June 5, 2013

Audit Report

Office of Audits

NASA's Information Technology Governance

Office of Inspector General

National Aeronautics and
Space Administration

Report No. IG-13-015 (Assignment No. A-12-018-00)

Final report released by:

Paul K. Martin
Inspector General

Acronyms

BSMB	Business System Management Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ECAB	Enterprise Change Advisory Board
FY	Fiscal Year
GAO	Government Accountability Office
IT	Information Technology
ITMB	Information Technology Management Board
IT PMB	Information Technology Program Management Board
ITSAB	Information Technology Security Advisory Board
I3P	Agency IT Infrastructure Integration Program
MSC	Mission Support Council
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
SOC	Security Operations Center
USPS	United States Postal Service
VA	Department of Veterans Affairs

OVERVIEW

NASA'S INFORMATION TECHNOLOGY GOVERNANCE

The Issue

Information technology (IT) plays an integral role in every facet of NASA's space, science, and aeronautics operations. The Agency spends more than $1.5 billion annually on a portfolio of IT assets that includes approximately 550 information systems it uses to control spacecraft, collect and process scientific data, provide security for its IT infrastructure, and enable NASA personnel to collaborate with colleagues around the world. Hundreds of thousands of individuals, including NASA personnel, contractors, members of academia, and the public, rely on these IT systems daily.

IT governance is a process for designing, procuring, and protecting IT resources. Because IT is intrinsic and pervasive throughout NASA, the Agency's IT governance structure directly affects its ability to attain its strategic goals. For this reason, effective IT governance must balance compliance, cost, risk, security, and mission success to meet the needs of internal and external stakeholders.

In 2011, the Office of Management and Budget (OMB) issued a memorandum shifting the primary responsibilities of Federal Chief Information Officers (CIO) from policymaking and infrastructure maintenance to IT portfolio management.[1] The memorandum mandated that Federal agencies equip their CIOs with authority over IT governance, commodity IT, program management, and information security.[2]

For over 2 decades, NASA has struggled to implement an effective IT governance approach that appropriately aligns authority and responsibility commensurate with the Agency's overall mission. Since at least 1990, the Government Accountability Office (GAO) and NASA's Office of Inspector General (OIG) have highlighted a series of challenges stemming from the limited authority of the Agency CIO, decentralization of Agency IT operations, ineffective IT governance, and shortcomings in the Agency's IT security.[3] Reports by GAO and OIG have noted that NASA has limited Agency-level oversight of its wide-ranging IT operations, and recently, the OIG reported that the

[1] Office of Management and Budget "Chief Information Officer Authorities," M-11-29, August 8, 2011.

[2] Commodity IT includes hardware, software, and technology services such as data centers, IT infrastructure, and mobile devices.

[3] GAO, "Administrative Systems: NASA Should Reassess Its AIM Program and Rescind Its IBM-Compatible Policy" (GAO/IMTEC-90-41, May 1, 1990). GAO, "NASA Chief Information Officer: Opportunities to Strengthen Information Resources Management" (GAO/AIMD-96-78, August 15, 1996). NASA OIG, "Final Memorandum on Review of Organization Structure and Management of Information Technology and Information Technology Security Services at NASA" (IG-05-013, March 30, 2005).

NASA CIO could not fully account for the Agency's IT assets or ensure those assets complied with applicable IT security policies and procedures.[4]

We initiated this audit to examine whether NASA's current IT governance structure appropriately aligns authority and responsibility to support the overall mission of the Agency. Specifically, we reviewed whether NASA's Office of the Chief Information Officer (OCIO) has the organizational, budgetary, and regulatory framework needed to effectively meet the Agency's varied missions.

Results

The decentralized nature of NASA's operations and its longstanding culture of autonomy hinder the Agency's ability to implement effective IT governance. The Agency CIO has limited visibility and control over a majority of the Agency's IT investments, operates in an organizational structure that marginalizes the authority of the position, and cannot enforce security measures across NASA's computer networks. Moreover, the current IT governance structure is overly complex and does not function effectively. As a result, Agency managers tend to rely on informal relationships rather than formalized business processes when making IT-related decisions. While other Federal agencies are moving toward a centralized IT structure under which a senior manager has ultimate decision authority over IT budgets and resources, NASA continues to operate under a decentralized model that relegates decision making about critical IT issues to numerous individuals across the Agency, leaving such decisions outside the purview of the NASA CIO. As a result, NASA's current IT governance model weakens accountability and does not ensure that IT assets across the Agency are cost effective and secure.

Limited CIO Control of IT Funding and Investments. We found that the Agency CIO had little control and visibility over the majority of NASA's IT budget. Of the $1.46 billion allocated for IT in fiscal year (FY) 2012, the Agency CIO had direct control of $159 million or 11 percent, the Centers had direct control of $393 million or 27 percent, and the Mission Directorates controlled the remaining $912 million or 62 percent.[5] An anecdote recounted to us during our review illustrates the CIO's limited visibility and control of NASA's overall IT spending. According to the Agency CIO, although planned IT expenditures for FY 2010 were $1.6 billion, the Agency actually spent $2 billion. However, the CIO was unaware of the $400 million in additional spending until the Mission Directorates reported actual expenditures to her office in a data call responding to an OMB request. We also determined that the Agency CIO's lack of authority over IT funding limits the Agency's ability to consolidate IT expenditures to

[4] NASA Inspector General, testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, February 29, 2012.

[5] NASA has four Mission Directorates – Aeronautics Research, Human Exploration and Operations, Science, and Space Technology – responsible for carrying out the Agency's core programmatic mission. Approximately 12 percent of this funding pays for the Mission Directorates' institutional IT spending for items such as laptops, email, and printers.

realize cost savings and drive improvements in the delivery of IT services. With decreased budgets across the Federal Government and the reduction of NASA's IT budget by almost $1 billion since 2006, it is imperative that NASA find efficiencies in its IT operations, purchases, and investments.

Organizational Structure Marginalizes the Agency CIO. We found that NASA's organizational structure marginalizes the position and authority of the CIO. When NASA established the CIO position in 1995, it purposely limited the authority of the position to preserve control by the Mission Directorates and Centers over the IT assets related to their space, science, and aeronautics programs. Despite technological advances over the intervening 17 years and integration of IT into all Agency programs, the role of the NASA CIO has changed very little. Each Mission Directorate and each NASA Center continues to employ their own CIO and IT security personnel who oversee hundreds of independently operated networks and tens of thousands of computers and other IT hardware over which the Agency CIO has little control or oversight. Moreover, although the Center CIOs report to the Agency CIO, the Mission Directorate CIOs do not. We found that this partitioning of authority and control has not served the Agency well in terms of securing its IT systems or achieving economies and efficiencies in IT acquisitions and management.

NASA employs 1 CIO at the Agency level, 10 CIOs at the Center level, 1 CIO at the Jet Propulsion Laboratory, 1 CIO at the NASA Shared Services Center, and 1 CIO within each of the Mission Directorates.[6] Having numerous officials with the same title and similar roles as the Agency CIO, some of whom do not report to the CIO, dilutes the CIO's authority and blurs the lines of accountability and responsibility for overseeing NASA's IT systems. Moreover, the Agency CIO is the only one of seven "Chief" positions at NASA that does not report directly to the Agency Administrator, a reporting structure that is out of line with Federal policy and best practices.[7] In our judgment, affording the Agency CIO the same visibility as the other "Chiefs" would send a message about the significance of IT and better ensure that NASA's IT posture aligns with the strategic direction of the Agency.

The issues currently challenging the NASA CIO are not new and we and others have raised them repeatedly since NASA established the position almost 2 decades ago. While recognizing the problem, the OCIO has often advocated solutions that rely on "improved collaboration" between the OCIO, the Centers, and the Mission Directorates.[8] While coordination and collaboration are important components of any IT strategy, we do not believe they alone will be sufficient to overcome the significant and longstanding issues

[6] The NASA Shared Services Center is a partnership between NASA and a contractor that consolidates certain support functions such as financial management, human resources, IT, and procurement.

