NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

NASA's Efforts to Improve the Agency's Information Technology Governance

October 19, 2017

Report No. IG-18-002

Office of Inspector General

To report, fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD) or visit https://oig.nasa.gov/hotline.html. You can also write to NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, D.C. 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

To suggest ideas for or to request future audits contact the Assistant Inspector General for Audits at https://oig.nasa.gov/aboutAll.html.

NASA Office of Inspector General
Office of Audits

RESULTS IN BRIEF

NASA's Efforts to Improve the Agency's Information Technology Governance

October 19, 2017 IG-18-002 (A-16-013-00)

WHY WE PERFORMED THIS AUDIT

Information technology (IT) plays an integral role in every facet of NASA's space, science, and aeronautics operations. The Agency spends approximately $1.4 billion annually on a portfolio of IT assets it uses to control spacecraft, collect and process scientific data, secure its IT infrastructure, and enable NASA personnel to collaborate with colleagues around the world.

For more than two decades, NASA has struggled to implement an effective IT governance framework, a critical component to making decisions that balance compliance, cost, risk, and mission success. Conversely, ineffective IT governance can result in security breaches, increased costs, missed deadlines, and provision of low quality IT products and services.

In our 2013 report, we found that the decentralized nature of Agency operations and longstanding culture of autonomy hindered NASA's ability to implement effective IT governance. We made eight recommendations and NASA agreed to take action to address our concerns. In this audit, we evaluated NASA's progress in implementing changes to its IT governance structure. To complete this work, we interviewed IT officials at Headquarters and across the Agency and reviewed relevant NASA policy, prior audit reports, data, and documents related to IT governance.

WHAT WE FOUND

In the 4 years since issuance of our IT governance report and the 3 years since completion of its own internal review, the Office of the Chief Information Officer (OCIO) has made insufficient progress to improve NASA's IT governance, casting doubt on the office's ability to effectively oversee the Agency's IT assets. Specifically, the NASA Chief Information Officer (CIO) continues to have limited visibility into IT investments across the Agency and the process NASA developed to correct this shortcoming is flawed.

In 2016, NASA established the Annual Capital Investment Review (ACIR) as its formal response to a Federal mandate that CIOs have approval authority over all agency IT spending. The ACIR process is designed to collect IT investment data across NASA, including institutional, mission, and highly specialized IT, for review and approval by the Agency's senior IT governance board – a process expected to help increase the Agency CIO's authority in IT acquisition planning throughout NASA.

Despite these efforts, the OCIO's insight into and control over the bulk of the Agency's nearly $1.4 billion in annual IT funding remains limited, with the Mission Directorates and Centers controlling $739 million (53 percent) and $311 million (22 percent), respectively, in fiscal year 2017. This lack of authority and visibility over the majority of the IT budget limits the Agency's ability to consolidate IT expenditures, realize cost savings, and drive improvements in the delivery of IT services.

The success of NASA's IT governance processes also depends on a comprehensive Agency enterprise architecture – the map of IT assets, business processes, and governance principles that drive ongoing investment and management decisions – together with well-functioning IT governance boards. However, the Agency's current enterprise architecture remains immature after a decade-long effort, a situation that contributes to the undisciplined manner in which NASA makes IT investments. Moreover, despite changes to two of the Agency's three top-level IT governance boards, IT managers across the Agency remain unsure of board functions and their decision making processes and the boards have yet to make strategic decisions that substantively impact how IT at NASA is managed. In addition, as of August 2017 the roles and responsibilities associated with NASA's IT governance structure have not been finalized by the OCIO – one of the most basic and critical pieces of the Agency's Business Services Assessment (BSA) Implementation Plan.

Lingering confusion about security roles coupled with poor IT inventory practices continues to negatively impact NASA's security posture. For example, while NASA's Senior Agency Information Security Officer (SAISO) is responsible for managing Agency-wide IT security, the Mission Directorates and Centers operate hundreds of networks and have their own IT security personnel responsible for security, risk determination, and risk acceptance on those systems – yet none of these personnel report to the SAISO. In addition, high turnover of senior IT managers, including the Agency CIO and the SAISO, have impacted NASA's IT operations, affected the Agency's ability to execute its IT governance structure, and hindered the Agency's ability to significantly improve NASA's IT security posture.

Finally, the OCIO continues to exercise limited ability to influence IT management within the Mission Directorates and Centers due to the autonomous nature of NASA operations and the office's lack of credibility on IT issues in the eyes of its customers.

What We Recommended

To increase transparency, accountability, and oversight of NASA's IT investments and strengthen its governance framework, we recommended NASA's CIO: (1) reevaluate and implement necessary changes to the ACIR process, its reporting requirements, and approval thresholds to ensure the Agency CIO gains adequate visibility and authority over all NASA IT assets; (2) complete the charters for all IT governance boards and educate personnel on their functions; (3) complete the BSA Implementation Plan steps related to the roles and responsibilities of positions within the Agency's IT structure; (4) address the Agency's dispersed security responsibilities and long-standing security weaknesses by empowering the SAISO position to include operational responsibilities and address basic IT security practices in the areas of inventory, patching, vulnerability, and configuration management; and (5) implement a mitigation plan to address skill set and capability issues facing the OCIO in order to improve its credibility among its customers.

We provided a draft of this report to NASA management who concurred with three recommendations, partially concurred with two others, and described corrective actions it has taken or will take. For one of the recommendations the Agency partially concurred with, we do not find the proposed actions responsive to our concerns about the dispersal of IT security responsibilities which results in the lack of authority and marginalization of the SAISO position. Therefore, four of the five recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

For more information on the NASA Office of Inspector General and to view this and other reports visit http://oig.nasa.gov/.

TABLE OF CONTENTS

Acronyms

ACES	Agency Consolidated End-User Services
ACIR	Annual Capital Investment Review
ATO	Authority to Operate
BSA	Business Services Assessment
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLT	Chief Information Officer Leadership Team
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
GAO	Government Accountability Office
IT	Information Technology
IT PMB	Information Technology Program Management Board
ITC	Information Technology Council
MSC	Mission Support Council
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NSSC	NASA Shared Services Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PPBE	Planning, Programming, Budgeting, and Execution
SAISO	Senior Agency Information Security Officer
SOC	Security Operations Center

INTRODUCTION

Information technology (IT) plays an integral role in every facet of NASA's space, science, and aeronautics operations. The Agency spends approximately $1.4 billion each year on a portfolio of IT assets that includes approximately 500 information systems it uses to control spacecraft, collect and process scientific data, secure its IT infrastructure, and enable NASA personnel to collaborate with colleagues around the world.

In the broadest sense, governance refers to the rules, processes, and laws pursuant to which an organization operates and is regulated or controlled. In the IT context, governance is the process that seeks to ensure the effective and efficient use of IT in an organization to achieve its goals. It involves managing IT operations and IT projects to ensure alignment between these activities and the needs of the organization. An effective IT governance model is critical to accommodating the varied interests of internal and external stakeholders and making decisions that balance compliance, cost, risk, and mission success. Conversely, ineffective IT governance can result in security breaches, increased costs, missed deadlines, and provision of low quality IT products and services.

For more than two decades, NASA has struggled to implement an effective IT governance framework. In a 2013 report, the Office of Inspector General (OIG) found the decentralized nature of Agency operations and longstanding culture of autonomy hindered NASA's ability to implement effective IT governance.[1] We made eight recommendations in that report and NASA agreed to take action to address our concerns. Four years later, we evaluated NASA's progress in implementing changes to its governance structure. See Appendix A for details of the audit's scope and methodology.

Background

NASA consists of a Headquarters office in Washington, D.C.; nine geographically dispersed Centers; and the Jet Propulsion Laboratory, a federally funded research and development center operated under contract by the California Institute of Technology.[2] Historically, NASA has operated as a decentralized organization based on the philosophy that its Centers and project managers should be given as much autonomy as possible to accomplish the Agency's mission. Consistent with this philosophy, the Agency's organizational structure has three primary levels:

- Agency or "corporate" management - Located primarily at NASA Headquarters and responsible for providing NASA's strategic direction, top-level requirements, schedules, and budgets. Included in the Headquarters operation is the Mission Support Directorate and the Offices of the Chief Scientist, Chief Technologist, Chief Engineer, Chief Financial Officer, Chief Health and Medical Officer, Chief of Safety and Mission Assurance, and the Chief Information Officer (CIO).

[1] NASA OIG, "NASA's Information Technology Governance" (IG-13-015, June 5, 2013).

[2] NASA also has six supporting facilities that, among other things, conduct climate research and manufacture rockets, and the NASA Shared Services Center, a partnership between NASA and a contractor to address a variety of support functions such as financial management, human resources, and procurement.

- Program or project management - NASA has four Mission Directorates, each led by an Associate Administrator: Aeronautics Research, Human Exploration and Operations, Science, and Space Technology. Associate Administrators, located at NASA Headquarters, are responsible for managing their Directorate's portfolio of programs and projects. Much of the work associated with Mission Directorate programs occurs at the NASA Centers.
- Center management - NASA Centers are led by Directors who are responsible for managing Center operations and determining how best to support the programs and projects located there.

The Associate Administrators of the Mission Directorates depend on Center Directors to provide the resources needed to execute Directorate programs and projects, such as engineers and test stands at Marshall Space Flight Center (Marshall) to test rocket components. Associate Administrators do not have decision-making authority regarding the day-to-day operations of the Centers and Center Directors do not provide programmatic direction to programs or projects. Both the Mission Directorate Associate Administrators and Center Directors report to the Associate Administrator, the number three person in the NASA hierarchy and the Agency's senior civil servant.

NASA manages its operations with three Headquarters-based councils that provide high-level oversight, set requirements and priorities, and guide key Agency assessments: the Executive Council, the Program Management Council, and the Mission Support Council (MSC). Major IT decisions flow through the MSC when necessary, although some issues may be elevated to the Executive Council.

NASA Information Technology

The Office of the Chief Information Officer (OCIO) is responsible for developing an effective Agency IT governance structure and managing and securing NASA's IT assets and operations. The basic structure of NASA's IT organization has seen little change since our 2013 audit. Authority for developing IT policies and implementing an Agency-wide IT program lies with the Headquarters-based Agency CIO and OCIO staff. The Agency CIO is responsible for providing leadership, planning, policy direction, and oversight of the management of NASA IT resources Agency-wide. The Agency CIO also serves as the principal advisor to the Administrator and other senior officials on IT matters and is responsible for ensuring IT investments align with NASA's mission and meet cost, schedule, and performance goals.

The Federal Information Security Management Act of 2002 establishes information security program and evaluation requirements for Federal agencies.[3] Under the Act, each agency CIO is directed to identify a Senior Agency Information Security Officer (SAISO), also known as an agency Chief Information Security Officer (CISO). The SAISO is the principal advisor to the Agency CIO and other senior officials on matters pertaining to information security. The OCIO also has a Senior Advisor for Cybersecurity who reports directly to the Agency CIO and serves as a liaison to build partnerships with internal and external entities.

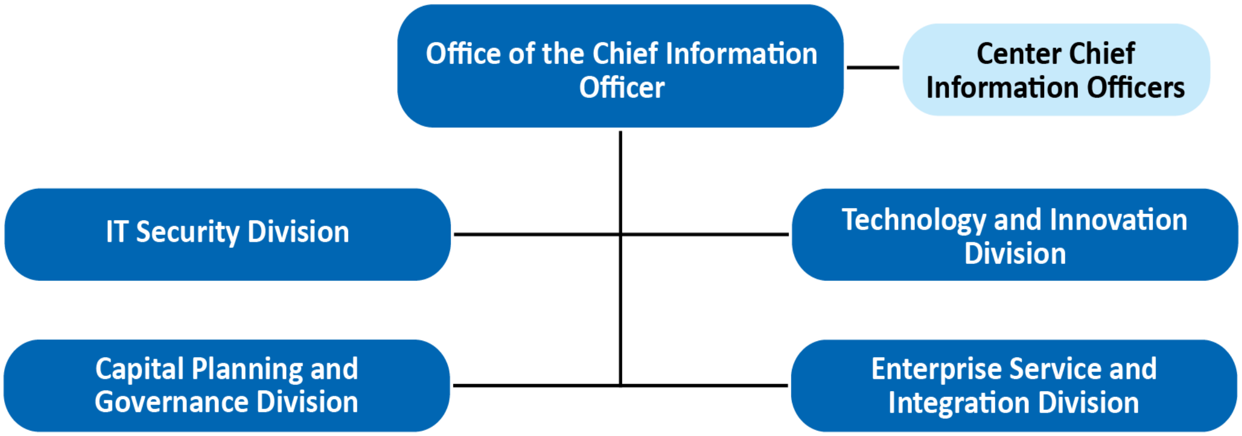
The Agency OCIO operation is comprised of 117 positions – 48 civil servants and 69 contractor staff.[4] The office has four divisions: (1) IT Security, which manages Agency-wide security operations and policy; (2) Capital Planning and Governance, which develops, implements, and promotes the use of information

[3] The Federal Information Security Management Act of 2002 and its successor, the Federal Information Security Modernization Act of 2014, identifies specific IT security requirements Federal agencies must satisfy and assigns responsibilities to agency officials and Inspectors General for addressing and assessing these requirements.

[4] As a point of comparison, our 2013 review noted the OCIO had 86 positions – 52 civil servants and 34 contractor staff.

resource management policies, evaluates related practices, and determines compliance; (3) Technology and Innovation, which identifies emerging IT technologies and addresses issues such as technology infusion; and (4) Enterprise Service and Integration, which implements NASA's enterprise architecture including networks, data centers, web services, desktop computers, enterprise applications, and other end-user tools. Figure 1 illustrates the current OCIO organizational structure which has been in place since at least November 2011.

Figure 1: NASA OCIO Organizational Structure


Office of the Chief Information Officer
Center Chief Information Officers
IT Security Division
Technology and Innovation Division
Capital Planning and Governance Division
Enterprise Service and Integration Division

Source: NASA OIG presentation of NASA information.

Each NASA Center has its own CIO and IT staff, whose numbers vary from single digits to several hundred depending on the size of the Center. Center CIOs are responsible for the Center's IT portfolio and for ensuring that Center IT activities align with Federal and Agency requirements. Historically, Center CIOs reported to their respective Center Directors, but in 2010 NASA revised its management structure to make Center CIOs report to the Agency CIO. However, Center CIOs receive their funding through each Center's budget rather than through the Agency CIO's budget, and for this reason the Center CIO, in essence, works for and reports to both the Agency CIO and the Center Director.

