plans, including specific IT capability and system changes, should be part of a strategic plan since these are at a lower level than an Agency IT strategic plan. Detailed IT implementation plans are more dynamic than the four-year NASA IT Strategic Plan. The Agency will document the process for implementing the NASA IT Strategic Plan, including the approach for planning for IT capabilities and systems.

Estimated Completion Date: October 31, 2018.

Recommendation 2: The Administrator should direct the Chief Information Officer to update the IT strategic plan for 2018 to 2021 and develop associated implementation plans to ensure it fully describes strategies the agency will use to achieve the desired results and descriptions of interdependencies within and across programs.

Management's Response: NASA partially concurs with this recommendation. The NASA IT Strategic Plan provides the context and parameters to support achievement of the Agency's vision and mission through the strategic use of IT. This plan describes the business outcomes, strategies, major actions, and performance measures to achieve the

desired results. NASA maintains that the implementation plans, including descriptions of interdependencies within and across programs, are at a lower level than IT strategic plan since detailed IT implementation plans are more dynamic than the four-year NASA IT Strategic Plan. NASA will develop the associated implementation plans to accomplish the NASA IT Strategic Plan, including descriptions of interdependencies within and across programs.

Estimated Completion Date: January 18, 2019.

Recommendation 3: The Administrator should direct the Chief Information Officer 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.

Management's Response: NASA does not concur with this recommendation. NASA recognizes work is underway in the area of IT workforce planning. Currently, NASA is conducting a comprehensive, Agency-wide effort called the Mission Support Future Architecture Program (MAP). This effort is designed to ensure that NASA mission support resources, including workforce, are optimally structured to achieve the NASA mission. MAP will transform mission support services while maintaining mission focus, improving efficiency, ensuring local authority, and valuing the workforce. Simply put, MAP's goal is to optimize mission support services by moving toward a more interdependent model and freeing up resources to re-invest in facilities, IT, and other capabilities necessary for achieving NASA's ambitious portfolio of missions. In addition, GAO has two ongoing audits of IT workforce and recommendations from those audits would be in conjunction with this work. NASA recommends continued progress in the MAP effort and activities related to IT workforce planning remain centered in recommendations from the two GAO IT workforce audits.

Recommendation 4: The Administrator should direct the Chief Information Officer to institute an effective IT governance structure by completing planned improvement efforts and finalizing charters to fully establish IT governance boards, clearly defining roles and responsibilities for selecting and overseeing IT investments, and ensuring that the governance boards operate as intended.

Management's Response: NASA concurs with this recommendation. Charters will be published for all IT governance boards. The six IT program plans will define roles and responsibilities for selecting and overseeing IT investments. The Agency ITC will conduct an annual review of the governance board operations.

Estimated Completion Date: January 31, 2019

Recommendation 5: The Administrator should direct the Chief Information Officer to update policies and procedures for selecting investments to provide a structured process, including thresholds and criteria needed for, among other things, evaluating investment risks as part of governance board decision making, and outline a process for re-selecting investments.

Management's Response: NASA concurs with the recommendation. The Office of the Chief Information Officer guidance for Strategic Programming Guidance for fiscal year 2020 articulates how to document and report the Agency's IT investment information to enable the appropriate analysis of IT investments. The ITC will review and approve the Agency's IT portfolio of investments as part of this existing Program, Planning, Budgeting and Execution (PPBE) process in the summer of 2018, prior to the Agency's budget submission in September.

Estimated Completion Date: January 31, 2019.

Recommendation 6: The Administrator should direct the Chief Information Officer to address weaknesses in oversight practices and ensure routine oversight of all investments by taking action to document criteria for escalating investments among governance boards and establish procedures for tracking corrective actions for underperforming investments.

Management's Response: NASA concurs with the recommendation. NASA is documenting the criteria for escalating IT investments among governance boards and establishing procedures for tracking corrective actions for underperforming IT investments.

Estimated Completion Date: January 18, 2019.

Recommendation 7: The Administrator should ensure that the Chief Information Officer fully defines policies and procedures for developing the portfolio criteria, creating the portfolio, and evaluating the portfolio.

Management's Response: NASA concurs with the recommendation. NASA is updating policies and procedures for developing the portfolio criteria, creating the portfolio, and evaluating the portfolio.

Estimated Completion Date: February 28, 2019.

Recommendation 8: The Administrator should direct the Chief Information Officer to establish an agency-wide approach to managing cybersecurity risk that includes a cybersecurity strategy that, among other things, makes explicit the agency's risk tolerance, accepted risk assessment methodologies, a process for consistently evaluating

risk across the organization, response strategies and approaches for monitoring risk over time, and priorities for risk management investments.

Management's Response: NASA concurs with the recommendation. NASA has established an approach to developing its cybersecurity risk management strategy which it believes meets the requirements for this recommendation. This approach includes (1) approving a charter for an Agency-wide Cybersecurity Integration Team to address key cybersecurity risk management needs; and (2) hiring a Chief Cybersecurity Risk Officer specifically to establish and oversee Agency-wide cybersecurity risk management initiatives. NASA completed these actions on April 2, 2018, as its approach to developing its cybersecurity risk management strategy and can provide documentation as needed.

Completion Date: April 2, 2018.

Recommendation 9: The Administrator should direct the Chief Information Officer to establish an agency-wide approach to managing cybersecurity risk that includes an information security program plan that fully reflects the agency's IT security functions and services and agency-wide privacy controls for protecting information.

Management's Response: NASA concurs with the recommendation. NASA is in the process of updating its information security program plan in accordance with the National Institute of Standards and Technology Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

Estimated Completion Date: October 18, 2018.

Recommendation 10: The Administrator should direct the Chief Information Officer to establish an agency-wide approach to managing cybersecurity risk that includes policies and procedures with well-defined roles and responsibilities that are integrated and reflect NASA's current security practices and operating environment.

Management's Response: NASA concurs with the recommendation. NASA is reviewing and updating its policy management framework to facilitate consistent reviews and updates based on current security practices and the current operating environment.

Estimated Completion Date: March 29, 2019.

Thank you for the opportunity to comment on the subject draft report. If you have any questions or require additional information, please contact Ruth McWilliams on (202) 358-5125.

Sincerely,

Renee P. Wynn
Chief Information Officer

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris at (202) 512-4456 or harriscc@gao.gov

Staff Acknowledgments

In addition to the contact name above, the following staff also made key contributions to this report: Eric Winter (Assistant Director), Donald Baca, Rebecca Eyler, Amanda Gill (Analyst in Charge), Tom Johnson, Kate Nielsen, Teresa Smith, and Niti Tandon.