[7] The Chief Financial Officer, Chief Scientist, Chief Technologist, Chief Engineer, Chief Safety and Mission Assurance, and Chief Health and Medical Officer all report to the Administrator. See 44 USC Chapter 35, Coordination of Federal Information Policy.

[8] NASA Draft Report "Implementation of Administrative Remedy Regarding Cyber Security" pursuant to H.R. 112-169 accompanying H.R. 2596.

we and others have identified. NASA's diffuse responsibility for IT matters prevents the Agency CIO from taking and enforcing meaningful actions and instead, often reduces the position to issuing calls for increasing "cooperation and communication" – calls that at least up to this point largely have gone unanswered. In short, NASA's culture and current structure hinders the CIO's ability to implement and enforce new IT initiatives across the Agency.

Responsibilities and Interaction between IT Boards Unclear. In addition to the various layers of CIOs and associated IT personnel, NASA's IT governance structure includes three primary governance boards that report to the Mission Support Council (MSC) as well as numerous sub-boards and working groups.[9] We found that the complexity of the board structure and a lack of documentation and training to explain the interrelationship of the boards has led to confusion among Agency IT personnel about the roles and responsibilities of the boards and diminished their value to the governance process. While the design of NASA's IT governance structure requires coordination and collaboration between the boards, in practice, IT managers are often unsure of the interrelation and function of the various boards and how decisions are intended to be made. Even though Mission Directorates are not required to utilize the boards for Mission specific IT decisions, the Mission Directorate CIOs cited time constraints, impact on Mission security, and potential non-approval by the Agency CIO as reasons to circumvent the board process. Moreover, NASA policy, including the charters for each of the boards, does not provide clear guidance or criteria for determining the issues or initiatives that must go before the boards for approval. As a result, NASA IT managers tend to rely on informal relationships rather than formalized business processes when making IT decisions.

CIO Cannot Enforce Security Measures over a Majority of NASA IT Assets. Over the past several years, our audits 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. Although the Agency CIO is responsible for developing IT security policies and procedures and implementing an Agency-wide IT security program, because the CIO lacks authority and control over Mission networks, the CIO is unable to enforce the implementation of IT security programs on a large portion of NASA's IT assets.

In 2012 Congressional testimony, the CIO acknowledged that the Agency's culture does not support building effective cyber security processes, and stated that the largest impediment to effective IT security is persuading and changing the Mission Directorate culture.[10] Mission Directorates often fund their own computer networks and Directorate personnel are responsible for IT security, risk determination, and risk acceptance on those networks, limiting the ability of the Agency CIO to standardize those assets across the

[9] The Mission Support Council is the Agency's senior decision-making body regarding the integrated Agency mission support portfolio, inclusive of IT.

[10] NASA CIO, testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, February 29, 2012.

Agency or ensure they adhere to security policies. Further, the OCIO's internal continuous monitoring function, the Security Operations Center (SOC), does not have purview over all of NASA's networks. According to the NASA IT Security Operations Manager, the SOC currently has visibility over approximately 90 percent of NASA's institutional networks but only over a very small portion of the Agency's Mission networks. As a result, the SOC relies on the Mission Directorates to self-report vulnerabilities and security incidents.

NASA's ability to secure its networks is further complicated because the Agency lacks a complete inventory of IT assets. For example, five Center CIOs told us they could not account for 100 percent of the IT systems and hardware at their Centers. Center Chief Information Security Officers (CISO) told us that the Agency's efforts to establish an inventory have been hindered by inconsistent enforcement of the policies and implementation of the tools meant to capture the information, pockets of resistance to providing the information, and inconsistent or lack of guidance from OCIO IT security management.

IT Governance across Government. Although NASA's mission is unique, the challenges the Agency faces in managing a decentralized IT environment are not. As part of this review, we benchmarked with IT officials at the Department of Interior, the Department of Veterans Affairs, and the United States Postal Service. Each of these organizations had a decentralized IT environment that was geographically diverse, independently operated, and that supported thousands of users. With support from Congress and agency leaders, each organization revamped their IT governance model and moved from decentralized IT systems to a more consolidated, centralized structure giving the CIO authority over IT budgets and resources agency-wide. Officials from each of these organizations reported that centralization – while time consuming and not without its detractors – has resulted in increased efficiency, security, and lower operating costs for their agencies.

Management Action

For almost 2 decades, the OIG and GAO have reported issues associated with NASA's limited CIO authority, decentralized IT operations, and ineffective IT governance. Although division of authority between Headquarters management, the Mission Directorates, and the Centers is historically the cornerstone of NASA's program and project governance, in our view mirroring this structure for managing IT purchases, operations, and security is no longer in the Agency's best interest. With mission critical assets at stake and shrinking budgets, NASA must take a holistic approach to managing its portfolio of IT systems.

To overcome the barriers that have resulted in the inefficient and ineffective management of the Agency's IT assets and operations, we recommend that NASA overhaul its IT governance structure to centralize IT functions and establish the Agency CIO as the top management official responsible for NASA's entire IT portfolio. Strong leadership by the CIO and OCIO staff will be required, but the CIO cannot make these changes alone. Rather, the NASA Administrator – backed by support and possibly additional resources from Congress – must be the driving force behind such organizational change. With the recent departure of the Agency CIO, NASA currently has a prime opportunity to reevaluate its IT organizational structure and personnel resources to ensure it is best positioned to meet its IT challenges.

Therefore, we recommend the NASA Administrator – in consultation with the Mission Directorate and Center CIOs and the Agency's senior management team – consolidate the overall governance of IT within the OCIO and ensure the OCIO has adequate visibility into Mission-related IT assets and activities. The Agency CIO should approve all IT procurements over an established monetary threshold that captures the majority of IT expenditures, regardless of procurement instrument. Additionally, the Administrator should make the Agency CIO a direct report and revise the job titles of the Center and Mission Directorate CIOs to more clearly delineate roles and responsibilities. Further, the renamed Mission Directorate CIO positions should directly report to the Agency CIO. We also recommend that the Administrator reevaluate the relevancy, composition, and purpose of the three primary governance boards in light of the changes made to the IT governance structure and require the use of reconstituted governance boards for all major IT decisions and investments. Further, we recommend revision of the board charters to include all information critical to ensuring the effective use of the boards and development of a plan to educate IT managers and personnel regarding the roles and responsibilities of the boards. Finally, in light of the changes recommended in this report, the NASA Administrator should reevaluate the resources of the OCIO to ensure that the Office has the appropriate number of personnel with the appropriate capabilities and skill sets.

In response to a draft of this report, NASA's Administrator concurred or partially concurred with our recommendations and proposed corrective actions to improve NASA's IT governance. We consider the Administrator's planned actions responsive and will close the recommendations upon verification that the Agency has completed them.

Management's response is reprinted in Appendix B.

CONTENTS

INTRODUCTION

RESULTS

APPENDIX A

APPENDIX B

APPENDIX C

INTRODUCTION

Background

Information technology (IT) plays an integral role in every facet of NASA's space, science, and aeronautics operations. The Agency spends more than $1.5 billion annually on a portfolio of IT assets that includes approximately 550 information systems with 140,000 components it uses to control spacecraft, collect and process scientific data, provide security for its IT infrastructure, and enable NASA personnel to collaborate with colleagues around the world. One of NASA's most valuable assets is the technical and scientific information generated by its research, science, engineering, technology, and exploration initiatives. The Agency relies on computer networks and systems to collect, access, and process this information, including mission-critical, proprietary, or otherwise sensitive data.

In the broadest sense, governance refers to the rules, processes, and laws pursuant to which an organization operates and is regulated and controlled. In the IT context, governance is the process that seeks to ensure the effective and efficient use of IT resources and provides the structure for integration of those resources across an 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.