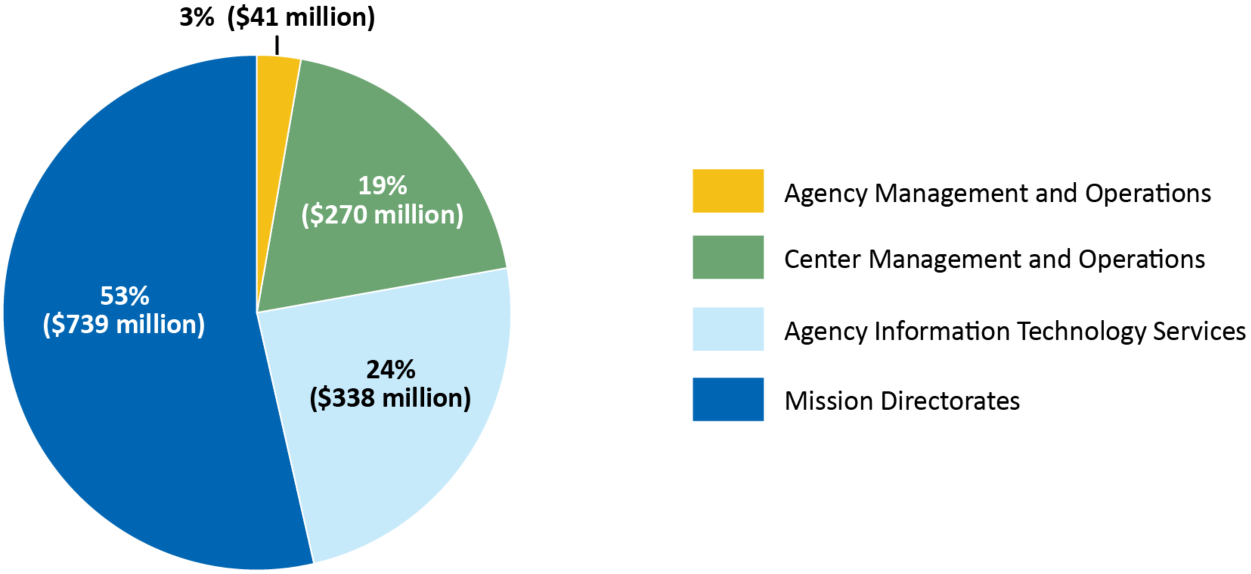
Three high-level boards are part of NASA's IT governance structure. The Information Technology Council (ITC) serves as the Agency's senior decision-making body for information resources management. If the ITC cannot reach a decision, the board may elevate an issue to the MSC. The two other advisory boards are the Chief Information Officer Leadership Team (CLT) and the Information Technology Program Management Board (IT PMB). The CLT, chaired by the Agency CIO, is composed of the Deputy CIO, Associate CIOs (who oversee the OCIO's four divisions), Center CIOs, Jet Propulsion Laboratory CIO, NASA Shared Services Center (NSSC) CIO, and Mission Directorate representatives. The CLT examines Mission Directorate and Center IT requirements, risk strategies, and other stakeholder issues. The IT PMB includes the Associate CIO for Capital Planning and Governance, officials from the Office of the Chief Engineer, the Enterprise Architecture Lead Representative, and staff from the Mission Directorates, Centers, and CLT. The group, chaired by the NASA Deputy CIO, serves as a forum for top-level oversight and evaluation of Agency IT programs and projects. Six Program Boards below the three high-level boards make operational decisions on a variety of issues including IT security and software applications.

NASA Information Technology Assets

NASA's IT assets generally fall into two broad categories: institutional or mission.[5] Institutional systems support the day-to-day work of NASA employees and include networks, data centers, web services, desktop and laptop computers, enterprise business applications, and other end-user tools such as email and calendaring. Mission systems include highly specialized IT assets that support the Agency's aeronautics, science, and space exploration programs; host IT systems that control spacecraft; collect and process scientific data; and perform other critical Agency functions. NASA Mission Directorates fund their own computer networks and IT personnel and therefore, in most cases, directorate personnel rather than OCIO staff have authority over the operational and security aspects of mission networks.[6] Directorate personnel also determine risk and risk acceptance for these networks. As noted in our 2013 report, this structure limits the OCIO's visibility into mission IT operations, security, and spending.

NASA's fiscal year (FY) 2017 IT budget was approximately $1.4 billion. Funding for this budget comes from four main sources: (1) Agency Information Technology Services, (2) Agency Management and Operations, (3) Center Management and Operations, and (4) Mission Directorates. Of this overall amount, the Agency CIO controlled $338 million or 24 percent, the Centers controlled $311 million or 22 percent, and the Mission Directorates controlled $739 million or 53 percent. Similar to what we found in 2013, Mission Directorates control over half of the IT budget, as illustrated in Figure 2.[7]

Figure 2: NASA's Fiscal Year 2017 IT Budget



Source: NASA's FY 2017 budget.

[5] In September 2017, the Agency CIO informed us that NASA added a third category to account for physical IT assets such as environmental monitoring and control systems (e.g., systems that control heating, cooling, ventilation, and power).

[6] Funding for IT investments associated with many NASA programs and projects is embedded in the funding for the underlying missions.

[7] In 2013, we reported that the Mission Directorates controlled 62 percent of the Agency's IT budget, Centers 27 percent, and the Agency CIO the remaining 11 percent. In the FY 2017 budget, the Agency CIO controls 24 percent of the Agency's IT budget, an increase of 13 percent. The OCIO attributes this increase, in part, to a shift in funding for certain enterprise service functions from Centers to the Agency CIO.

Prior Office of Inspector General Audits

In 2005 and 2013, we issued reports examining NASA's IT governance.[8] In 2005, we reported that the Agency CIO and IT security officials had very limited oversight and influence over IT purchases and IT security decisions at the Centers. Even though the Agency CIO reviewed and concurred with major IT investments, the position had little influence over Center and Mission-specific IT investment decisions. As a result, IT purchases could be incompatible with other Centers or with NASA's enterprise architecture. Furthermore, we found that management of IT and IT security throughout NASA was less efficient, cohesive, and effective because of the CIO's inability to exercise its authority over Agency-wide IT. In response, the Agency CIO commissioned an independent study that found NASA's management of IT resources to be very decentralized in a mission-focused environment. The study noted that given the OCIO's limited staff, it faced a tremendous challenge to fulfill its IT responsibilities. The study recommended stronger lines of accountability and an enforced delegation of authority through the governance structure, a more formal reporting structure between the Agency CIO and Mission Directorate and Center CIOs, a series of personnel improvements, and improved reporting and monitoring capabilities on program performance.

In 2013, we reported the Agency CIO continued to have limited visibility and control over the majority of the Agency's IT investments, operated in an organizational structure that marginalized the authority of the position, and could not enforce security measures across the Agency's computer networks. Moreover, NASA's IT governance structure was overly complex and did not function effectively, which resulted in Agency managers relying on informal relationships rather than formalized business processes when making IT-related decisions. Finally, we found NASA's IT governance model weakened accountability and did not ensure that IT assets across the Agency were cost effective and secure.

We made eight recommendations in 2013 to overhaul NASA's IT governance structure by centralizing IT functions and establishing the Agency CIO as the top management official responsible for the Agency's entire IT portfolio. We recommended empowering the CIO to approve all IT procurements over an established monetary threshold. We also recommended reevaluating the relevancy, composition, and purpose of NASA's IT governance boards and require the use of the reconstituted boards for all major IT decisions and investments. Finally, we suggested the NASA Administrator reevaluate the OCIO's resources to ensure the Office has the appropriate number of personnel with the appropriate skills.

In response to our report, the OCIO hired Forrester Research, a private technology consulting firm, to address several of our recommendations. That assessment examined the decentralized nature of NASA's operations and how the autonomous culture was stifling the Agency's ability to execute effective IT governance. In addition, Forrester examined the CIO's limited visibility of the Agency's IT budget and spending. Forrester concluded that NASA has a highly fragmented organizational structure and culture with inadequate mechanisms for determining which IT assets are common across the enterprise and which are Center- or Mission-specific.

[8] IG-13-015 and NASA OIG, "Final Memorandum on Review of Organizational Structure and Management of Information Technology and Information Technology Security Services at NASA" (IG-05-013, March 30, 2005).

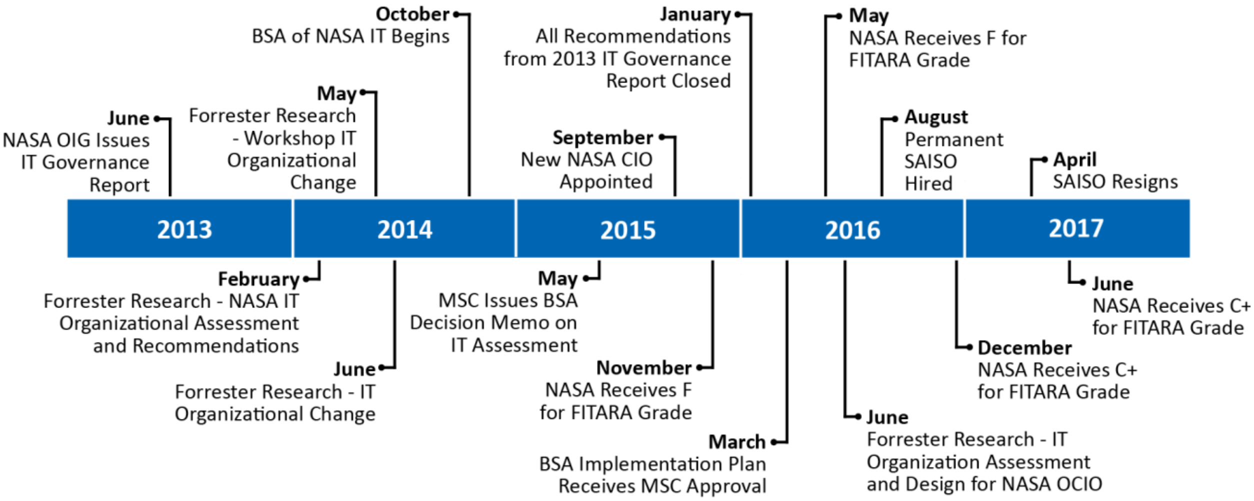
Based on these findings, Forrester made two recommendations. The first suggested an incremental approach to revising NASA's IT structure, processes, and culture that recognizes the difficulty of overcoming existing barriers. The second, taking a more aggressive approach, would require dramatic changes in NASA's IT structure, processes, and functions to provide greater governance and oversight. The report concluded that if NASA does nothing else, it should: (1) establish a centralized IT architecture group, (2) establish a centralized IT vendor management group, (3) clearly define who has what decision making authority within the IT organization, and (4) evaluate Centers as functions of excellence.[9]

In June 2014, Forrester completed a follow-up report, "IT Organizational Change." Similar to the findings of our 2013 audit, they reported the following characteristics within NASA's IT culture:

- Fear of centralization;
- Centers enjoy sense of autonomy;
- Historic lack of confidence in OCIO;
- Highly structured in areas such as project planning;
- Program managers for missions are "kings" and highly autonomous;
- 10 Centers run like 10 cities; and
- Lots of studies but not enough action.

A timeline of events to improve NASA's IT governance, including internal and external reviews of its structure beginning with our 2013 audit, is displayed in Figure 3. The following section further describes these events.

Figure 3: Timeline of Key Events Impacting NASA's IT Governance


June
NASA OIG Issues IT Governance Report
May
Forrester Research - Workshop IT Organizational Change
October
BSA of NASA IT Begins
September
New NASA CIO Appointed
January
All Recommendations from 2013 IT Governance Report Closed
May
NASA Receives F for FITARA Grade
August
Permanent SAISO Hired
April
SAISO Resigns
2013
2014
2015
2016
2017
February
Forrester Research - NASA IT Organizational Assessment and Recommendations
June
Forrester Research - IT Organizational Change
May
MSC Issues BSA Decision Memo on IT Assessment
November
NASA Receives F for FITARA Grade
March
BSA Implementation Plan Receives MSC Approval
June
Forrester Research - IT Organization Assessment and Design for NASA OCIO
December
NASA Receives C+ for FITARA Grade
June
NASA Receives C+ for FITARA Grade

Source: NASA OIG analysis of Agency information.

Note: Business Services Assessment (BSA) and Federal Information Technology Acquisition Reform Act (FITARA).

[9] The term "functions of excellence" refers to one Center's capabilities and expertise that can potentially be provided to other Centers as a service.

NASA Information Technology Business Services Assessment and the Federal Information Technology Acquisition Reform Act

In 2012, as part of an Agency-wide effort led by the Associate Administrator to "rightsize" its workforce and facilities to best position itself for current and future missions, NASA established Technical Capability Assessment Teams. Building upon lessons learned from the technical assesments, NASA established teams to evaluate the Agency's IT, procurement, human capital, budget management, and facilities functions. These teams conduct business services assessments (BSA) to examine key capabilities across NASA by interviewing stakeholders, reviewing audits and regulations, benchmarking external organizations, and performing a detailed assessment of internal operations.[10] Recommendations from the BSAs are forwarded to the Mission Support Council or MSC who, after review, instructs the business areas to implement certain decisions. When assessing NASA's IT environment, the BSA team identified seven areas for detailed study: (1) Roles and Responsibilities, (2) Governance, (3) Data Centers, (4) Communications, (5) End-User Services – Workstations, (6) End-User Services - Collaboration and Content Management Tools, and (7) IT Security.

Like our 2013 IT governance audit, the BSA IT team found the Agency CIO has limited visibility into IT management and operational decisions made by Center, Mission, and Program Directors resulting in risks to the quality and security of Agency IT services. The review team also pointed out that shadow IT, multiple collaboration tools, and stand-alone IT systems exist within the Agency.[11] The BSA reported its findings to the MSC, which made specific decisions in seven IT-related areas. In May 2015, the MSC tasked the Agency CIO with developing what became the BSA Implementation Plan. This Plan was required to address all of the decisions made by the MSC, which are detailed in Table 1 below. The Plan included an extensive 15-page schedule with over 600 action items intended to improve the Agency's management of IT, including improvements to the Agency's governance structure.

[10] The BSA is a strategic assessment of business and mission support services that examines a function's current activities and opportunities for improvement.

[11] Shadow IT consists of IT assets on an agency's network that the CIO or Chief Information Security Officer did not purchase or authorize for use by agency personnel.

Table 1: Mission Support Council Decision Memorandum for NASA IT

	Decision Title	Decision Description
1	Roles and Responsibilities	The OCIO was directed to create a level 0 – 3 management structure, appointing level 2 Program Executives for each IT domain by July 31, 2015, and defining the responsibilities and authorities of each level by November 15, 2015.[a] The OCIO was also to create a 5-year strategic plan that described a path forward that facilitated incremental growth in operational maturity and IT management. The Agency CIO's IT-related oversight was expanded to all non-highly specialized IT, including NSSC investments.
2	Governance	The OCIO was directed to restructure and streamline misaligned, duplicative, and ineffective IT boards by July 31, 2015. The Agency CIO, working with the Chief Financial Officer, was to conduct a formal Annual Capital Investment Review (ACIR) as part of the Planning, Programming, Budgeting, and Execution (PPBE) process by September 30, 2015, and the CIO's role in monitoring non-highly specialized Agency IT program performance was to be expanded by that date.[b] In addition, the OCIO was to work with NASA Procurement to formalize guidance on strategic sourcing for IT by November 15, 2015, followed by functional reviews of all Centers with the first cycle completed by May 15, 2016.
3	Data Centers	The OCIO was directed to develop by November 2015 an integrated, Agency-wide data center architecture to guide future investments and consolidation, including on-site, outsourced, and cloud-based data center services as well as strategic sourcing and contract optimization. Beginning with the PPBE for 2018, the OCIO and the Office of the Chief Financial Officer were to approve any investments in new or existing data centers through the ACIR, addressing the full cost of data center services, life cycle costs, strategic sourcing options, and alignment with NASA's data center architecture. The CIO Computing Services Service Office and Center CIOs were to collaborate on all Center-based cloud efforts.
4	Communications	By the end of September 2015, the OCIO was directed to address risk mitigation actions to ensure successful implementation of the network transformation initiative. NASA-provided voice services, network operations, and transformation funding was to be realigned under the Agency CIO to enable an enterprise funded and managed approach by October 1, 2015.
5	End-User Services (Workstations)	The OCIO was directed to consolidate non-Agency Consolidated End-User Services (ACES) workstation administration and support by the end of FY 2017 and set a target for each Center to obtain at least 80 percent of their desktop, laptop, and workstation computing services through ACES by December 31, 2017.[c]
6	End-User Services (Collaboration and Content Management Tools)	The OCIO was directed to define a Core Suite of Collaboration Tools and standards by November 15, 2015, to be implemented as enterprise-managed services under the End-User Services Program Executive. Funding will be provided via Agency Management and Operations Agency IT Services or the NSSC Working Capital Fund for development, migration, and operations of the base capability through the PPBE for 2018.
7	IT Security	The MSC was directed to conduct an independent review of IT security spending and alignment to the Agency's IT security strategy by November 15, 2015. The OCIO was to establish an Agency IT security risk management framework and IT security architecture that aligns with NASA's business risks by that same date.