Federal Information Technology Policy. The Clinger-Cohen Act of 1996 makes Federal agency Chief Information Officers (CIO) 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.[11] In 2010, the Federal CIO released a "25-Point Plan" for IT reform across the Federal Government that outlined a series of initiatives to improve the management of IT assets and reform the execution, oversight, and transparency of Federal IT operations.[12] One initiative focuses on streamlining IT governance and improving accountability for IT portfolios by (1) redefining the role of Agency CIO; (2) reforming and strengthening review boards that analyze potential IT investments; and (3) implementing face-to-face, evidence-based reviews of agency IT programs.

[11] Public Law 104–106 (1996), codified at 40 U.S.C. 1425.

[12] U.S. Chief Information Officer, 25 Point Implementation Plan to Reform Federal Information Technology Management, December 9, 2010.

In 2011, the Office of Management and Budget (OMB) followed up the 25-Point Plan with a memorandum that shifts the primary responsibilities of Federal CIOs from policymaking and infrastructure maintenance to portfolio management.[13] Specifically, OMB mandated that Federal agencies give their CIOs authority for IT governance, commodity IT, program management, and information security.[14] In addition, OMB instructed CIOs to lead the review process for Agency IT investments, justify those investments, and eliminate duplication. According to OMB, agencies should position their CIOs so they have authority and primary responsibility for implementing an agency-wide program that provides security for both the information collected and maintained by the agency and the information systems that support the agency's operations, assets, and mission. Furthermore, agency CIOs are to improve the overall management of large Federal IT projects by identifying, recruiting, and hiring top IT program management talent.

NASA's IT Organizational Structure. NASA consists of a Headquarters Office in Washington, DC; 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.[15] Historically, NASA has operated as a decentralized organization based on the philosophy that its Centers and project managers should be given as much freedom and 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, program or project management, and Center management.

Agency management, including the Administrator and Deputy Administrator, is located primarily at NASA Headquarters and responsible for providing NASA's strategic direction, top-level requirements, schedules, and budgets. Also part of 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 CIO. All of the chief positions except the CIO report directly to the Administrator while the CIO reports to the Deputy Administrator.

NASA has four Mission Directorates, each led by an Associate Administrator: Aeronautics Research, Human Exploration and Operations, Science, and Space Technology.[16] The Associate Administrators, who also are located at NASA Headquarters, are responsible for managing their Directorate's portfolio of programs and

[13] Office of Management and Budget, "Chief Information Officer Authorities" M-11-29, August 8, 2011.

[14] Commodity IT includes hardware, software, and technology services such as data centers, IT infrastructure, mobile devices, and security.

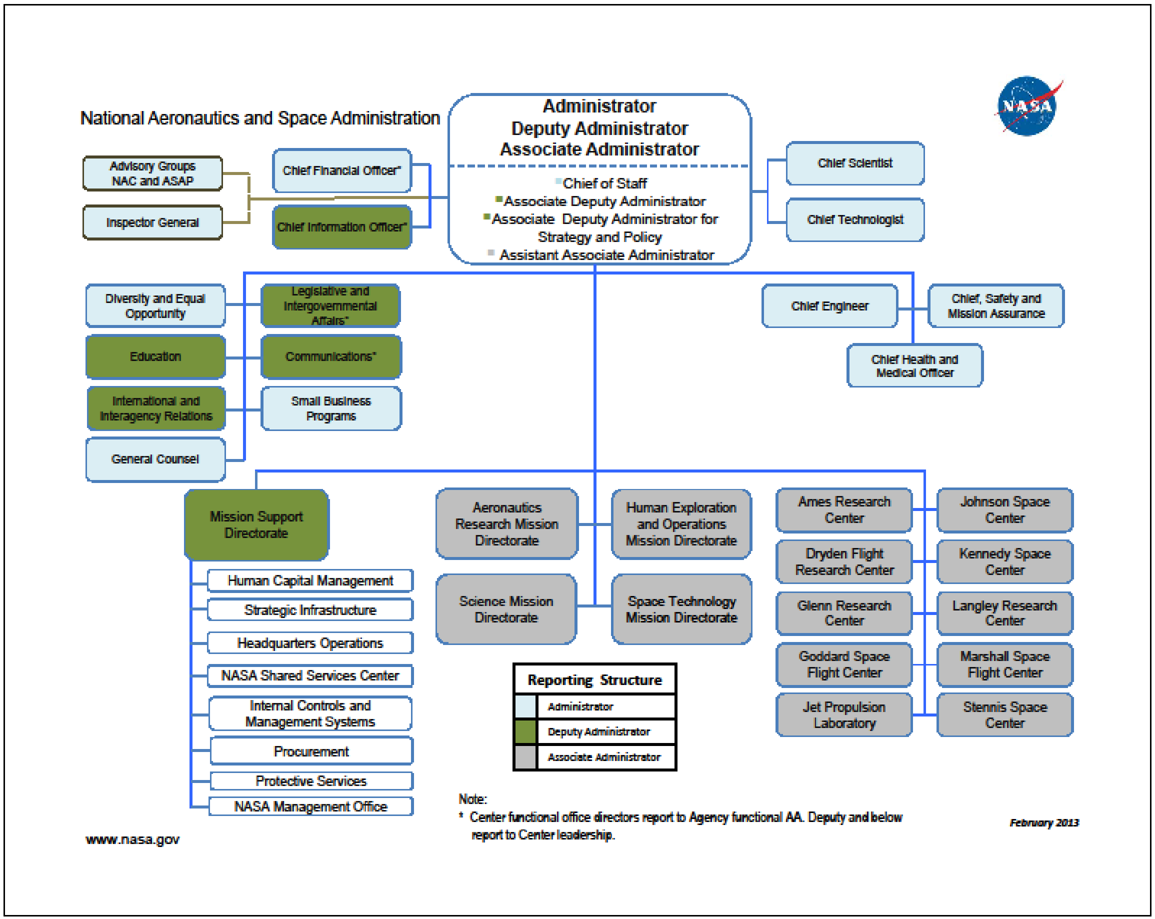
[15] NASA also has six supporting facilities and the NASA Shared Services Center, a partnership between NASA and a contractor to consolidate certain support functions such as financial management, human resources, IT, and procurement.

[16] The NASA Administrator reorganized existing personnel and infrastructure to create the Space Technology Mission Directorate in February 2013.

projects and have ultimate responsibility for their projects' mission success. Much of the work associated with Mission Directorate projects and programs, such as the new heavy lift rocket known as the Space Launch System, occurs at the NASA Centers.

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 the Center Directors to provide and oversee the human and facility resources needed to execute Directorate programs and projects. 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. The Mission Directorate Associate Administrators and the Center Directors report to NASA's Associate Administrator, the most senior civil servant at the Agency. Figure 1 depicts NASA's organizational structure.

Figure 1. NASA's Organizational Structure

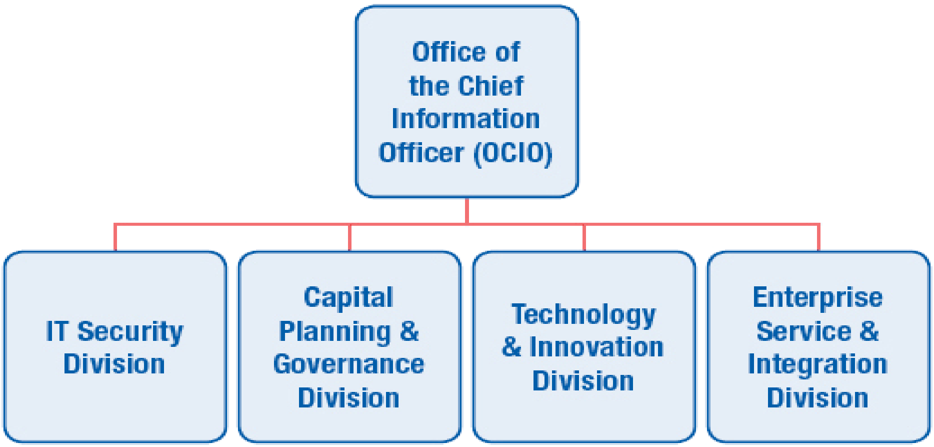

National Aeronautics and Space Administration
Administrator
Deputy Administrator
Associate Administrator
Chief of Staff
Associate Deputy Administrator
Associate Deputy Administrator for Strategy and Policy
Assistant Associate Administrator
Advisory Groups NAC and ASAP
Inspector General
Chief Financial Officer*
Chief Information Officer*
Chief Scientist
Chief Technologist
Diversity and Equal Opportunity
Legislative and Intergovernmental Affairs*
Education
Communications*
International and Interagency Relations
Small Business Programs
General Counsel
Chief Engineer
Chief, Safety and Mission Assurance
Chief Health and Medical Officer
Mission Support Directorate
Human Capital Management
Strategic Infrastructure
Headquarters Operations
NASA Shared Services Center
Internal Controls and Management Systems
Procurement
Protective Services
NASA Management Office
Aeronautics Research Mission Directorate
Human Exploration and Operations Mission Directorate
Science Mission Directorate
Space Technology Mission Directorate
Ames Research Center
Dryden Flight Research Center
Glenn Research Center
Goddard Space Flight Center
Jet Propulsion Laboratory
Johnson Space Center
Kennedy Space Center
Langley Research Center
Marshall Space Flight Center
Stennis Space Center
Reporting Structure
Administrator
Deputy Administrator
Associate Administrator
Note:
* Center functional office directors report to Agency functional AA. Deputy and below report to Center leadership.
www.nasa.gov
February 2013

Source: NASA.

In many ways, NASA's IT infrastructure mirrors its overall organizational structure. Authority for developing IT policies and implementing an Agency-wide IT program lies with the Headquarters-based Agency CIO and staff of the Office of the Chief Information Officer (OCIO).[17] The Agency CIO is responsible for providing leadership, planning, policy direction, and oversight of the management of NASA information and IT resources Agency-wide. The Agency CIO serves as the principal advisor to the Administrator and other senior officials on matters pertaining to IT and is responsible for ensuring that NASA acquires and manages its information assets in accordance with Federal policies, procedures, and legislation. The Headquarters OCIO is comprised of 86 positions – 52 civil servants and 34 contractor staff.

As shown in Figure 2, the OCIO 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 resource management policies, evaluates related practices, and determines compliance; (3) Technology and Innovation, which guides NASA's IT strategy and investment decisions, identifies emerging IT technologies, and addresses issues such as technology infusion, procurement, and future IT workforce development; 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 2: OCIO Structure


Office of the Chief Information Officer (OCIO)
IT Security Division
Capital Planning & Governance Division
Technology & Innovation Division
Enterprise Service & Integration Division

Source: NASA.

NASA's IT assets generally fall into two broad categories: institutional and Mission. The 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. The Mission

[17] NASA Policy Directive (NPD) 1000.3D, "The NASA Organization," December 3, 2008.

systems support the Agency's aeronautics, science, and space exploration programs and host IT systems that control spacecraft, collect and process scientific data, and perform other critical Agency functions. For example, the Human Exploration and Operations Mission Directorate operates the Deep Space Network, which provides critical communications and tracking for multiple spacecraft.

The Mission Directorates fund the IT assets on NASA's Mission networks. Moreover, funding for the IT investments associated with many NASA programs and projects is embedded in the funding for the underlying mission. In fiscal year (FY) 2012, NASA spent 38 percent of its IT budget on institutional assets directly controlled by the OCIO or NASA Centers and the remaining 62 percent on assets controlled by the Mission Directorates.[18]

Under NASA's current governance structure, the Agency CIO has little visibility into the Agency's Mission IT assets. Each Mission Directorate employs a CIO and IT security personnel who report through the Directorate's management chain rather than to the Agency CIO. The Mission Directorate CIO and IT personnel are responsible for security, risk determination, and risk acceptance for the Mission networks and associated IT assets. This organizational structure provides the Agency CIO with limited insight and control over the security of NASA's Mission IT assets.

Each NASA Center also employs a CIO and IT staff. For many years, Center CIOs reported to their respective Center Directors. In 2010, NASA revised this management structure and the Center CIOs now report to the Agency CIO.[19] The Agency CIO has delegated to the Center CIOs the responsibility, authority, and accountability for the Centers' IT portfolios. Center CIOs are responsible for ensuring that Center IT activities align with Federal and Agency requirements and for supporting the Agency CIO's review of Center IT investments. The Center CIOs receive their funding through each Center's budget, not through the OCIO.

NASA's IT Governance. NASA appointed its first Agency CIO in February 1995. Although NASA empowered the CIO to establish Agency-wide IT policy, it limited the authority of the position to enforce those policies. For example, as originally designed the CIO did not control any part of the Agency's IT budget. NASA's position at the time was that budget authority was not necessary to ensure that Agency personnel followed CIO guidance.

NASA also designed its CIO function to ensure that the CIO would not take part in individual program decisions or have responsibility for setting priorities, making trade-offs, or forming investment decisions relating to Agency-wide IT systems and

[18] Approximately 12 percent of this funding pays for the Mission Directorates institutional expenses.

[19] This reorganization mirrors management centralization efforts NASA made in other departments, including the Office of the Chief Financial Officer.

programs.[20] NASA's position was that the CIO would not be familiar with detailed program requirements and the Agency structured the position so that program offices and Centers would continue to independently manage their IT budgets and implement the systems needed to support their programs. Because of these restrictions, the CIO's responsibility was essentially limited to formulating high-level policy and managing cooperative initiatives to achieve efficiencies across administrative and crosscutting IT issues. Despite technological advances over the intervening 17 years and integration of IT into all Agency programs and projects, the role of the NASA CIO has changed very little and the Agency's IT governance structure continues to rest in large part on cooperation and coordination between three sets of CIO organizations.

In addition to the CIOs, various boards and councils play a role in NASA's IT governance structure. The three primary boards for IT-related issues are the IT Management Board, the Business Systems Management Board, and the IT Program Management Board.

- The IT Management Board (ITMB) consists of the Agency CIO, the Deputy and Associate CIOs, the Center CIOs, and the Mission Directorate CIOs and makes decisions regarding the Agency's IT infrastructure strategy, operations, and budget. The ITMB is a forum for oversight and evaluation of Agency IT operations and maintenance and for reviewing and approving high-level requirements of critical infrastructure initiatives. For example, the ITMB oversees NASA's IT infrastructure and IT security budgets and makes recommendations relating to projects and investments such as the Security Operation Center (SOC) and penetration testing.[21] The NASA CIO serves as the decision authority for the ITMB.

- The Business Systems Management Board (BSMB) includes representatives from the Mission Support Directorate; the Mission Directorates; the Centers; the ITMB; and the Offices of the Chief Financial Officer, CIO, and Chief Engineer. The BSMB oversees and makes decisions regarding strategy, operational performance, and budget priorities pertaining to the Agency's enterprise business systems. For example, decisions about travel management systems or electronic forms would go before the BSMB. The Deputy Associate Administrator for the Mission Support Directorate, and the Deputy Chief Financial Officer are co-chairs and serve as the decision authority for the BSMB.

- The IT Program Management Board (IT PMB) is chaired by either the NASA Deputy CIO or a Center CIO (as designated by the Agency CIO) and includes other OCIO employees and representatives from the Centers, Mission

[20] GAO, "NASA Chief Information Officer: Opportunities to Strengthen Information Resources Management" (GAO/AIMD-96-78, August 1996).

[21] The SOC provides centralized, continuous monitoring of computer network traffic entering and leaving NASA Centers and includes an information system (the Incident Management System) for Agency-wide coordination, tracking, and reporting of IT security incidents.