Source: Decision Memorandum, Business Services Assessment Decision – IT Pilot Preliminary Findings and Decision on Deep Dive Targets, May 15, 2015.

[a] In the Level 0-3 structure, Level 0 is the Agency CIO, Level 1 includes Associate CIOs, Level 2 includes Program Executives, and Level 3 includes Program Offices.

[b] ACIR is part of the Agency's formal response to the Federal Information Technology Acquisition Reform Act , which mandates that CIOs have approval authority over their Agency's IT budget and increases the CIO's responsibility in the IT procurement process. The ACIR is intended to make the CIO more directly accountable for IT investments through increased authority in the PPBE cycle. The PPBE process includes developing the Agency's strategic goals and performance plans, formulating the annual budget, and developing Agency Operating and Execution Plans.

[c] In December 2010, NASA awarded a 4-year contract with two, 3-year option periods to HP Enterprise Services for Agency Consolidated End-User Services, or ACES, to provide and manage most of NASA's personal computing hardware, software, mobile IT services, peripherals and accessories, associated end-user services, and supporting infrastructure.

In December 2014, concurrent with the BSA and building upon the Federal CIO responsibilities as outlined in the Clinger-Cohen Act of 1996, Congress passed the Federal Information Technology Acquisition Reform Act (FITARA).[12] FITARA significantly strengthened the CIO's role in overseeing IT investments, IT procurement, and the IT workforce. The Act's main objectives were to enhance the authority of CIOs to plan, approve, and execute IT acquisitions; provide better visibility and improve risk management of IT investments; and engage senior agency officials in the coordination and oversight of IT investments. The Office of Management and Budget (OMB), which coordinates government-wide reporting of IT investments, issued FITARA guidance and directed agencies to submit implementation plans by December 2015.

To meet these requirements, NASA developed a FITARA Common Baseline that relied heavily on the new IT governance structure outlined in the BSA IT decisions prescribed by the MSC.[13] The Agency's position was that its current IT policies were sufficient and aligned with FITARA requirements while its management, governance, and operating processes did not. However, NASA management believed the final set of approved recommendations from the BSA - the restructuring of the IT governance councils and the new Annual Capital Investment Review (ACIR) process - would increase CIO visibility and authority and thereby meet FITARA requirements.

The ACIR is the Agency's formal response to FITARA and the Act's mandate that NASA's CIO have approval authority over the Agency's entire IT budget as well as increased responsibility for the IT procurement process. The ACIR's scope includes institutional and mission IT (including highly specialized IT purchases) and IT investments. Under the ACIR process, the Agency CIO is responsible for ensuring IT investments align with NASA's mission and programmatic priorities. NASA completed its first ACIR in May 2016, an accomplishment the Agency views as a key milestone in overhauling its IT governance and addressing prior OIG recommendations and FITARA mandates.

In January 2016, we agreed to close all outstanding recommendations from our 2013 audit based on planned actions in the BSA for the Agency's IT operations (see Appendix B). However, recent OIG audits have found NASA is still struggling with limited Agency CIO authority, decentralized IT operations, and ineffective IT governance casting doubt on whether the Agency has implemented the changes agreed to when we closed our recommendations.

[12] The Clinger-Cohen Act of 1996 makes Federal agency CIOs responsible for advising agency heads on IT investments and improving the way Federal agencies acquire and manage IT resources. The Act requires that each agency establish a CIO position with clear accountability for IT management.

[13] FITARA requires Agencies to establish a "Common Baseline" for roles, responsibilities, and authorities of the Agency CIO and responsibilities of other senior agency officials in managing IT as a strategic resource.

Information Technology Governance at NASA Remains Ineffective

In the 4 years since issuance of our IT governance audit and the 3 years since completion of its IT Business Services Assessment, the OCIO has made insufficient progress to improve NASA's IT governance, casting doubt on the office's ability to effectively oversee the approximate $1.4 billion the Agency spends annually on IT. Specifically, the Agency CIO continues to have limited visibility into IT investments across NASA and the process NASA developed to correct those shortcomings is flawed. Moreover, the OCIO continues its decade-long struggle to establish an effective enterprise architecture, but its current iteration remains perpetually immature. While the OCIO has made changes to its three senior advisory boards over the past few years, these boards have yet to make strategic decisions that substantively impact how IT at NASA is managed. Consequently, slow implementation of the OCIO's revised IT governance structure has left many Agency IT officials operating under the previous inefficient and ineffective framework. Case in point: as of August 2017 the OCIO has failed to finalize the roles and responsibilities for IT management at NASA, one of the most basic and critical pieces of both its governance structure and BSA Implementation Plan. Further, lingering confusion about security roles coupled with poor IT inventory practices negatively impacts NASA's security posture. Finally, the OCIO continues to exercise limited ability to influence IT management within the Mission Directorates and at the Centers due to the autonomous nature of NASA's operations and the OCIO's lack of credibility on IT issues in the eyes of its customers.

CIO Control and Insight of IT Funding and Investments Remains Limited

We previously reported that the Agency CIO had little control or visibility over the majority of NASA's IT budget.[14] We also emphasized that the CIO's lack of authority over IT funding limited the Agency's ability to consolidate IT expenditures, realize cost savings, and drive improvements in the delivery of IT services.

NASA traditionally has used its Capital Planning and Investment Control process to report planned IT investments to OMB, a process overseen by Center CIOs and program liaisons. As part of the BSA Implementation Plan, the MSC directed the Agency CIO to work with the Agency Chief Financial Officer to improve this process so it could serve as the basis for its new Annual Capital Investment Review or ACIR. As previously discussed, NASA conducted the first ACIR in 2016 as its formal response to the FITARA mandate that the Agency CIO have approval authority over all IT spending. The ACIR process is designed to collect IT investment data across the Agency, including institutional, mission, and highly specialized IT, for review and approval by the Agency's senior IT governance board, the Information Technology Council. By including all Agency IT, the intent of the ACIR was to increase the Agency CIO's authority in IT acquisition planning across NASA.

[14] IG-13-015.

The OCIO attempted to leverage the ACIR process to address two of our previous recommendations: 1) the need to increase the office's visibility into the Agency's current IT assets and planned purchases and 2) the need to obtain CIO approval of all IT procurement expenditures over an established dollar threshold.[15] However, upon reviewing the ACIR implementation plan we remain concerned about the effectiveness of the ACIR process since its success is contingent upon completion of several high-level requirements, many of which are still in their infancy. These requirements include:

- Approved Agency enterprise architecture;
- Updated IT Baseline Service Levels;
- Data collection in each IT Program area;
- Center, Mission, and IT Program stakeholder engagement;
- Ongoing portfolio management within each IT Program area; and
- Establishment of an Information Technology Council.

Even though the OCIO revised the way IT investments are reported by instituting the ACIR, the bulk of IT budget authority did not change and still lies with the Mission Directorates and Centers. The majority of IT procurements at NASA – an estimated $739 million annually – are considered specialized IT embedded in Mission projects and operations and controlled by the Mission Directorates. At the Centers, IT spending is part of each Center's management and operations budget, over which the Agency CIO has limited oversight. The CIO only directly managed IT spending estimated at approximately $338 million in FY 2017. In addition, the CIO is only required to review IT procurements across the Agency in excess of $50 million. Apart from IT acquisitions above $50 million, most Mission Directorate and Center IT purchases are conducted outside the purview of the Agency CIO. IT procurements less than $50 million follow Center IT procurement procedures and generally are not reviewed by the Agency CIO before moving forward, unless presented to the CLT and ITC, as the CIO is the decision authority for those boards. We previously recommended the Agency establish a threshold that captures the majority of IT expenditures regardless of procurement instrument to provide the Agency CIO with increased visibility and authority over all Agency IT assets. In our opinion, setting the threshold at $50 million enables significant IT purchases to be made outside the purview of the Agency CIO.

Successful implementation of the ACIR plan also requires cooperation between the OCIO, Mission Directorates, and Centers. The ACIR places heavy reliance on Agency, Mission, IT Program Executives, and Center Investment Leads and requires more involvement by the OCIO in IT planning activities than in the past. However, we have reservations about the OCIO's ability to effectively engage the Mission Directorates in this manner. The decentralized nature of NASA's operations and its longstanding culture of autonomy historically have marginalized the authority of the Agency CIO, limiting the OCIO's visibility and control over a majority of the Agency's IT investments.

Complete and accurate IT investment data is another crucial element to the ACIR process. However, once NASA initiated the ACIR, it became clear that obtaining accurate investment data was difficult and to date the Agency cannot accurately identify its IT spending. For example, in FY 2015 NASA reported $1.4 billion in IT investments to OMB. However, OMB suspected that NASA was under-reporting and, using data from other Federal procurement databases, calculated $1.8 billion in NASA IT investments for

[15] The threshold established for Agency CIO approval is $50 million.

the same year. OMB officials attributed this $400 million discrepancy to a lack of detail provided by Center IT officials, limited insight into highly specialized mission IT, and a low number of projects reported to OMB as major IT investments.[16] Moreover, the incomplete IT investment data reported to OMB was the same data the OCIO used in the ACIR process. As a result of inconsistencies in NASA's IT investment reporting, in August 2016 the Agency's Executive Council instructed the Deputy Associate Administrator and the CIO to establish an IT Portfolio Review Team (also known as a "tiger team") to review and clarify the definitions of IT, review the Agency's current IT portfolio, identify unreported IT spending, and refine IT expenditure reporting processes.

However, the tiger team was unable to capture the total amount of IT spending at NASA even after consulting multiple sources including NASA's IT Portfolio, IT Security, Procurement, and Financial systems. Team members cited both significant gaps in reporting of IT investments by the Mission Directorates, the Jet Propulsion Laboratory and other contractor-managed laboratories, as well as the widely-held assumption that highly specialized and contractor-managed IT was excluded from reporting. Specifically, the review team found NASA's current IT portfolio is not organized in a way that maps to the Agency's programs and projects or reflects the plan envisioned under the BSA IT governance process. We noted similar shortcomings in our 2013 audit report when we reported that NASA spent $2 billion on IT in FY 2010 even though it planned to spend $1.6 billion – a $400 million discrepancy that did not come to the Agency CIO's attention until the Mission Directorates reported actual expenditures in response to a separate OMB request.

A major factor in NASA's ongoing deficiencies in accurately reporting its IT spending is the lack of an agreed-upon definition of IT. In fact, during its work the tiger team identified 33 different definitions of IT used at NASA. In addition, the OCIO concluded the acronym "ACIR" was confusing stakeholders and proposed changing the name to "Information Technology Capital Investment Review." In its December 2016 final report, the tiger team offered definitions of six information technology terms to improve reporting on the Agency's IT investment portfolio by making it more consistent and accurate.[17]

The Information Technology Council (ITC) accepted the tiger team's recommendations to clarify IT-related definitions; improve transparency, management, oversight, and accountability of NASA's IT portfolio; and reduce the multiple data calls that are taxing organizations responsible for reporting IT investments. Nevertheless, the tiger team acknowledged in its final report that the OCIO would be challenged to implement its recommendations given the office's multiple issues with the current IT portfolio process and suggested a phased approach to build capability and maturity. We noted the ITC did not specifically assign implementation responsibility for the recommendations to anyone as is the case in most of these decision memorandums.

Portfolio Reviews are another integral piece of the ACIR process and are designed to increase the Agency CIO's visibility into the Agency's IT portfolio. These reviews involve Mission Directorate and Center representatives and are designed to assess NASA's entire IT portfolio, including program and project execution and results, capabilities, service delivery, and assets. However, the OCIO's limited or lack of insight into non-institutional IT hinders its ability to conduct accurate Portfolio Reviews. For example, during a May 2016 ITC meeting the Communications Program Executive presented the concern

[16] For FY 2015, OMB compared NASA's reported total to data extracted from the Federal Procurement Data System on IT products.

[17] The review team provided definitions for Information Technology, Information Technology Service, Information Technology Project, Information Technology Investment, Candidate Major Information Technology Investment, and Highly Specialized Information Technology. See Appendix C for its definitions of these terms.

that limited or lack of insight into non-institutional communications services does not allow him to perform accurate portfolio analysis across the Communications Program. In fact, subsequent to the FY 2017 budget submission, the Program Executive identified $48 million spent on communication services outside the purview of the OCIO. While the OCIO's original implementation schedule had Portfolio Reviews starting in October 2016, the first review did not take place until late March 2017. In late January 2017, the Agency CIO expressed concerns that OCIO personnel did not have the skills to conduct such reviews but has since assigned four staff to IT portfolio data collection and reviews, including a Business Management specialist hired to lead the review process.

In addition, the BSA IT team recommended the Agency CIO conduct Center Functional Reviews every 3 years to examine each Center's compliance with NASA IT policies, assess the adequacy of internal controls and management systems, and to assess the effectiveness and efficiency of Center IT operations. The BSA Implementation Plan assumed that Center Functional Reviews would be used to help ensure the implementation and effective use of the new IT governance framework and processes. These reviews assess six areas: (1) Information Security, (2) Enterprise Architecture, (3) Governance, (4) Requirements, (5) Enterprise Adoption, and (6) Performance, Outcomes, and Efficiencies. While the first cycle of reviews were scheduled to be completed in May 2016, the OCIO did not begin its first Center Functional Review until November 2016 at Langley Research Center (Langley), followed by Kennedy Space Center (Kennedy) in April 2017.

The OCIO provided the standards, metrics, and assessments for each IT program reviewed at Langley and Kennedy. We noted that the majority of the information gathered was summary-level and offered only a cursory examination of the information provided. Therefore, we question whether the Center Functional Reviews, as currently executed, accurately and comprehensively evaluate compliance with NASA IT policies, assess the adequacy of internal controls, and measure the implementation of the new IT governance structure or satisfy the intent of the MSC and BSA.

In sum, NASA is relying on the ACIR process to address our 2013 audit recommendations, meet FITARA requirements, and provide the Agency CIO with greater visibility into IT spending across the Agency. The OCIO is making some progress in engaging organizations outside the OCIO in these initiatives. For example, half of the Agency's IT portfolios have been updated and several Missions are clarifying their IT reporting guidance. However, to date the OCIO is executing the reviews without the benefit of complete investment data or the necessary enterprise architecture in place. As a result, the ACIR review has not met its intent of producing comprehensive and high-quality information to help the Agency CIO better manage NASA's IT expenditures.

NASA Enterprise Architecture Remains Immature

Enterprise architecture in the IT context is essentially a map of IT assets, business processes, and governance principles that drive ongoing investment and management decisions.[18] NASA's enterprise architecture is intended to align all aspects of the Agency's technology infrastructure to improve IT performance, support NASA's mission, and assist the IT governance boards in making informed investment and management decisions. As noted above, the ACIR process cannot be successful absent

[18] Daniel Minoli, *Enterprise Architecture A to Z: Frameworks, Business Process Modeling, SOA, and Infrastructure Technology* (Boca Raton, FL: CRC Press, 2008), accessed July 26, 2017, https://books.google.com/books?id=Fs5bMNBXLEMC&pg=PA10&source=gbs_selected_pages&cad=2#v=onepage&q&f=false.

a comprehensive Agency enterprise architecture. In fact, according to the BSA Implementation Plan, there is a risk that significant IT decisions will be suboptimal if the appropriate level of enterprise architecture is not defined and communicated to support the IT governance framework and processes. However, NASA has struggled to establish such an architecture for many years, contributing to the undisciplined manner in which NASA makes IT investments.

In 2005, we first reported that the NASA OCIO was developing requirements and plans for an enterprise-wide IT architecture and associated management processes.[19] At the time, we warned that until those efforts were fully integrated into the budget and operations for each Mission Directorate and Center, the ability of the CIO to have insight into and influence over IT organizations, their operations, and their budgets would be limited.

Twelve years later, NASA's enterprise architecture remains in its infancy. NASA policy appropriately describes the Agency's enterprise architecture as a mechanism designed to map all IT initiatives, capabilities, and services to Agency needs; identify all potential shortfalls and redundancies in IT capabilities; and analyze solutions. Yet, most of this work remains incomplete. Development of an effective enterprise architecture for NASA should be based on information about IT services, applications, and assets from across the enterprise, including the Centers and Missions, and also take into account project and activity reviews, IT service catalogs, end-user configuration management, databases, applications, and inventories of all IT systems. However, because much of this information is still not readily available, the OCIO continues to lack the basic building blocks to create such an architecture. Specifically, the OCIO lacks visibility into all Agency IT networks, has yet to develop a network diagram that captures the entirety of NASA's existing network configuration, and does not maintain a comprehensive and accurate inventory of IT assets.

Development of an effective enterprise architecture also helps create a unified IT environment across an organization. However, IT at NASA remains highly fragmented and lacks mechanisms for determining what hardware, software, and services should be provided enterprise-wide versus those specific to a Center or Mission. According to NASA's Enterprise Architect – a position that resides in the Agency OCIO – the Agency should develop a roadmap to move forward as a single enterprise as opposed to individual Centers developing their own IT architectures as has been the case historically at NASA. In a prior audit, several NASA IT representatives recommended the Agency establish strict guidelines to identify when individual Centers are permitted to deviate from enterprise-wide IT standards based on unique requirements. Other IT officials said the Agency needs to develop a comprehensive IT foundation before an enterprise-based IT solution could be successful.[20] Many of the IT officials we interviewed for this audit stressed the need for an IT "roadmap" to understand the path the Agency is taking with its IT investments because of the OCIO's limited visibility into IT infrastructure or IT spending at the Center and Mission levels. The varying infrastructure, applications, and processes across NASA's Mission Directorates and Centers create procurement and labor redundancies among common business processes and encourages shadow IT.

Previous OIG and Government Accountability Office (GAO) evaluations have concluded that NASA's lack of a mature enterprise architecture has contributed to significant governance issues and an inability to successfully manage Agency-wide IT services. In January 2014, we found that the lack of a mature enterprise architecture contributed to the unsuccessful implementation of Agency Consolidated

[19] IG-05-013.

[20] NASA OIG, "Review of NASA's Agency Consolidated End-User Services Contract" (IG-14-013, January 30, 2014).

End-User Services or ACES, an Agency-wide IT services contract that provides basic hardware and software computing services to NASA employees.[21] Prior to ACES, each Center tailored its IT contract to meet its individual needs using Center-specific delivery orders by purchasing hardware and services and establishing security parameters. Likewise, a November 2013 GAO report found only 17 percent of NASA's IT investments were included in its enterprise architecture, which in turn limited the Agency's ability to identify low-value, duplicative, or wasteful investments.[22] These issues are well-known to NASA management and surfaced most recently during the BSA IT security spending review in April 2016 when the Agency acknowledged that the $93 million it spends annually on IT security is not optimized across the Centers. We also found that NASA has over 3,000 software applications written in 59 different programming languages, a situation the Agency's Applications Program Executive recognized leads to unnecessary duplication. Further, Agency data indicated over 20 instances of collaboration software in use across the Centers at a cost of $12.6 million.

As of July 2017, NASA's Enterprise Architect is working to develop an enterprise architecture for the IT domains under the control of the OCIO. In addition, the position is being moved from the Capital Planning and Governance Division within the OCIO to its Enterprise Services Integration Division to help drive decisions made by Program Executives. Moreover, the two primary policies governing NASA's enterprise architecture are being updated with expected completion dates in December 2017 and July 2018, respectively.[23] However, as we pointed out above, the development of an enterprise architecture has been ongoing for many years and the current lack of insight, authority, and accurate data continue to be major risks to the success of the ACIR process and the Agency's overall efforts to restructure its IT governance.

New IT Governance Boards Ineffective

The effectiveness of IT governance processes depends, in large measure, on effective engagement by the entity's governing boards and senior management. Best practices dictate that any such board or senior manager should exercise an active role in directing, evaluating, and monitoring IT operations, projects, and security. In 2013, we found that the complexity of NASA's IT advisory board structure coupled with a lack of understanding about the relationship among the boards caused confusion and diminished their value to the Agency's IT governance process. Moreover, NASA policy failed to provide clear guidance regarding the issues that had to be submitted to the boards for approval. As a result, we found when making IT decisions NASA managers tended to rely on informal relationships outside the board structure rather than formalized business processes.

To address these issues, we recommended that NASA reevaluate the relevancy, composition, and purpose of its IT boards; require the use of governance boards for all major IT decisions and investments, including those made by Mission Directorates; revise the board charters; and develop a plan to educate IT personnel regarding the charters and interrelationships of the boards.

[21] IG-14-013.

[22] GAO, "Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Saving" (GAO-14-65, November 2013).

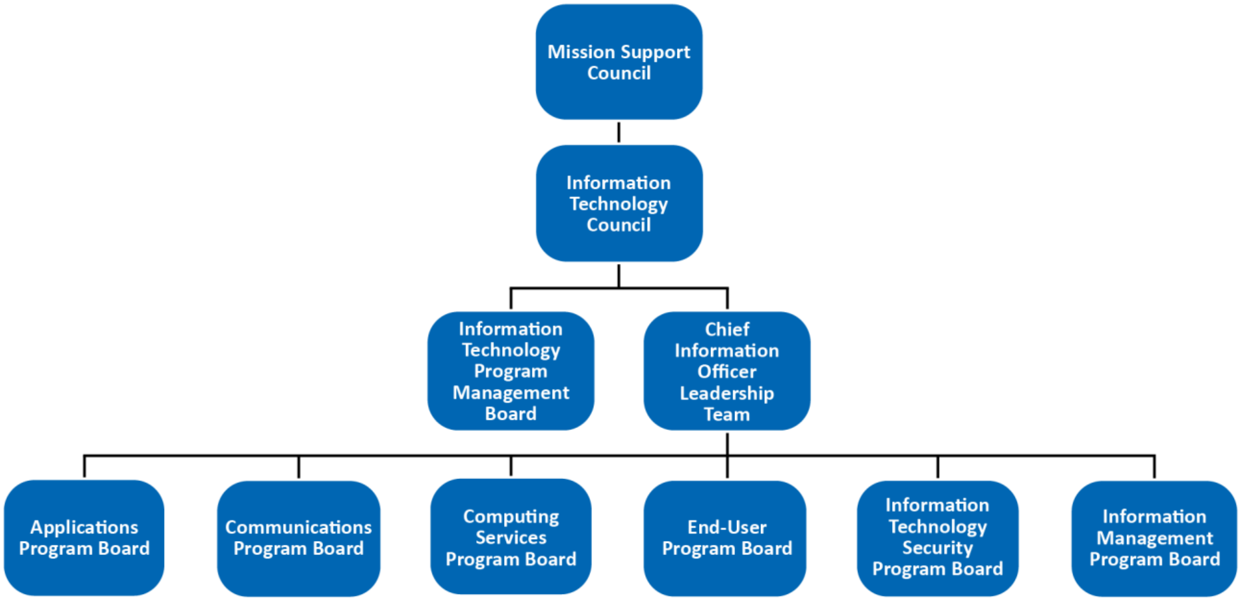
[23] NASA Policy Directive (NPD) 2830.1A, "NASA Enterprise Architecture," November 2, 2011, and NASA Procedural Requirements (NPR) 2830.1A, "NASA Enterprise Architecture Procedures," December 19, 2013.

Since our 2013 audit, the OCIO made changes to two of the three top-level governance boards: creating the Information Technology Council (ITC) and the Chief Information Officer Leadership Team (CLT). As with the previous structure, the Agency CIO is the decision authority of NASA's senior IT advisory board (ITC) and the board reports to the MSC. However, unlike the previous structure, the new CLT serves as an advisory board that reports to the ITC. The IT Program Management Board (IT PMB) – the third board we examined in our previous review – also reports to the ITC and serves as a forum for Agency oversight and evaluation of active IT projects. NASA's three top-level IT governance boards and their supporting Program Boards are discussed in detail below while the Agency's IT governance framework is depicted in Figure 4.

- *Information Technology Council*. Serves as the Agency's senior decision-making body for IT and information resources management. The board, which reports to the MSC, meets every other month or as needed as issues arise. The Agency CIO serves as Chair, while the Chief Financial Officer, Assistant Administrators, Associate Center Directors, and Deputy Associate Administrators of the Mission Directorates serve as board members. The ITC approves all Agency IT investments annually through the ACIR, approves unplanned investments with acquisition and implementation costs above $10 million, and authorizes NASA-funded investment or divestment as recommended by the CLT and approved by the Agency CIO.
- *Chief Information Officer Leadership Team*. The CLT, chaired by the Agency CIO with the Deputy CIO, Associate CIOs, Center CIOs, Jet Propulsion Laboratory CIO, NASA Shared Services Center (NSSC) CIO, and Mission Directorate representatives, is intended to provide visibility into Mission Directorate and Center IT operations. The CLT meets weekly or as needed to review requests forwarded to the ITC for disposition. Under NASA policy, the Agency CIO approves investments between $1 – $10 million while Center CIOs approve unplanned IT investments under $1 million.
- *Information Technology Program Management Board*. This board – the only one of the three senior advisory boards left unchanged since our 2013 report – serves as a forum for high-level Agency oversight and evaluation of active Agency IT projects. Chaired by the NASA Deputy CIO, the board holds monthly or as-needed meetings and includes the Associate CIO for Capital Planning and Governance, officials from the Office of the Chief Engineer, Enterprise Architecture lead, and rotating members from the Mission Directorates, Centers, and CLT representatives. The IT PMB is responsible for reviewing IT projects costing $1 million or more.
- *Program Boards*. Six Program Boards (Applications, Communications, Computing Services, End-User, IT Security, and Information Management) continue to support the ITC and CLT even though, as of August 2017, their charters had not been finalized.

In addition to these formal IT advisory boards, the BSA Implementation Plan identified a need for a variety of "support functions" critical to efficient and effective operations of the board structure. These include both permanent functions within the CIO, Mission, and Programmatic organizations as well as temporary "working groups" that may be established by the Agency CIO or boards to address specific issues.

Figure 4: NASA's IT Governance Framework


Mission Support Council
Information Technology Council
Information Technology Program Management Board
Chief Information Officer Leadership Team
Applications Program Board
Communications Program Board
Computing Services Program Board
End-User Program Board
Information Technology Security Program Board
Information Management Program Board

Source: BSA Implementation Plan.

As part of this current review, we surveyed the Center CIOs, Center Chief Information Security Officers (CISO), and Mission Directorate IT Representatives to solicit their opinions about the effectiveness of NASA's revised IT governance structure. Overall, these IT officials found the governance structure immature, unstable, and difficult to understand. For example, one official stated that inconsistencies between organizational hierarchies made it difficult to understand why and how decisions are made. Other IT officials were unsure of what types of decisions were being brought to the boards and how the decisions were subsequently communicated to Center officials. In fact, several officials told us they remain confused about how to even raise an issue to the boards. Moreover, we were told that decisions made by the boards are not consistently communicated to the Center officials required to implement them. Finally, another official commented the boards were change-resistant and its decision-making process was more like a popularity contest that often resulted in continuation of misguided policies. In light of these concerns, we reviewed meeting minutes of the IT PMB and found that while the board appears to serve its purpose by discussing key decision points for a variety of IT programs, each of the 15 projects up for review was approved even though one or more board members voiced significant concerns on 7 of the projects.

We interviewed all 11 Center CISOs and found half of them confused by the new board structure, specifically regarding the role of IT security within the Agency's overall IT framework. The majority of Center and other security officials we spoke with complained they did not have enough input into the boards' decisions. Several of the security officials raised concerns that the majority of board members are from the OCIO and Mission Directorates do not have a large enough presence on the advisory boards. These concerns echo findings in our 2013 audit where we reported that security officials did not believe IT security was adequately built into the Agency's IT governance model, suggesting that it appeared to be an afterthought.

Completion of all the charters for NASA's revised IT advisory boards is essential to educate employees about the new governance process and how to raise important Agency-wide issues to the three top-level IT boards. Until then, the new board structure will remain incomplete.

OCIO Roles and Responsibilities Remain Unclear

Despite a two-year effort, the OCIO has not finalized the roles and responsibilities associated with the Agency's new governance structure. We previously reported that NASA's organizational structure marginalized the Agency CIO's role because that position was the only one of seven "Chiefs" who did not report directly to the NASA Administrator.[24] Additionally, we noted that the Mission Directorates and Centers employed their own CIOs and IT security personnel who manage hundreds of independently operated networks and tens of thousands of computers.

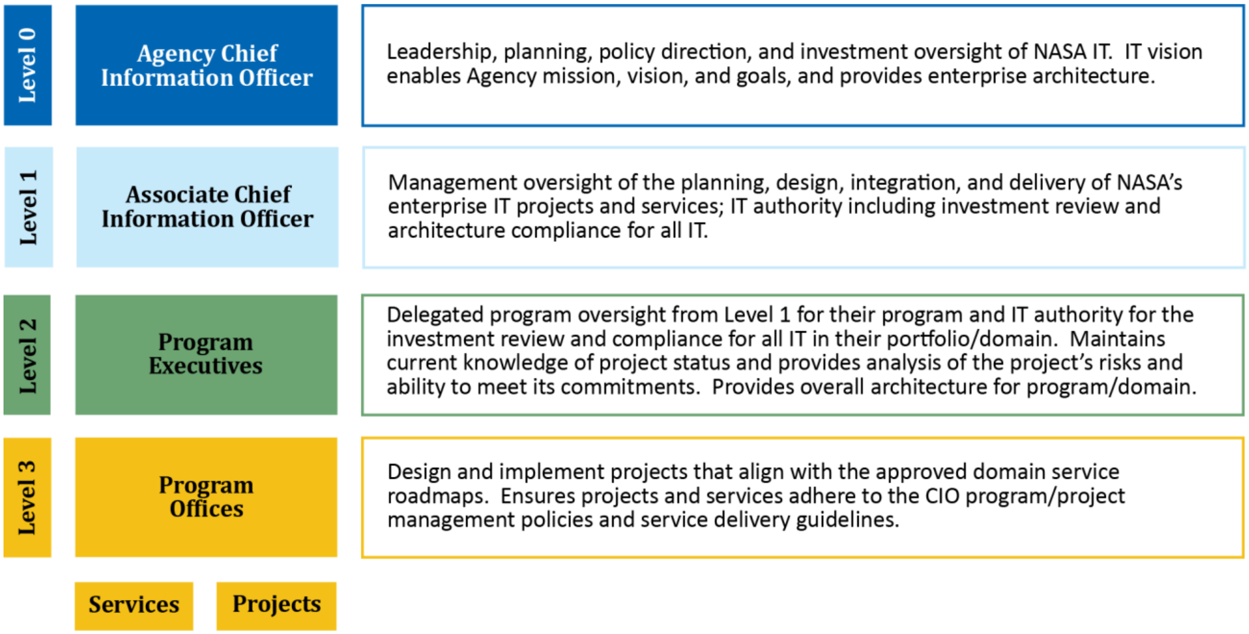
In response to our recommendations, NASA revised its organizational chart to make the Agency CIO a direct report to the NASA Administrator.[25] We also recommended NASA revise the job titles of the Mission Directorate and Center CIOs to more clearly delineate their roles and responsibilities, and make the Mission Directorate CIO position a direct report to the Agency CIO and the principal advocate for the IT needs of their respective Directorates. The Agency agreed with most of these recommendations except changing the title of the Center CIOs and making the Mission Directorate CIOs direct reports to the Agency CIO. We agreed to close these recommendations based on actions described in the BSA Decision Package.