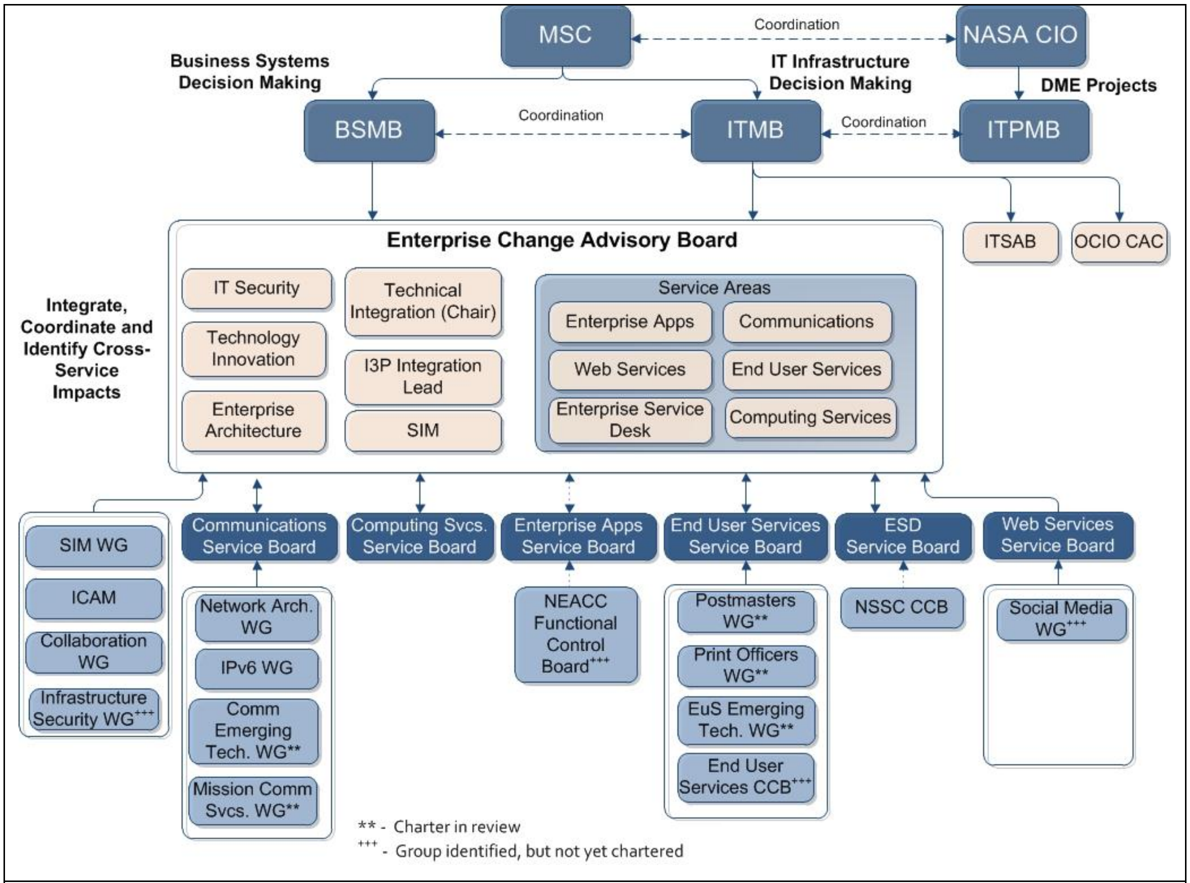
> Directorates, Office of the Chief Engineer, and the ITMB. The IT PMB oversees application and infrastructure projects during development and implementation and conducts key decision point reviews to ensure that projects meet cost, schedule, and scope commitments. All major IT development projects, such as the recent project to consolidate networks to the corporate network operations center, report to the IT PMB. The IT PMB makes recommendations to the Agency CIO, who is the decision authority for Agency infrastructure investments.

All three boards report to the Mission Support Council (MSC), NASA's senior decision-making body for all aspects of the Agency's mission support portfolio, including IT.[22] The MSC serves as the highest level IT governing body and approves large IT investments, divestments, and strategy.

In addition to the primary boards, the NASA OCIO established the Enterprise Change Advisory Board (ECAB) as well as numerous sub-boards and working groups to review specialized technical issues such as social media and emerging technologies. According to its charter, the ECAB is responsible for reviewing proposed changes that have impacts on more than one IT service area with enterprise-wide consequences. The ECAB membership consists of executives from other boards, such as the End User Services Board, and representatives from the OCIO and the Centers. The ECAB reports to the ITMB for IT infrastructure-related issues and to the BSMB for business system-related issues. The ECAB also interfaces and coordinates with the other lower-level boards. Figure 3 illustrates NASA's current IT governance structure.

[22] The core membership of the MSC includes the Associate Deputy Administrator (chair), the Associate Administrator, the Associate Administrator for Mission Support, Chief Financial Officer, CIO, and Chief of Safety and Mission Assurance.

Figure 3. NASA IT Governance Structure



CAC – Customer Advisory Council
CCB – Configuration Control Board
DME - Develop, Modernize, Enhance
ESD – Enterprise Service Desk
EuS – End User Services
ICAM – Identity, Credential, and Access Management
I3P – Agency IT Infrastructure Integration Program
ITSAB – Information Technology Security Advisory Board
IPv6 – Internet Protocol Version 6
NEACC – NASA Enterprise Applications Competency Center
NSSC – NASA Shared Services Center
SIM - Service Integration Management
WG – Working Group

Source: NASA.

Longstanding Concerns About NASA's IT Governance. Historically, NASA has struggled to develop and effectively implement an IT governance approach that adequately aligns authority and responsibility with the overall mission of the Agency. For almost 2 decades, the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) have reported issues stemming from the limited authority of the Agency CIO, decentralization of Agency IT operations, ineffective IT governance, and shortcomings in IT security. For example, in 1996 GAO reported that a CIO who had greater authority would be in a better position to foster economies and efficiencies, settle disputes among the Centers, and initiate standardization and consolidation of Mission-related IT projects, thereby achieving cost savings.[23] NASA disagreed with the GAO and in its response to the report stated that the Agency's infrastructure derives strength and effectiveness through partnership, as opposed to a rigid, centralized compliance and control-based hierarchy.

NASA has traditionally favored a decentralized management structure for its projects and operations. For example, in the beginning of the Manned Space Flight Program, NASA shifted the bulk of decision making downward from the Associate Administrator to Center Directors, the heads of program offices, and project managers. The strategy was intended to give the Centers the resources and authority they needed to get the job done, but not so much autonomy that their work would lose relevance to the Agency's overall mission and priorities.

In March 2005, the OIG raised concerns about the organizational structure of the CIO offices at the Agency and Center levels, the limited Agency-level oversight of IT operations, and the OCIO's minimal involvement in the Agency's operations and budget activities.[24] In response, NASA hired a contractor to conduct an independent study and provide recommendations for the optimal organization and structure of IT governance at the Agency. The study recommended: (1) strengthening the current IT management model to ensure appropriate decision-making authority and levels of accountability are in place; (2) adopting an appropriate governance structure for each of NASA's IT portfolios with Center and Mission Directorate CIOs reporting directly to the NASA CIO; (3) aligning the IT organization with the Agency's focus on strategic management of human capital to ensure appropriate levels and competencies of resources; and (4) implementing an operational structure under the Agency CIO that clearly communicates strategic and tactical IT plans and measure, evaluate, and publish indicators of IT performance against the plans. NASA did not formally respond to these recommendations, and none of the personnel we interviewed were aware of any changes resulting from the study.

In December 2007, the OCIO conducted an internal assessment of NASA's IT management. The resulting report identified misalignments between IT management, the overall NASA mission, and the Agency's strategic plan. Subsequently, the Strategic Management Council tasked the CIO with developing a strategy in collaboration with the Center and Mission Directorate CIOs that would fully align the NASA IT environment to the Agency's mission and strategic plan.[25] As a result, NASA made changes to its IT

[23] GAO, "NASA Chief Information Officer: Opportunities to Strengthen Information Resources Management" (GAO/AIMD-96-78, August 15, 1996).

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

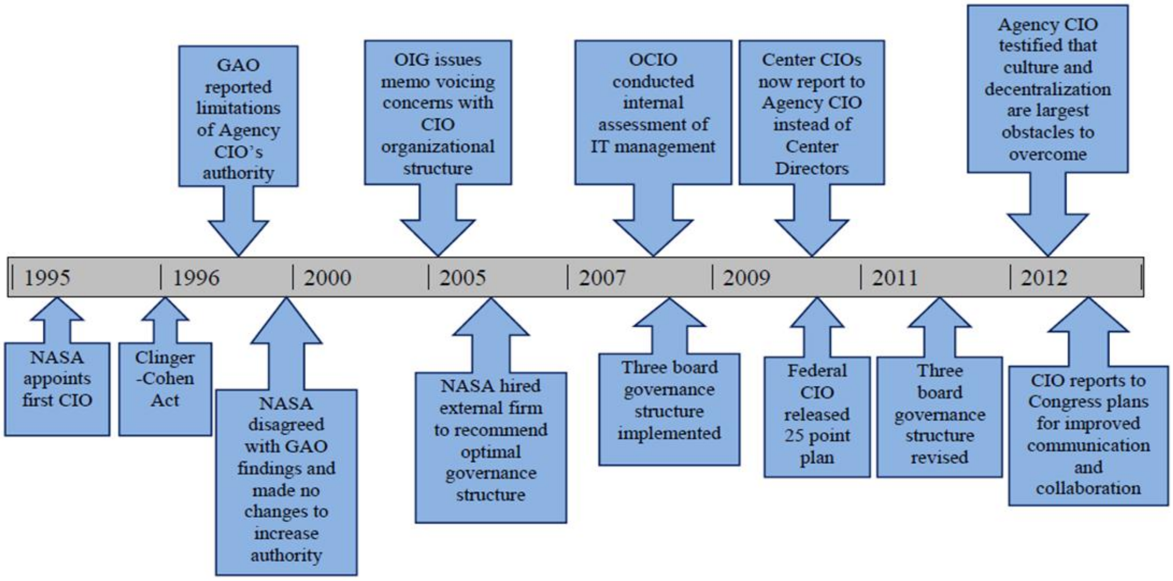
[25] The Strategic Management Council is one of three councils that make up NASA's overall governance structure and is the senior decision-making body for strategic direction and planning. NASA uses these councils when decisions require high degrees of integration, visibility, and approval.

governance board structure and began developing an Agency-wide acquisition plan to procure IT infrastructure services.[26]

In February 2012, the CIO testified before the House Committee on Science, Space, and Technology's Subcommittee on Oversight and stated that the largest impediment to effective IT security is persuading and changing the Mission Directorate culture. In 2013, in response to a legislative directive, the NASA CIO drafted a report to Congress outlining the Agency's plan to address cyber security issues.[27] The CIO recommended improving communication and collaboration among the OCIO, the Centers, and the Mission Directorates, but did not address the decentralization and related cultural issues noted in her February 2012 testimony.

Figure 4 depicts the evolution of NASA's IT governance structure over the past 17 years.

Figure 4. Evolution of NASA's IT Governance


GAO reported limitations of Agency CIO's authority
OIG issues memo voicing concerns with CIO organizational structure
OCIO conducted internal assessment of IT management
Center CIOs now report to Agency CIO instead of Center Directors
Agency CIO testified that culture and decentralization are largest obstacles to overcome
1995
1996
2000
2005
2007
2009
2011
2012
NASA appoints first CIO
Clinger -Cohen Act
NASA disagreed with GAO findings and made no changes to increase authority
NASA hired external firm to recommend optimal governance structure
Three board governance structure implemented
Federal CIO released 25 point plan
Three board governance structure revised
CIO reports to Congress plans for improved communication and collaboration

Source: OIG analysis.

Benchmarking. NASA's IT governance issues are not unique. Other Federal agencies have faced similar challenges related to decentralized IT management structures and limited CIO authority. To gain insight into lessons learned and industry best practices, we spoke with IT officials from the Department of the Interior (Interior), Department of Veterans Affairs (VA), and the United States Postal Service (USPS), all of which have

[26] The acquisition plan is known as the IT Infrastructure Integration Program or I3P and provides end-user services and equipment, application service technologies, networking, and Web infrastructure services and equipment.

[27] The directive was included in House Report 112-169, accompanying H.R. 2596, Fiscal Year 2012 Commerce, Justice, Science, and Related Agencies appropriations bills.

made substantial changes to their IT governance models in recent years. We selected these organizations based on similarities in size, IT architecture, and geographic dispersion relative to NASA.[28]

Department of the Interior. Interior uses its IT systems and data for a variety of diverse purposes, including providing the public with information about national parks; collecting royalties; and monitoring wildlife, fires, earthquakes, tsunamis, and volcanic activity. According to the Interior CIO, for many years the Department's independently operated "franchise-like" bureaus controlled their own IT resources and assets, which resulted in an IT governance structure that was inefficient, wasteful, and lacked accountability. As with NASA, GAO and Interior's OIG repeatedly cited the Department for ineffective IT governance. For example, in 2009, the OIG reported that the Department faced broad problems stemming from a decentralized IT organization and "fragmented governance processes."[29] In 2010, the Secretary consolidated accountability and control of the Department's IT assets under its CIO. All of the Department's IT services, personnel, and infrastructure that had been owned and controlled by other offices were placed under the CIO's purview and Department employees were required to obtain prior approval from the CIO for all IT procurements over $2,500. The Secretary instructed the Department to complete this transition within 4 years.

Department of Veterans Affairs. The VA consists of three administrations: the Veterans Health Administration (responsible for the VA health system), the Veterans Benefit Administration (responsible for veterans' pensions), and the National Cemetery Administration (responsible for administering burials and operating VA cemeteries). The largest of these, the Veterans Health Administration, has a budget of approximately $35 billion and oversees 155 medical centers, 872 ambulatory clinics, 135 nursing homes, 45 residential rehabilitation treatment programs, 209 veterans' centers, and 108 comprehensive home-care programs, which in turn are affiliated with 107 medical schools, 55 dental schools, and more than 1,200 other schools nationally. In 2005, the VA began consolidating its sprawling, aging, and complex system of computer and communications technologies as part of a multi-year effort to centralize all IT budgeting, planning, and development, including full control of the IT budget and staff, under the Agency CIO.

United States Postal Service. The USPS has annual revenue of more than $65 billion, delivers mail to 151 million addresses, and provides mailing services at 32,000 retail locations. USPS has the world's third-largest computing network, maintains one of the world's largest intranets, and has the most frequently visited website in the Federal Government. The USPS communications network maintains 125,000 desktop computers, 21,000 notebook computers, and 85,000 printers. The USPS began the process of centralizing its IT governance structure in the early 1990s. In the ensuing years, the

[28] In 2007, NASA OCIO benchmarked with the USPS on its IT security program, citing similar management characteristics.

[29] Department of Interior OIG, "Fiscal Year 2009 FISMA Evaluation Report – Revised," November 16, 2009.

USPS centralized all aspects of IT management under the Agency CIO, improving the organization's ability to leverage purchasing power, consolidate IT infrastructure on one network, and monitor that network for security threats.

Objectives

We initiated this audit to examine whether NASA's current IT governance structure appropriately aligns authority and responsibility to support the overall mission of the Agency. Specifically, we reviewed whether NASA's OCIO had the organizational, budgetary, and regulatory framework needed to fulfill the Agency's mission effectively. See Appendix A for details of the audit's scope and methodology, our review of internal controls, and a list of prior coverage.