Specifically, the BSA examined IT roles and responsibilities across the Agency and, based on that assessment, the MSC directed the OCIO to create a level 0 through 3 management structure and to appoint Program Executives for each IT domain (see Figure 5 below for an explanation and depiction of this structure). The OCIO was also directed to develop a 5-year strategic plan that facilitated incremental growth in IT management with MSC approvals between phases. The May 2015 BSA Decision Package included a high-level description of the roles and responsibilities of the management structure and, after some minor revisions by the OCIO, the office included it as part of its BSA Implementation Plan in March 2016.

[24] The other "Chiefs" at NASA are the Chief Financial Officer, Chief Scientist, Chief Technologist, Chief Engineer, Chief of Safety and Mission Assurance, and the Chief Health and Medical Officer.

[25] See NPD 1000.3E, "The NASA Organization," April 15, 2015. However, in the section of this policy that details the Agency CIO's mission and responsibilities, the NPD states the CIO reports to the NASA Deputy Administrator – the reporting structure in place in 2013 when we made our initial recommendation.

Figure 5: IT Roles and Responsibilities – CIO Program Level Descriptions



Level 0	Agency Chief Information Officer	Leadership, planning, policy direction, and investment oversight of NASA IT. IT vision enables Agency mission, vision, and goals, and provides enterprise architecture.
Level 1	Associate Chief Information Officer	Management oversight of the planning, design, integration, and delivery of NASA's enterprise IT projects and services; IT authority including investment review and architecture compliance for all IT.
Level 2	Program Executives	Delegated program oversight from Level 1 for their program and IT authority for the investment review and compliance for all IT in their portfolio/domain. Maintains current knowledge of project status and provides analysis of the project's risks and ability to meet its commitments. Provides overall architecture for program/domain.
Level 3	Program Offices	Design and implement projects that align with the approved domain service roadmaps. Ensures projects and services adhere to the CIO program/project management policies and service delivery guidelines.
	Services Projects	

Source: BSA Implementation Plan.

The BSA Implementation Plan, approved by the MSC in March 2016, does not include defined roles and responsibilities for IT personnel other than the high-level description included above. Rather, the Plan outlines a schedule for completing actions needed to:

- Finalize detailed roles and responsibilities at each of the levels;
- Assess, define, and implement changes to current organizational structures;
- Define or update positions and position descriptions to mirror the updated roles and responsibilities;
- Address skill and resource gaps necessary to implement the new structure and roles; and
- Communicate and manage cultural and organizational change required to migrate to the new structure.

The author of the Implementation Plan, who previously served as a Center CIO and is currently Marshall's Associate Director, stated that defining roles and responsibilities by the summer of 2016 was crucial to establishing the new governance structure; however, as of August 2017, the task had not been completed. The OCIO missed many of the target dates in the BSA Implementation Plan schedule including fundamental tasks associated with roles and responsibilities for IT, which has been delayed from May 2017 until December 2017. For example, a task identified as "Confirm Detailed Definition of Roles and Responsibilities" which includes several subtasks, originally expected to be completed in February 2016 has been moved to December 2017 – a 22-month delay.

Additionally, the Plan only includes a single reference to Mission Directorate IT Representatives in the roles and responsibilities section even though it states that implementation of BSA IT decisions requires closer integration between the Agency CIO and the mission and programs across NASA. However, the task to define their relationship to the OCIO, originally assigned to the Agency CIO with a completion date of May 2016, subsequently was reassigned to the Deputy CIO with a new completion date of April 2017. This deadline was not met and as of August 2017 the task remained incomplete. At the close of our fieldwork, the OCIO was evaluating the progress made in revising the governance structure. As of June 2017, the Agency CIO considers NASA to be at the mid-point of implementation – four years since we made our recommendation to clarify roles and responsibilities related to IT governance.

In its implementation plan, the OCIO identified several constraints and risks that could impact successful implementation of the new governance model. Many of these risks are longstanding and have thwarted previous efforts to improve IT governance at NASA. Perhaps most telling is the following constraint:

> *The plan is dependent on the level of cooperation, communication, and discipline of the leadership and stakeholders that are engaged at each level of the new structure. Primarily, this constraint is associated with the ability to leverage resources in a collaborative way to meet agency needs across Center boundaries.*[26]

Similarly, under potential risks, the plan notes that given NASA's history of failing to enforce IT policy, the potential exists for these new roles and responsibilities to go unimplemented or be ignored by stakeholders. In our view, this risk has a high likelihood of being realized given the Agency's lack of success overcoming these same barriers in the past.

Without clearly defining roles and responsibilities under NASA's revised IT governance structure, it is much less likely that key stakeholders will understand or follow the new model. Even among senior IT officials, several we interviewed said they have not seen many changes in the governance structure in the four years since our previous audit. In fact, a June 2016 review conducted by Forrester found that Program strategy and expectations were not well understood or being met and that Program Executives felt they had limited decision-making power. The review stated that key managers and functions including Program Executives, Program Managers, Center CIOs, Program Management Office, Enterprise Architecture, Emerging Technology and Desktop Standards, and Enterprise Integration needed clearer definitions of responsibilities and accountabilities. We found the slow process to define key elements of the Agency's new governance model has delayed its implementation, resulting in confusion and reduced their chance of success in improving NASA's IT governance model.

Unclear Security Roles and Lack of Accurate Inventory Weaken NASA's IT Security

We found significant confusion at NASA as to the roles, responsibilities, and chain-of-command regarding IT security operations. This confusion coupled with the lack of visibility and accountability over IT assets has weakened NASA's security posture and undermined the Agency's efforts to implement an effective IT governance structure.

Unclear IT Security Roles and Responsibilities

The NASA Senior Agency Information Security Officer (SAISO) is the Agency-level official responsible for managing IT security at the Agency. The SAISO leads the IT Security Division within the OCIO, an office that coordinates information security operations, security governance, security architecture and

[26] NASA MSC/BSA "Information Technology Implementation Plan," March 9, 2016.

engineering, and cyber-threat analysis. However, individual Mission Directorates and Centers have their own IT security personnel who do not report to the SAISO and this diffusion of authority adds a level of complexity and lack of accountability that negatively impacts coordinated and comprehensive efforts to secure NASA's IT.

The IT BSA identified a similar lack of coordination across IT security service delivery as a significant issue caused by an absence of an enterprise-wide IT security risk management framework and strategy. Further, we found in 2013 and continue to find the Agency CIO and SAISO challenged to enforce IT security initiatives on a large portion of NASA's IT assets that fall outside of their control. NASA's IT environment contains hundreds of networks operated by the Mission Directorates and Centers, and consequently Center- and Mission-based personnel are responsible for security, risk determination, and risk acceptance on those systems. Mission Directorates fund their IT networks, and Mission security personnel rather than the CIO or SAISO are responsible for securing these networks. Even though Center CIOs are "direct reports" to the Agency CIO (except those at Armstrong Flight Research Center and the Jet Propulsion Laboratory) funding for Center-based IT generally comes from the Center Director's budget, essentially creating two reporting structures for Center CIOs.

NASA has over 170 positions designated as IT security (both civil service and contractor employees) at Headquarters and the Centers in addition to IT security personnel imbedded within the Mission Directorates. These resources are used to secure NASA's 496 known information systems with 297 unique system owners, the vast majority of which are outside the SAISO's direct control. System owners are required to implement effective security controls and take actions to identify and eliminate security deficiencies and weaknesses. The fact that many systems exist outside the OCIO's control limits the Agency's ability to monitor its security posture. In fact, in response to a May 2017 Executive Order NASA commissioned a tiger team to identify the Agency's cybersecurity risk posture. The Agency CIO told us that she could not determine whether security lapses truly exist or whether it was the result of limited oversight into the totality of Agency IT assets. This disconnect hampers NASA's ability to make informed operational and investment decisions that mitigate IT security risks.

The lack of a single chain-of-command for IT security creates confusion and complicates responsibilities. OCIO management has two senior positions with IT security responsibilities: (1) Senior Advisor for Cybersecurity and (2) Senior Agency Information Security Officer. During our fieldwork, the SAISO raised concerns about the Agency's fragmented reporting hierarchy for IT security. For example, apart from the OCIO's IT Security Division, the Enterprise Service and Integration Division has their own security function whose employees do not report to the SAISO. Additionally, the Mission Directorates have their own IT security operations and personnel, none of which report to the Agency SAISO. Likewise, the responsibilities of the Security Operations Center (SOC), NASA's nerve center for detection and monitoring of IT security incidents at the Agency, are dispersed. The SOC is located at the Ames Research Center (Ames) with key personnel reporting to management at that Center, yet its funding and funding-related decisions are made by the IT Security Division within the OCIO. When an incident is detected, Center-based incident response personnel are often responsible for resolution. Given the SOC's limited access to Mission Directorate IT systems, it relies on relationships established with Center personnel to address Mission-related issues. Moreover, the Center CISOs do not report to the Agency SAISO but rather to the Center CIO and Center Director.

These challenges are not unique to NASA. In August 2016, GAO identified several factors that challenged SAISO authority across the Federal government: (1) competing priorities between Agency operations and information security, (2) coordination with component organizations and other offices, (3) availability of security-related information from component organizations and IT contractors, (4) oversight of indirect reports and IT contractors, and (5) the position of the CISO within the Agency's hierarchy.[27]

As a result of the dispersed security responsibilities at NASA, Center CISOs told us the Agency does not have a viable IT security strategy and has not made IT security a priority. In their opinion, timely actions are not taken once a security issue is identified, NASA lacks a common IT security strategy architecture or baseline, CISOs are managing significant vulnerabilities without proper tools, and IT security practices vary widely across the Agency. We noted that even basic IT security practices – such as defining which users are granted elevated privileges to access IT systems – varies by Center. By default, employees at Langley, Johnson Space Center (Johnson), and Marshall automatically receive elevated privileges that permit them to download or update software and make configuration or other changes to their NASA computers. Conversely, employees at Kennedy and Glenn Research Center (Glenn) require several levels of approval to achieve the same level of access.[28]

When we asked senior OCIO officials about the CISOs' concerns, they indicated that the ongoing Continuous Diagnostics and Mitigation (CDM) program would address many of these issues. CDM is a Federal IT security program developed by OMB and run by the Department of Homeland Security that provides agencies with IT security tools to identify security issues and help meet Federal security requirements. NASA started implementing CDM tools in November 2016 and expects the software to, among other things, identify assets connected to its networks, support patch and vulnerability management, prevent malicious software, and increase visibility over all networks to identify the Agency's true risk posture. While using the CDM security tools will provide NASA large amounts of data about its IT environment, the real question is what, if any, actions Agency IT managers will take based on this information. Because IT managers told us they do not have the resources to address this information, we are concerned that NASA will miss an important opportunity to improve the Agency's IT security posture without guidance from the SAISO on how to prioritize and take action on this data.

NASA's Information Technology Security Posture Continues to be Hobbled by an Incomplete and Inaccurate Inventory of IT Assets

According to OMB, agencies without an empowered CIO regularly lack a complete and accurate inventory of IT assets and services across the enterprise. In our 2013 report, we found Agency efforts to establish a comprehensive IT security inventory had been thwarted by inconsistent enforcement of policies and implementation of tools intended to capture critical inventory information, pockets of opposition from groups within NASA who would not agree to provide requested information, and inconsistent guidance from OCIO IT security managers.

[27] GAO, "Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority" (GAO-16-686, August 2016).

[28] In an effort to protect Agency IT assets and information, NASA's security policy directs users to receive the minimum privileges necessary to complete their job. See NPR 2810.1A, "Security of Information Technology," May 16, 2006.

Despite its criticality to developing an effective IT security program, NASA continues to lack a complete and accurate inventory of all IT equipment operating on its networks. Lack of such an inventory results in reduced or diminished visibility by the OCIO over the Agency's assets and an inability to effectively manage, monitor, and report the security status of all devices connected to its networks.

During this current review, we asked Center CIOs if they were able to account for all institutional and mission systems and hardware at their respective Centers. Only 4 of the 11 CIOs said they could account for all inventory at their Center. We posed the same question to the Center CISOs and only 1 of the 11 stated they could account for all inventory at their Center. While IT managers across the Agency admitted they were still struggling to understand the inventory of all mission systems and hardware at their Centers, the situation has improved since our 2013 review. The lack of an accurate inventory of IT assets is an ongoing weakness that, if not rectified, will continue to negatively impact the Agency's attempt to improve its IT governance. While the Agency expects CDM to assist in addressing its inventory concerns, CDM's success will depend on collaboration across functional boundaries within NASA to ensure all assets are identified.

Concerns About Staffing, Expertise, and Retention Continue to Impact Effectiveness of NASA's IT

Contributing to the slow pace of improvement at NASA is the lack of OCIO staff with the skills needed to successfully execute the new IT governance model. We recognize the decentralized nature of NASA's IT organization coupled with the Agency's historic culture of operating in silos are major obstacles. However, a high turnover in senior IT managers and lack of deep technical expertise are significant impediments to a well-functioning OCIO and, ultimately, the Agency's IT operations.

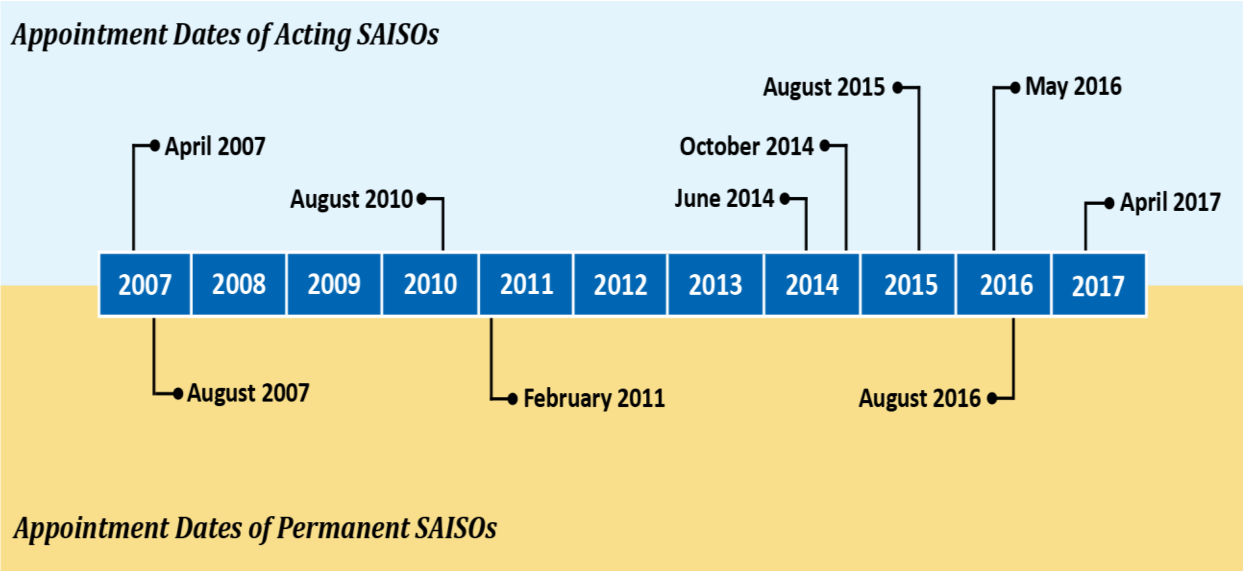
In 2013, we recommended the NASA Administrator evaluate the OCIO's resources to ensure the Office has the appropriate number of personnel with the appropriate skills. The Administrator concurred and instructed the then-new Agency CIO to identify the resources and skills necessary to support planned improvements to the Agency's IT governance and to the expanded responsibilities for the OCIO inherent in the OIG's recommendations. In response, the Agency CIO hired Forrester to conduct an organizational assessment to evaluate the personnel, skill sets, and capabilities within his organization. Forrester's February 2014 report described a highly fragmented IT structure and culture at NASA with inadequate mechanisms for determining what IT should be common ("within the enterprise") and what IT should be specific to individual Centers or Missions. The assessment compared NASA to both best industry practices and other large organizations in 10 organizational characteristic areas.[29] NASA scored well below average in 7 of 10 areas and average in the remaining 3. Based on its review, Forrester identified IT architecture, infrastructure, applications management, and vendor management as the primary areas where OCIO skills needed to be strengthened. However, based on our current work it appears the OCIO has been unsuccessful in rectifying these shortcomings.