NASA'S IT GOVERNANCE IS INEFFECTIVE

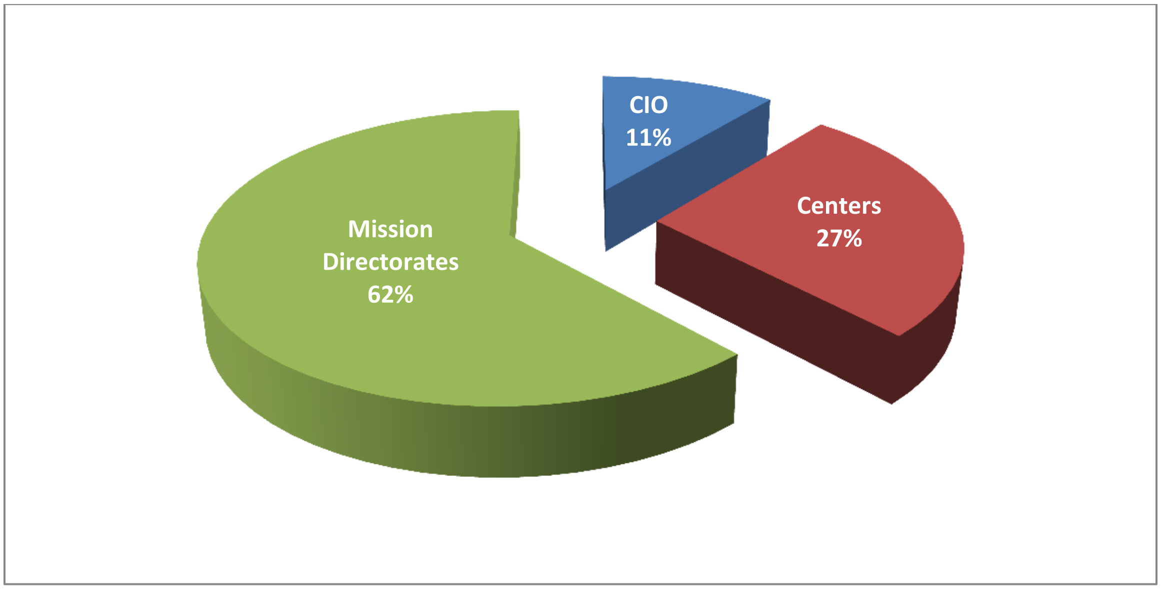
Decentralized operations and a culture of autonomy for Centers and Mission Directorates have hindered NASA's ability to implement effective IT governance. Although Federal policies make agency CIOs accountable for agency IT assets, we found that the NASA CIO has limited visibility and control over a majority of the Agency's IT investments, operates in an organizational structure that marginalizes the authority of the position, and cannot enforce security measures across NASA's computer networks. We also found that NASA's IT governance board structure is overly complex and does not function effectively. Accordingly, when making IT decisions managers tend to rely on informal relationships rather than formalized business processes that consider input from the full range of stakeholders and ensure accountability. While other Federal agencies are moving to organizational structures that centralize IT decision-making authority in the agency CIO, NASA's IT governance model limits the CIO's authority, weakens accountability, and does not ensure that the Agency's IT assets are cost effective and secure.

Limited CIO Control of IT Funding and Investments

NASA's CIO has little visibility or control over a large portion of the Agency's IT funding. For FY 2012, NASA's budget for IT operations and new asset acquisitions was $1.46 billion. As illustrated in Figure 5, the Agency CIO had direct control of only $159 million, or 11 percent of these funds. The Centers controlled $393 million, or 27 percent of these funds, while the Mission Directorates controlled the remaining $912 million, or 62 percent. Moreover, the Agency CIO and many of the Center CIOs we spoke with stated that they lack visibility of Mission Directorate IT asset purchases because funding for Mission-related IT is often embedded in program and project funding.

An anecdote recounted to us during our review illustrates this dynamic. According to the Agency CIO, although planned IT expenditures for FY 2010 were $1.6 billion, the Agency actually spent $2 billion. However, the CIO was unaware of the $400 million overage until the Mission Directorates reported actual expenditures to the OCIO in a data call needed to respond to an OMB request.

Figure 5. Total FY 2012 IT Budget Responsibility



Source: NASA OCIO.

In a November 2012 internal presentation, the OCIO identified several challenges that resulted from its lack of visibility over IT spending: difficulty obtaining financial data; having to rely on data calls for information about IT spending; difficulty in identifying IT expenditures embedded in task orders; reluctance by Center managers to identify IT funds for fear the funds might be redirected; and a significant amount of unplanned year-end IT spending. To address several of these issues, the OCIO is working with the Office of the Chief Financial Officer and the Office of the Chief Engineer to update the Agency's policies and financial system to give the Agency CIO greater visibility into IT expenditures. However, even with this increased visibility the Agency CIO will still learn of purchases only after they are made and continue to have no authority to approve expenditures before they occur.

Our audit work over the years has identified similar issues. In September 2004, the NASA CIO established an Agency-wide process for selecting and managing IT capital investments. While the Agency CIO was responsible for establishing and updating the policy, the CIO relied on Mission Directorate and Center CIOs for policy execution and recommendations on how to prioritize investments. In a 2006 audit, we found numerous inconsistencies in the ways in which three Centers implemented the Agency CIO's policy.[30] Specifically, two of the Centers used their own prioritization methodology because they did not believe they were required to comply with the Agency CIO's policy. Officials from the third Center stated they believed they were acting consistently with the

[30] NASA OIG, "Final Memorandum of NASA's Information Technology Capital Planning and Investment Control" (IG-06-017, September 14, 2006).

policy requirements, even though they assigned investment scores that deviated from the established process for prioritizing and selecting investments. Because of these weaknesses, we concluded that the Agency CIO was unable to ensure consistency in NASA's IT investments.

The Agency CIO's lack of visibility and approval authority over the majority of NASA's IT expenditures also limits NASA's ability to realize cost savings and improve the delivery of IT services. For example, NASA's I3P initiative is an effort to centralize purchases of IT infrastructure services such as networks, Web technologies, and applications. However, even with the implementation of I3P, Mission Directorates and Centers still have authority to make many IT purchases without the OCIO's review or approval. One Center Chief Information Security Officer (CISO) told us that Centers are free and indeed often required to perform their own requirements analyses, product evaluations, and product purchases, leading to the purchase of inconsistent and sometimes duplicative tools existing at different Centers at an increased overall cost to NASA. To this point, our office recently reported that NASA does not have a process that captures, consolidates, and assesses IT security tool requirements across the Agency.[31] Because of this deficiency, the Agency made 242 separate purchases of IT security assessment and monitoring tools at a cost of $25.7 million without Agency-wide coordination. With the IT budget decreasing by almost $1 billion over the last 6 years, it is imperative that the Agency increase efficiencies in its IT purchases and investments to reduce costs.

Organizational Structure Marginalizes the Agency CIO

Over its 50-year history, NASA's organizational structure has valued autonomy. Dispersion of authority between Headquarters, the Mission Directorates, and the Centers is the cornerstone of NASA's program and project governance. NASA has traditionally given its Centers and project managers the autonomy to independently conceive projects, develop specifications, and supervise contractors. In line with this philosophy, when NASA chartered the Agency CIO position in 1995, the authority of the position was intentionally limited to ensure that Agency program offices and Centers would retain broad flexibility in managing IT activities related to their projects. However, with this autonomy comes issues of organizational control, coordination, reporting requirements, and the manner in which information flows between Agency decision-makers. A recent external review of NASA's overall governance and decision-making commissioned by the Strategic Management Council found that the Agency's highly matrixed organizational structure adds complexity to decisions involving issues that cross Center, Mission, or functional chains of command.[32]

[31] NASA OIG, "NASA's Process for Acquiring Information Technology Security and Assessment and Monitoring Tools" (IG-13-006, March 18, 2013).