In November 2015, the CIO who commissioned the Forrester review retired after 28 months as CIO. The Deputy CIO had left the Agency 8 months prior and the current CIO – hired in July 2015 as the Deputy CIO – assumed the CIO position in September 2015. In the ensuing 2 years, new senior leaders were appointed for all four OCIO Divisions. The OCIO also created and filled the position of IT Governance

[29] The 10 organizational characteristics reviewed were: (1) Basic Services, (2) Applications Management, (3) Architecture, (4) Budgeting, (5) Culture, (6) Governance, (7) Data, (8) Vendor Management, (9) Projects, and (10) Structure.

Lead in Janaury 2014. Similarly, senior Center-based IT positions also experienced high turnover from May 2012 to June 2016 with the departure of 9 of 11 Center CIOs and 8 Center-level CISOs.[30] Moreover, as discussed previously, in April 2017 the Agency SAISO left NASA after only 8 months and as of August 2017 the position had not been permanently filled. Compounding the managerial instability in this position, during the 26 months prior to the SAISO's arrival in August 2016, four different employees served as NASA's Acting Senior Security Officer. In fact, since 2007, 10 individuals have served as the Agency SAISO, either in an acting or permanent role. See Figure 6 for a timeline of the acting and permanent SAISO's appointment dates over the past 10 years. IT security officials across NASA told us the instability and high turnover in this position has hindered the Agency's ability to sustain core IT security processes and led to changing security priorities. Apart from these senior IT positions, Center CIOs and CISOs expressed concerns in response to an OIG survey about NASA's aging IT workforce and impending retirements as well as a competitive labor market that makes it difficult for the Agency to retain workers with necessary skills.

Figure 6: Appointment Dates of Acting and Permanent SAISOs



Source: OIG analysis of OCIO-provided data.

IT officials across the Agency said they believe the organization lacks the staff and skills necessary to successfully execute the BSA Implementation Plan given its size and scope. In fact, the OCIO had to seek assistance from outside its Headquarters staff to complete the BSA Implementation Plan. The CIO informed us she plans to leverage Center IT resources to assist with implementation of the Plan despite concerns from Center IT officials that they are short-staffed and lack resources to contribute to this effort.

Concerns about the lack of staff with IT security skills are nothing new at NASA. Five years ago in its workforce planning document, the OCIO acknowledged that its Headquarters staff did not possess the technical knowledge or skills required to significantly improve NASA's IT security posture.[31] Moreover,

[30] The turnover occurred at the following Centers: Ames, Armstrong Flight Research Center (Armstrong), Glenn, Goddard Space Flight Center (Goddard), Headquarters, Johnson, Kennedy, Marshall, and NSSC for the nine Center CIO positions and Ames, Armstrong, Glenn, Goddard, Johnson, Marshall, NSSC, and Stennis Space Center for the eight Center-level CISO positions.

[31] NASA OCIO, "NASA OCIO Workforce Plan 2012-2015," July 1, 2012.

NASA does not require its cybersecurity personnel to maintain industry certifications and reported to Congress in 2016 that only 58 of its 129 civil service cybersecurity staff (45 percent) had current industry recognized certifications. As noted earlier, the Agency CIO engaged private consultants to review NASA's IT organizational structure and IT governance and many of the findings and recommendations reached by these outside consultants are similar to the conclusions in our 2013 IT governance report.

Study after study over more than a decade has resulted in similar findings, but the OCIO has exhibited limited forward momentum in substantively addressing the challenges facing NASA's IT security and governance. For example, a December 2005 organizational study concluded that the OCIO, with its limited staff, faced tremendous challenges in fulfilling its responsibility to manage NASA's IT given the Agency's decentralized and mission-focused environment.[32] The report also found that NASA IT organizations needed stronger lines of accountability and authority throughout the governance structure, a more formal reporting structure between the Agency CIO and Mission Directorate and Center CIOs, personnel improvements, and better reporting and monitoring capabilities regarding program performance. Eleven years later, another organizational assessment found several NASA IT functions misaligned, a lack of an optimal organizational structure, and only a portion of the IT management capabilities needed to be successful.[33] This June 2016 review acknowledged that while the OCIO was trying to create positive change, the Agency's organizational structure perpetuated the same IT management challenges related to accountability, clear priorities, governance, and decision making.

In an August 2016 organizational study, the OCIO acknowledged the significant challenges it faces and described what success would look like.[34] Specifically, the current Agency CIO said success would entail: (1) clarifying roles and responsibilities, (2) positioning all NASA IT for the future, (3) organizational stability, and (4) eliminating redundancies and overlaps of functions. Unfortunately, the OCIO, and by extension NASA, continues to struggle with these issues today.

Finally, in March 2017 the Agency CIO proposed reorganizing the OCIO to create a vendor management office, potential name changes for the four existing divisions, and minor changes to division responsibilities.[35] While not finalized, in our opinion the proposed reorganization fails to address deep-seated structural and organizational IT issues that have impeded past efforts to address NASA's IT deficiencies. For example, under the plan responsibility for IT security would remain dispersed among multiple entities with no clarification in the chain-of-command. In fact, this reorganization would reverse a decision the Agency CIO made in December 2015 to align most IT security functions within the IT Security Division instead of having security functions spread throughout its other divisions. Unfortunately, this decision was never fully implemented and the proposed reorganization would reverse course less than 2 years later. In our view, greater segmentation of the IT security structure limits the authority of the SAISO and weakens NASA's overall IT security posture.

[32] Tech Vision Consulting, LLC, "NASA CIO Organizational Study Final Report," December 15, 2005.

[33] Forrester Research, Inc., "IT Organization Assessment and Design for NASA OCIO," June 27, 2016.

[34] Renee Wynn, NASA CIO, "OCIO Organization," August 2016.

[35] The establishment of a vendor management office was a recommendation made several times in various Forrester studies. The consultants found that IT vendors were playing one Center against another in negotiations and that NASA would not benefit from enterprise-structured agreements with accompanying economies of scale without this office.

Credibility Further Diminished by Continued Struggles with Agency Consolidated End-User Services Contract

Mission Directorates and Centers are reluctant to use enterprise services provided by the OCIO due to a lack of confidence in that office's management of these services. Our survey found these officials do not believe the OCIO has demonstrated the ability to consistently deliver quality IT services and, as a result, efforts by the OCIO to manage services at the enterprise level are met with resistance, further undermining the Agency CIO's authority.

The first recommendation in Forrester's February 2014 study was for the OCIO to build credibility before taking on significantly more responsibilities. In a follow-up study in June 2016, Forrester identified a perception among OCIO senior leaders and Center CIOs that NASA's IT leadership is hesitant to take risks and then stand by the decisions it makes. During our current review, IT managers across NASA consistently pointed to Agency Consolidated End-User Services (ACES), the troubled Agency-wide personal computing contract as a prime example of an enterprise-level IT project that continues to damage the OCIO's credibility.

Agency Consolidated End-User Services

The ACES contract provides the bulk of NASA's personal computing hardware, standard software, mobile IT services, and associated end-user services. Unfortunately, neither the Agency nor the OCIO was prepared for an enterprise-wide IT approach when NASA entered into a $2.5 billion contract with HP Enterprise Services (HP) in 2010.[36] Seven years later, the Agency and service provider are still struggling to successfully manage an enterprise-wide IT delivery model within a historically decentralized IT environment.

The ACES contract demonstrates the tension over enterprise-level IT services between the OCIO, Mission Directorates, and Centers. For example, the MSC tasked the OCIO with consolidating non-ACES workstation administration and support where feasible. While Agency-wide usage of ACES workstations stands at 62 percent, Centers were given a target to obtain at least 80 percent of their desktop, laptop, and workstation computing services through ACES with any deviations from acquiring a non-ACES system requiring a Center CIO-approved waiver. However, due to numerous problems with ACES machines, including thousands of missing software patches, missing back-ups, and problems with encryption, Centers maintain they can obtain lower costs and better security outside the ACES contract. In fact, 2 of NASA's 11 Centers – Ames and Goddard Space Flight Center – currently receive less than half of their workstation needs through the ACES contract while only 5 Centers are above the 80 percent goal.

We described NASA's challenges with ACES in a January 2014 memorandum timed to provide information to Agency leadership who at the time were deciding whether to extend HP's contract for an additional 3 years or seek a new vendor.[37] Our review noted that NASA's lack of adequate preparation prior to deploying ACES coupled with HP's failure to meet important contract objectives resulted in the contract falling short of Agency expectations. We attributed those shortcomings to several factors,

[36] NASA awarded the ACES contract to Hewlett Packard Enterprise Services in 2010. In April 2017, the Enterprise Services business of Hewlett Packard Enterprise merged with Computer Sciences Corporation to form DXC Technology. For ease of reference, we will refer to the contractor as HP in this report.

[37] See IG-14-013. In October 2015, NASA exercised a 3-year option to extend the contract with HP until 2018.

including: (1) a lack of technical and cultural readiness by NASA for an Agency-wide IT delivery model, (2) unclear contract requirements, and (3) the failure of HP to deliver on some of its contract obligations. We also identified specific IT security deficiencies related to inaccurate inventory, untimely patch management, and poor data management as contributing to the contract's shortcomings.

ACES Authority to Operate

In July 2016, the Agency CIO took dramatic action by allowing the authority to operate (ATO) to expire on two crucial ACES systems due to security concerns. The CIO's decision made headlines in the IT trade press with several news agencies describing the move as "unheard of in government" and "a bold move by the CIO."[38] However, as bold as the action may have been, the Agency has had few options apart from continuing to grant HP conditional ATOs to maintain operations (even while characterizing HP's performance as "dismal" and "unacceptable") given the criticality of the systems to NASA's everyday work. Consequently, this outcome has further weakened the OCIO's credibility.

Through issuance of an ATO, OMB requires Federal agencies to certify the soundness of the security controls on their information systems and to formally authorize and accept the risk associated with a system's operation. NASA requires a valid ATO for all unclassified information systems and decides whether to grant ATOs according to a risk-based framework that assesses whether a contractor – in this case HP – has implemented adequate security controls within the Agency's IT environment.

ACES is composed of multiple IT systems, each with a security plan that must be revalidated every 3 years as part of the ATO review process. Other ACES systems have transitioned to a continuous monitoring and ongoing authorization process over the past few years; however, two ACES systems used by thousands of NASA employees daily had not made that transition and therefore their ATOs, previously issued in July 2013, were scheduled for revalidation in 2016.[39] NASA relies on these systems for the following business functions:

- *ACES End-User Devices for End-User Services* system provides computer services – including standard desktop and laptop computers, printers, standard computer software, and mobile devices – that NASA employees and contractors use to support day-to-day Agency operations.
- *ACES Enterprise Tools for End-User Services* system provides support services such as document, asset, and mobile device management; software license management; end-point protection and data encryption; and incident and problem management.

Between April and June 2016, OCIO staff from Headquarters and CIO staff from Marshall assessed both systems and found, overall, they contained the minimum level of security to adequately protect the information processed or stored on them. However, the staff identified several security deficiencies they assessed at a moderate to high risk. The nature of the deficiencies (described below) combined with the fact the majority of the devices had access to external systems and networks, including the internet, resulted in the OCIO's determination the systems presented a significant risk to the Agency.

[38] Federal News Radio, "NASA's Act of Desperation Demonstrates Continued Cyber Deficiencies," August 22, 2016, and CSO, "NASA CIO Allows HPE Contract's Authority to Operate to Expire," August 26, 2016.

[39] The objective of the continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system continues to be effective over time. Continuous monitoring assesses security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation.

The review team identified the following primary deficiencies:

- The organization does not consistently maintain an accurate and updated inventory of information system components.
- No consistency in baseline security settings applied.
- No list of authorized or unauthorized software and no authorized mechanism to prevent detection or execution of unauthorized software. Users are granted elevated privileges and can download or install unauthorized software without prevention.
- Continued operation of devices not properly encrypted.
- Known software vulnerabilities not remediated and patched in accordance with Agency policy.

No longer willing to accept the risks posed by these systems, in July 2016 the Agency CIO allowed the ATOs to expire for both the ACES End-User Devices for End-User Services and ACES Enterprise Tools for End-User Services systems.[40] The CIO directed HP to provide a remediation plan within seven days of the ATO expiration. Four days after expiration, HP presented its plan to NASA management and the next day the Agency CIO issued a conditional ATO that permitted the two systems to operate for 180 days. The CIO pointed to the overarching business need to issue a conditional ATO and accept greater Agency-level risk given the importance of the systems, although OCIO officials admitted they had no contingency plan should HP fail to conform to the terms of the agreement.

Given the issues identified with the diffuse nature of IT security responsibilities throughout the OCIO, we asked the Acting SAISO what role his office and the IT Security Division played in identifying the ACES security deficiencies. The Acting SAISO indicated minimal involvement, stating that responsibility for security of the ACES computers ultimately lies with the system owner, who in this case is the End-User Service Executive in the Agency's End-User Service Office in the OCIO. Security staff in this Office is responsible for validating the accuracy of HP's remedial actions and ensuring deadlines are satisfactorily met. Ultimately, while the Agency SAISO is responsible for IT security across NASA, that office had limited involvement in the HP decertification process.

In the absence of a realistic "Plan B" for managing end-user services at NASA, the CIO has issued multiple conditional ATOs even though the CIO informed HP when it issued the first conditional ATO that "renewals or extensions to this time-bound approval will be granted only under the most extenuating of circumstances."

In late January 2017, the first 180-day conditional ATO expired on both ACES systems with the remedial terms unmet. However, the Agency CIO determined that the communication with and commitment from HP had improved since the first conditional ATO and therefore issued a second. This second ATO was for 90 days and also contained actions and deadlines HP had to meet before its expiration in late April 2017. With no other options available upon its expiration, on April 26, 2017, the Agency CIO issued HP a third conditional 90-day ATO.

[40] While the ATO for these systems expired, NASA end-users were not affected because the systems remained operational.

After a concerted one-year effort involving three conditional ATOs, the Agency CIO signed the ACES ATO on July 5, 2017. Based on the results of her office's security assessment, the CIO determined that actions taken by the ACES contractor reduced the risk to Agency operations, assets, and individuals to an acceptable level. The security assessment identified the systems' on-going weaknesses and made recommendations to mitigate those operational risks. However, we noted numerous security issues that were not fully resolved and multiple tasks that were still "in process." The Agency's mitigation plans, in part, enhance its continuous monitoring efforts to include updating the patch management process and coordinating with the SOC for monitoring support. While the Agency is making progress in addressing some long-standing security issues, it took drastic measures by the CIO to elicit action by the ACES contractor. These ACES security deficiencies continue to challenge the OCIO's credibility.

CONCLUSION

In 2013, we found NASA's IT governance inefficient, ineffective, and overly complex. Four years later, the OCIO has made little progress in rectifying these issues. With the Agency's new governance structure built around necessary but still incomplete actions, recurring issues such as limited oversight, lack of authority, and weak enforcement continue to plague management of the Agency's IT environment. Further, success under the new structure is dependent upon changing the Agency's culture and processes, including more robust cooperation between the OCIO, Mission Directorates, and Centers; full accounting of all Agency IT assets; and a mature Agency enterprise architecture. Each of these represent significant individual challenges but collectively an extremely steep hill for NASA to climb.

The OIG – as well as the GAO and numerous consultants – have consistently identified the lack of strong governance at the root of NASA's significant and ongoing IT security deficiencies. Over the last 7 years, our office has issued more than 30 audit reports containing 119 recommendations designed to improve NASA's IT operations. Our reviews have repeatedly identified poor management processes and inadequate operational and technical controls that affect NASA's ability to protect the information and IT systems vital to its mission. For many of the reasons discussed throughout this report, including high-level staff turnover and cultural resistance, the Agency's actions to date in response to our prior IT governance recommendations have fallen short. Moving forward, NASA needs to redouble its efforts to address these and other challenges to create and sustain a system of IT governance and operation that provides secure and efficient IT systems for Agency employees and contractors.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To increase transparency, accountability, and oversight of NASA's IT investments and strengthen its governance framework, we recommended NASA's Chief Information Officer:

1. Reevaluate and implement necessary changes to the ACIR process, its reporting requirements, and approval thresholds to ensure the Agency CIO gains adequate visibility and authority over all NASA IT assets.

2. Complete the charters for all IT governance boards and educate personnel on their functions.

3. Complete the BSA Implementation Plan steps related to the roles and responsibilities of positions within the Agency's IT structure.

4. Address the Agency's dispersed security responsibilities and long-standing security weaknesses by empowering the SAISO position to include operational responsibilities and address basic IT security practices in the areas of inventory, patching, vulnerability, and configuration management.

5. Implement a mitigation plan to address the skill set and capability issues facing the OCIO to improve its credibility.

We provided a draft of this report to NASA management who concurred or partially concurred with our recommendations and described corrective actions the Agency has taken or will take to address them. The Agency concurred with recommendations 2, 3, and 5. These recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

The Agency partially concurred with recommendations 1 and 4, pointing to its on-going progress in gaining adequate visibility into NASA IT assets through refinements to the ACIR process as well as unifying NASA's cybersecurity program under the SAISO through implementation of the federally mandated CDM program. With respect to recommendation 1, we found the Agency's corrective actions reflect concurrence and meet the intent of our recommendation. Therefore, this recommendation is also resolved and will be closed upon completion and verification of the proposed corrective actions. However, we do not find the Agency's proposed actions to address recommendation 4 responsive. While the CDM program should improve the Agency's visibility over network assets and provide greater insight into security vulnerabilities, successful implementation does not address our concerns about the dispersal of IT security responsibilities which results in the lack of authority and marginalization of the SAISO position. Therefore, recommendation 4 is unresolved pending further discussion with the OCIO. Management's comments are reproduced in Appendix D. Technical comments provided by management have also been incorporated, as appropriate.

Major contributors to this report include Laura Nicolosi, Mission Support Director; Julia Eggert, Project Manager; Jason Hensley; and Megan Paxton. Lauren Suls provided editorial and graphic assistance.

If you have questions about this report or wish to comment on the quality or usefulness of this report, contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or laurence.b.hawkins@nasa.gov.

Paul K. Martin
Inspector General

APPENDIX A: SCOPE AND METHODOLOGY

We performed this audit from April 2016 through September 2017 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 objectives.

To answer our objective and gain an understanding of the Agency's actions to improve IT governance, we interviewed the Agency CIO, Deputy CIO, SAISO, and many IT officials across the OCIO. We also surveyed in writing and interviewed in person the Center CIOs, Center CISOs, and Mission Directorate IT Representatives. We analyzed the Agency's IT BSA Implementation Plan, including the board charters and decision memorandum of the new governance boards. Additionally, we interviewed numerous individuals to gain an understanding of how NASA manages IT assets across the Agency. Finally, we reviewed NASA policy, FITARA requirements and supporting documentation, prior audit reports, external reviews, and various other documents related to IT governance. The documents we reviewed included, but were not limited to, the following:

- OMB Memorandum M-11-29, "Chief Information Officer Authorities," August 8, 2011
- U.S. Chief Information Officer, "25 Point Implementation Plan to Reform Federal Information Technology Management," December 9, 2010
- U.S. Code Title 44, Chapter 35, Subchapter 3506 "Federal Agency Responsibilities"
- Federal Information Technology Acquisition Reform Act, Public Law 113-291, December 19, 2014
- NASA Mission Support Council/Business Services Assessment, "Information Technology Implementation Plan," March 9, 2016
- NASA Policy Directive (NPD) 1000.3E, "The NASA Organization," April 15, 2015
- NPD 1000.0B, "Governance and Strategic Management Handbook," November 26, 2014
- NPD 2800.1B, "Managing Information Technology," March 21, 2008
- NPD 2810.1E, "NASA Information Security Policy," July 14, 2015
- NPD 2830.1A, "NASA Enterprise Architecture," November 2, 2011
- NASA Procedural Requirements (NPR) 2800.1B, "Managing Information Technology" March 20, 2009
- NPR 2810.1A, "Security of Information Technology," May 16, 2006
- NPR 2830.1A, "NASA Enterprise Architecture Procedures," December 19, 2013

Use of Computer-Processed Data

The computer-processed data used in this audit did not materially affect the findings and therefore, we did not test the reliability and validity of the data.

Review of Internal Controls

We reviewed Federal regulations and NASA policies and procedures to determine NASA’s internal controls for ensuring effective IT governance. We analyzed the execution of the policy requirements as it related to the internal control structure surrounding the IT governance boards, budgeting, and spending. The control weaknesses we identified are discussed in the body of this report. Our recommendations, if implemented, should correct the weaknesses identified.

Prior Coverage

During the last 5 years, the NASA OIG and GAO have issued 8 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at https://oig.nasa.gov/audits/reports/FY18/index.html and http://www.gao.gov, respectively.

NASA Office of Inspector General

Security of NASA’s Cloud Computing Services (IG-17-010, February 7, 2017)

Report Mandated by the Cybersecurity Act of 2015 (IG-16-026, July 27, 2016)

Review of NASA’s Information Security Program (IG-16-016, April 14, 2016)

Review of NASA's Agency Consolidated End-User Services Contract (IG-14-013, January 30, 2014)

NASA’s Information Technology Governance (IG-13-015, June 5, 2013)

NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools (IG-13-006, March 18, 2013)

Government Accountability Office

Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority (GAO-16-686, August 2016)

Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings (GAO-14-65, November 2013)

Appendix B: Actions Taken to Close the 2013 IT Governance Report Recommendations

In January 2016, the OIG closed all outstanding recommendations from our 2013 IT governance report. Table 2 outlines the recommendations we made and the associated actions proposed by NASA management.

Table 2: Actions Taken to Close the 2013 IT Governance Report Recommendations

	Recommendation	Management's Response	Date Closed	Agency Action Taken for Closure
1	Consolidate the overall governance of IT within the OCIO to ensure adequate visibility, accountability, and integration into all mission-related IT assets and activities.	Concurred	January 6, 2016	OCIO implemented the ACIR, providing the Agency CIO visibility into all IT investments and assets. The ACIR requires both the CIO and Chief Financial Officer to certify approval of the NASA IT spend submission to OMB. OCIO will conduct Center Functional Reviews and Program Reviews to ensure visibility, involvement, integration, and reporting of NASA's spend on non-highly specialized IT.
2	Require the Agency CIO to approve all IT procurement expenditures over an established threshold. The threshold should capture the majority of IT expenditures regardless of procurement instrument, to give the CIO visibility and authority over all Agency IT assets.	Concurred	December 2, 2015	The Agency CIO and Chief Financial Officer are responsible for the ACIR, which includes all IT spend on institutional and mission IT (including highly specialized), acquisition strategies, and alignment with Agency strategic priorities and enterprise strategies. The ITC is responsible for reviewing the ACIR prior to Agency CIO and Chief Financial Officer certification.
3	Reevaluate the relevancy, composition, and purpose of the existing boards in light of changes made to the Agency's IT governance structure.	Concurred	September 30, 2015	As part of the BSA for IT services, the current IT governing board framework was assessed and a modified IT governance framework was created, including the senior level ITC and elimination of the IT Management Board and Business Systems Management Board.
4	Require the use of governance boards for all major IT decisions and investments, including those made by Mission Directorates.	Concurred	November 30, 2015	Implemented the ACIR for all IT investments, including highly specialized and the requirement of the ITC as the governing board for the ACIR. A draft ITC Charter was attached to this request for closure.
5	Revise the board charters to include all information critical to ensuring the effective use of the boards and develop a plan to educate IT managers and personnel regarding the charters and the requirements and interrelationship of the boards.	Concurred	January 6, 2016	Requested closure of Recommendation 5 based on the actions related to Recommendation 1. The ITC Charter is in final draft because the ITC is scheduling their first meeting in the second quarter of FY16. Publication will occur after the ITC conducts a final review.

6	Make the Agency CIO a direct report and revise the job titles of the Center and Mission Directorate CIOs to delineate roles and responsibilities more clearly.	Partially concurred	December 14, 2015	The Agency CIO is a direct report to the NASA Administrator and NPD 1000.3 was updated to reflect that relationship. The BSA for IT details the roles and responsibilities for the Center CIOs and Mission Directorate participation on the ITC. Specifically, senior leaders in the Mission Directorate organization will support the ACIR and ITC decisions on NASA IT investments. The role of Mission Directorate CIO no longer exists and are now titled Mission Directorate IT Representatives. While not members of the ITC, they participate as members of various focused service boards pertaining to IT services.
7	Make the Mission Directorate CIO position a direct report to the Agency CIO and the principal advocate for the IT needs of their respective Directorates. Define and standardize the roles and responsibilities of the Mission Directorate CIOs to ensure consistency. Mission Directorate CIOs should coordinate with the Agency CIO to ensure that both Agency and Mission needs are considered in the development of Agency-wide IT requirements.	Partially concurred	January 13, 2016	Mission Directorate CIOs are now titled Mission Directorate IT Representatives. The BSA for IT details IT governance and roles and responsibilities for Mission Directorate representation and participation in the IT governance process. All Mission Directorates have senior level representation to the ITC. Mission Directorates are responsible for participating in Center Functional Reviews for non-highly specialized IT. And as a result of the recent FITARA legislation, the OCIO and Office of Procurement are analyzing solutions to ensure the Agency CIO and Mission Directorates collaborate on Mission Directorate procurements, whether for IT or contracts that contain IT.
8	Reevaluate the resources of the OCIO to ensure that the Office has the appropriate number of personnel with the appropriate capabilities and skill sets.	Concurred	November 26, 2014	Since April 2014, the Agency CIO has reassigned or hired new leadership for every OCIO Division, as well as hiring a new Deputy CIO. Additionally, over the past year, 6 of 11 new CIOs across the Agency were hired. These leadership assignments, coupled with continuing evaluations of staff assignments, organizational responsibilities, and individual staff member hiring actions and duties, are all components of this on-going effort.

Source: NASA OIG.

APPENDIX C: INFORMATION TECHNOLOGY DEFINITIONS

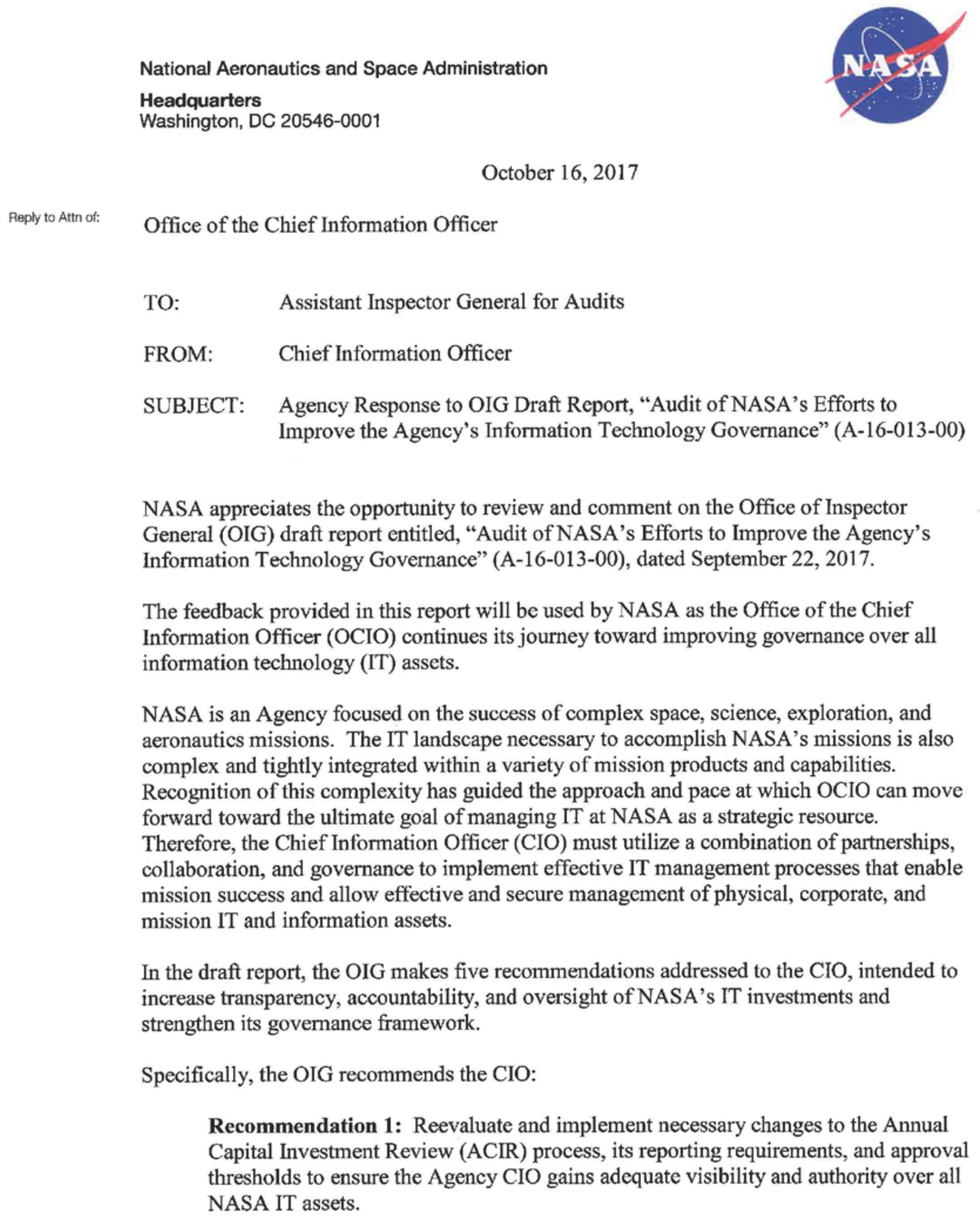
The Portfolio Review Team provided definitions for six Information Technology terms, which are noted in Table 3.

Table 3: Information Technology Terms and Definitions

Information Technology Term	Definition
Information Technology	• Any equipment or system used in the acquisition, storage, retrieval, manipulation, and/or transmission of data or information. This includes computers, ancillary and peripheral equipment, software, and firmware.
Information Technology Service	• A means of delivering IT, in combination with any inherent people or processes, where customers do not assume ownership of overall system costs and risks.
Information Technology Project	• A finite effort where the primary requirements involve developing or significantly modifying systems used in the acquisition, storage, retrieval, manipulation, and/or transmission of data or information. • Projects have defined start and end points, a budget, and specific completion objectives. • IT projects are normally considered part of an IT investment.
Information Technology Investment	• An IT investment is a commitment of funding, personnel, and facility resources to a specific IT project or service. Most IT investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the Investment.
Candidate Major Information Technology Investment	• The Agency Information Technology Council is responsible for designating which IT investments are deemed "major." • An IT investment is considered a candidate to be classified as a Major Investment if it is critical to fulfilling the Agency's mission, supports a critical Agency function, or has development costs greater than $10 million and/or operating costs greater than $10 million annually. • Agency leadership may also classify an IT investment as major if it is a high-visibility investment either internally or externally to the Agency or if there is significant developmental or operational risk associated with the investment.
Highly Specialized Information Technology	• Highly Specialized Information Technology is any equipment, system, and/or software 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. • Highly Specialized Information Technology development, implementation, and operations are managed by the responsible Mission Directorate.

Source: IT Portfolio Review Tiger Team, "Final Report to Information Technology Council," December 2016.

APPENDIX D: MANGAGEMENT'S COMMENTS



National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001

October 16, 2017

Reply to Attn of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Agency Response to OIG Draft Report, "Audit of NASA's Efforts to Improve the Agency's Information Technology Governance" (A-16-013-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "Audit of NASA's Efforts to Improve the Agency's Information Technology Governance" (A-16-013-00), dated September 22, 2017.

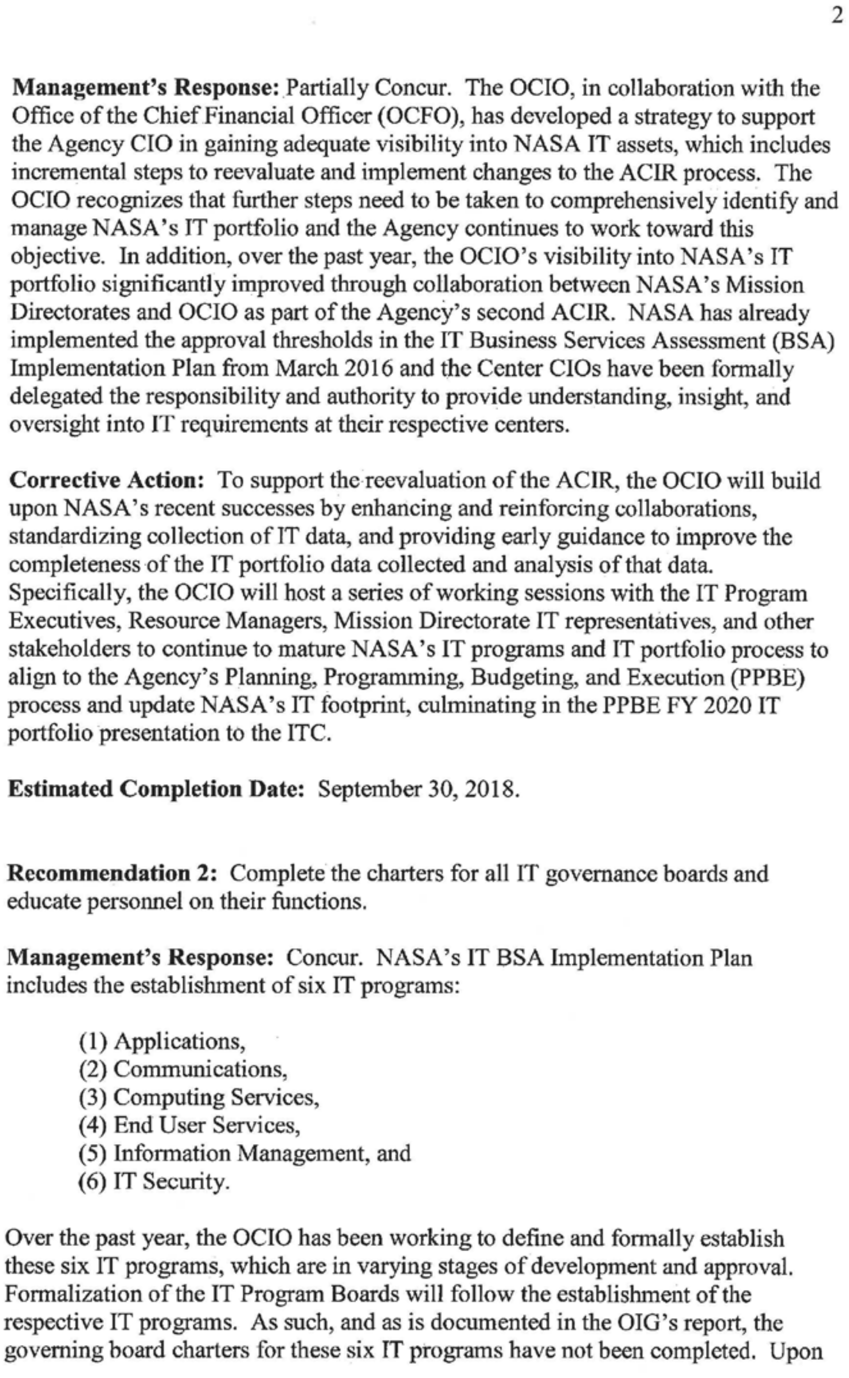
The feedback provided in this report will be used by NASA as the Office of the Chief Information Officer (OCIO) continues its journey toward improving governance over all information technology (IT) assets.

NASA is an Agency focused on the success of complex space, science, exploration, and aeronautics missions. The IT landscape necessary to accomplish NASA's missions is also complex and tightly integrated within a variety of mission products and capabilities. Recognition of this complexity has guided the approach and pace at which OCIO can move forward toward the ultimate goal of managing IT at NASA as a strategic resource. Therefore, the Chief Information Officer (CIO) must utilize a combination of partnerships, collaboration, and governance to implement effective IT management processes that enable mission success and allow effective and secure management of physical, corporate, and mission IT and information assets.

In the draft report, the OIG makes five recommendations addressed to the CIO, intended to increase transparency, accountability, and oversight of NASA's IT investments and strengthen its governance framework.

Specifically, the OIG recommends the CIO:

> **Recommendation 1:** Reevaluate and implement necessary changes to the Annual Capital Investment Review (ACIR) process, its reporting requirements, and approval thresholds to ensure the Agency CIO gains adequate visibility and authority over all NASA IT assets.



Management's Response: Partially Concur. The OCIO, in collaboration with the Office of the Chief Financial Officer (OCFO), has developed a strategy to support the Agency CIO in gaining adequate visibility into NASA IT assets, which includes incremental steps to reevaluate and implement changes to the ACIR process. The OCIO recognizes that further steps need to be taken to comprehensively identify and manage NASA's IT portfolio and the Agency continues to work toward this objective. In addition, over the past year, the OCIO's visibility into NASA's IT portfolio significantly improved through collaboration between NASA's Mission Directorates and OCIO as part of the Agency's second ACIR. NASA has already implemented the approval thresholds in the IT Business Services Assessment (BSA) Implementation Plan from March 2016 and the Center CIOs have been formally delegated the responsibility and authority to provide understanding, insight, and oversight into IT requirements at their respective centers.

Corrective Action: To support the reevaluation of the ACIR, the OCIO will build upon NASA's recent successes by enhancing and reinforcing collaborations, standardizing collection of IT data, and providing early guidance to improve the completeness of the IT portfolio data collected and analysis of that data. Specifically, the OCIO will host a series of working sessions with the IT Program Executives, Resource Managers, Mission Directorate IT representatives, and other stakeholders to continue to mature NASA's IT programs and IT portfolio process to align to the Agency's Planning, Programming, Budgeting, and Execution (PPBE) process and update NASA's IT footprint, culminating in the PPBE FY 2020 IT portfolio presentation to the ITC.

Estimated Completion Date: September 30, 2018.

Recommendation 2: Complete the charters for all IT governance boards and educate personnel on their functions.

Management's Response: Concur. NASA's IT BSA Implementation Plan includes the establishment of six IT programs:

(1) Applications,
(2) Communications,
(3) Computing Services,
(4) End User Services,
(5) Information Management, and
(6) IT Security.

Over the past year, the OCIO has been working to define and formally establish these six IT programs, which are in varying stages of development and approval. Formalization of the IT Program Boards will follow the establishment of the respective IT programs. As such, and as is documented in the OIG's report, the governing board charters for these six IT programs have not been completed. Upon completion of the charters, OCIO will educate its employees on the functions of the boards.

Corrective Action: Complete the Program Board Charters. Educate personnel on governing board functions.

Estimated Completion Date: January 31, 2019.

Recommendation 3: Complete the BSA Implementation Plan steps related to the roles and responsibilities of positions within the Agency's IT structure.

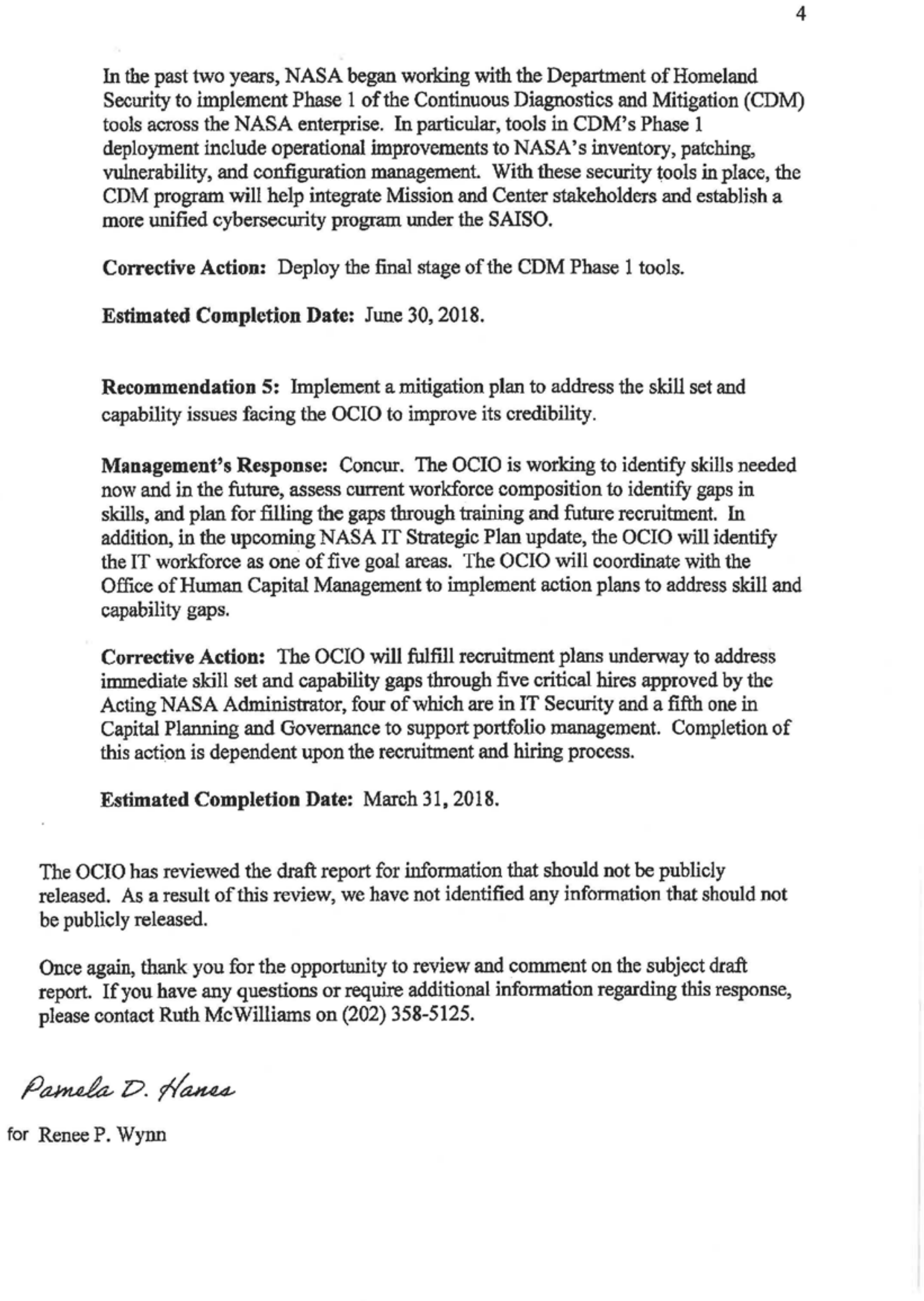
Management's Response: Concur. NASA's IT BSA Implementation Plan includes 24 separate decisions, approved by the NASA Mission Support Council, many of which have been successfully completed. Finalizing the roles and responsibilities remains at the top of OCIO's priority list. In fact, in August 2017, an OCIO leadership retreat determined that completion of this activity is a high priority and a focus area for FY 2018.

Corrective Action: Finalize roles and responsibilities within the Agency's IT structure.

Estimated Completion Date: March 31, 2018.

Recommendation 4: Address the Agency's dispersed security responsibilities and long standing security weaknesses by empowering the Senior Agency Information Security Officer (SAISO) position to include operational responsibilities and address basic IT security practices in the areas of inventory, patching, vulnerability, and configuration management.

Management's Response: Partially concur. The OCIO disagrees that dispersed responsibilities implicitly weaken the SAISO position. Rather, NASA IT security roles exist and operate in a federated manner across Mission Directorates and Centers, with the Center Chief Information Security Officer (CISO) being the responsible authority to oversee these responsibilities and to communicate directly with the SAISO. The SAISO's role and responsibilities are clearly defined in NASA Policy Directive 2810.1E in accordance with responsibilities defined in the Federal Information Security Modernization Act (FISMA) and relevant guidance from the National Institute of Standards and Technology. The SAISO has full authority over NASA's cybersecurity and reports to the Agency CIO.



In the past two years, NASA began working with the Department of Homeland Security to implement Phase 1 of the Continuous Diagnostics and Mitigation (CDM) tools across the NASA enterprise. In particular, tools in CDM's Phase 1 deployment include operational improvements to NASA's inventory, patching, vulnerability, and configuration management. With these security tools in place, the CDM program will help integrate Mission and Center stakeholders and establish a more unified cybersecurity program under the SAISO.

Corrective Action: Deploy the final stage of the CDM Phase 1 tools.

Estimated Completion Date: June 30, 2018.

Recommendation 5: Implement a mitigation plan to address the skill set and capability issues facing the OCIO to improve its credibility.

Management's Response: Concur. The OCIO is working to identify skills needed now and in the future, assess current workforce composition to identify gaps in skills, and plan for filling the gaps through training and future recruitment. In addition, in the upcoming NASA IT Strategic Plan update, the OCIO will identify the IT workforce as one of five goal areas. The OCIO will coordinate with the Office of Human Capital Management to implement action plans to address skill and capability gaps.

Corrective Action: The OCIO will fulfill recruitment plans underway to address immediate skill set and capability gaps through five critical hires approved by the Acting NASA Administrator, four of which are in IT Security and a fifth one in Capital Planning and Governance to support portfolio management. Completion of this action is dependent upon the recruitment and hiring process.

Estimated Completion Date: March 31, 2018.

The OCIO has reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Ruth McWilliams on (202) 358-5125.

Pamela D. Hanes

for Renee P. Wynn

APPENDIX E: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Acting Administrator
Acting Deputy Administrator
Associate Administrator
Associate Administrator for Strategy and Plans
White House Liaison
Executive Officer
General Counsel
Chief Information Officer
Chief Financial Officer
Associate Administrator for Aeronautics Research
Associate Administrator for Science
Associate Administrator for Human Exploration and Operations
Associate Administrator for Space Technology
Acting Associate Administrator for Mission Support

Non-NASA Organizations and Individuals

Office of Management and Budget
  Deputy Associate Director, Energy and Space Programs Division

Government Accountability Office
  Managing Director, Office of Financial Management and Assurance
  Director, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
  Subcommittee on Commerce, Justice, Science, and Related Agencies

Senate Committee on Commerce, Science, and Transportation
  Subcommittee on Space, Science, and Competitiveness

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Appropriations
  Subcommittee on Commerce, Justice, Science, and Related Agencies

House Committee on Oversight and Government Reform
  Subcommittee on Government Operations

House Committee on Science, Space, and Technology
  Subcommittee on Oversight
  Subcommittee on Space

(Assignment No. A-16-013-00)