[32] NASA Governance and Decision Making Discussion Document, McKinsey & Company, May 1, 2011.

We found that IT management is one area in which this separation has resulted in a "turf war" between three distinct interests – the OCIO, the Mission Directorates, and the Centers. For example, each Mission Directorate and Center employs their own CIO and IT security personnel, resulting in hundreds of independently operated networks and tens of thousands of computers and other IT hardware that is outside of the control or oversight of the OCIO. NASA policy states that the NASA CIO has the responsibility, authority, and accountability to develop and maintain an effective Agency IT governance structure. However, in practice, resistance from the Mission Directorates and the Centers to relinquish control over IT funding decisions, coupled with the ability of these entities to operate autonomously by funding for their project-level IT systems, significantly limits the Agency CIO's oversight and authority.

In March 2010, the OCIO surveyed the members of NASA's three IT governance boards concerning the effectiveness of the Agency's IT governance structure. A majority of board members responded that NASA's IT governance structure was not effective for Mission IT, decisions were made outside of the governance structure, intended benefits of IT investments were not tracked or realized, and officials lacked sufficient visibility into IT spending in order to make informed decisions.

Agency CIO Has Limited Authority. Having numerous Agency officials with the same title and similar roles, not all of whom report to the Agency CIO, dilutes the Agency CIO's authority. NASA employs 1 CIO at the Agency level, 10 CIOs at the Center level, 1 CIO at the Jet Propulsion Laboratory, 1 CIO at the NASA Shared Services Center, and 1 CIO within each of the Mission Directorates. This structure both undermines the Agency CIO as the ultimate decision authority and blurs the lines of accountability and responsibility. For many years, Center CIOs reported to their respective Center Directors. Although the Agency changed this reporting structure in 2010 and the Center CIOs now report to the Agency CIO, some Center CIOs told us that because Center Directors still control Center IT budgets, they saw no operational difference since the change other than that the Agency CIO now conducts their annual performance evaluations.

Moreover, the Agency CIO is the only one of seven "Chief" positions at NASA that does not report directly to the Agency Administrator.[33] This reporting structure is out of line with Federal policy and best practices.[34] In our judgment, affording the Agency CIO the same visibility as the other Chiefs sends a message about the significance of IT and would better ensure that NASA's IT posture aligns with the strategic direction of the Agency. For the Agency CIO to be in the best position to bring about fundamental changes to NASA's IT governance, the full awareness and support of the NASA Administrator and senior management staff is required.

[33] The Chief Financial Officer, Chief Scientist, Chief Technologist, Chief Engineer, Chief Safety and Mission Assurance, and Chief Health and Medical Officer all report to the Administrator.

[34] 44 USC Chapter 35, Coordination of Federal Information Policy.

Furthermore, the Mission Directorate CIOs do not report to the Agency CIO or the Center CIOs, but rather to the Associate Administrators of the Directorates. The Associate Administrators control the Mission Directorates' IT budgets and funding, which run into the hundreds of millions of dollars. Mission Directorate CIOs act as a liaison between the Mission Directorates and the OCIO by attending ITMB meetings and responding to OCIO data calls but are not involved in making Agency-wide IT strategic decisions. The Mission Directorate CIOs told us they do not feel included or thought of as partners by the OCIO and that the OCIO does not place sufficient emphasis on developing, implementing, and managing enterprise level infrastructure that meets the Mission Directorates' needs.

The significant amount Mission Directorates spend on IT purchases each year requires full visibility and integration between the OCIO, the Mission Directorate CIOs, and the Center CIOs. In our judgment, it is crucial that the Mission Directorate CIOs provide the OCIO with visibility into Mission Directorate IT projects, and in turn promote Agency-wide CIO initiatives within their respective directorates. Further, the Agency CIO should ensure that Mission interests are considered in the development of Agency-wide IT requirements. Without fundamental changes to NASA's current IT governance structure, we do not believe these goals can be accomplished.

In prior audit work, we found that NASA's multi-layered, organizationally, and geographically dispersed structure has led to wide variations in IT processes and a lack of awareness of and adherence to Agency IT policy. For example, in a December 2010 report, we found that IT personnel at three Centers were unfamiliar with and therefore did not follow NASA policy relating to the sanitization of excess IT equipment, which could lead to the unintended release of sensitive NASA data.[35] Our report highlighted the disparity in processes at four Centers and a lack of awareness and adherence to Agency policy requirements that resulted in one Center selling and preparing for sale computers that contained sensitive data. We also found a lack of accountability for IT equipment, including one Center that excessed hard drives in an unsecured dumpster accessible to the public.

Similarly, our recent special review of NASA's multi-year effort to encrypt its laptop computers pointed to weaknesses related to the Agency's IT governance.[36] In February 2012, the NASA Inspector General testified that only 1 percent of NASA portable devices including laptops had been encrypted compared to a Federal Government-wide encryption rate at the time of 54 percent.[37] On October 31, 2012, an unencrypted NASA laptop containing personally identifiable information for more than 40,000 individuals was stolen from the vehicle of a NASA employee. As a result of this loss, NASA

[35] NASA OIG, "Preparing for the Space Shuttle Program's Retirement: A Review of NASA's Disposition of Information Technology Equipment" (IG-11-009, December 7, 2010).

[36] NASA OIG "NASA's Effort to Encrypt its Laptop Computers (Special Report, December 17, 2012).

[37] NASA Inspector General, testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, February 29, 2012.

provided credit monitoring services to the affected individuals, which the Agency estimates could cost up to $850,000. Following this incident, the NASA Administrator accelerated the Agency's deadline for encrypting its laptop computers by several months, and the Agency estimated that this expedited effort cost at least $259,000, not including the time civil servants devoted to the project. Our review found that the highly decentralized nature of IT management at the Agency was one of the factors that contributed to the repeated delays in NASA's full-disk encryption effort for its laptop computers. For example, we found that the OCIO did not have a complete inventory of Agency IT assets, which made it difficult to ensure that all laptops had been accounted for and encrypted.

The issues currently challenging the NASA CIO are not new and have been raised repeatedly since the position was created. In response to both internal and external reviews, the OCIO has often advocated solutions that rely on "improved collaboration" between the OCIO, the Centers, and the Mission Directorates. Most recently, in a draft report to Congress, the Agency CIO proposed reducing cyber-attacks by coordinating among Agency and Mission security stakeholders to establish a strategy that standardizes procedures, policies, and tools deployed across NASA.[38]

While coordination and collaboration are important components of any IT strategy, we do not believe that coordination and collaboration alone will be sufficient to overcome the issues we and others have identified. NASA's autonomy of operations for IT matters prevents the Agency CIO from taking and enforcing meaningful actions, and instead reduces the position to issuing calls for increasing "cooperation and communication" – calls that at least up to this point have gone unanswered. In short, the Agency's culture and current structure hinders the CIO's ability to implement and enforce sound IT governance initiatives.

Responsibilities and Interaction between IT Boards Unclear

The ITMB, BSMB, and IT PMB all play a role in decision making for and oversight of Agency IT infrastructure projects. In addition, NASA has established numerous lower-level boards and working groups to discuss IT issues. We found that a lack of documentation and training regarding the roles and interrelationships of these boards and working groups has led to confusion over the information presented to and the procedures for communicating between them. The boards' policies and charters are unclear and only add to the confusion. As a result, the boards' value in making informed decisions about issues like future IT acquisitions and security has been greatly diminished.

NASA's governance structure calls for coordination and collaboration between the three primary boards and the numerous underlying service boards and working groups;

[38] NASA Draft Report, "Implementation of Administrative Remedy Regarding Cyber Security," pursuant to H.R. 112-169 accompanying H.R. 2596.

however, several of the IT managers we interviewed did not understand the structure of the boards or their interaction and cited poor communication between the groups. We also found confusion as to how and what information is passed from the service boards and working groups to the primary boards where decisions are made. For example, one ITMB member told us he had difficulty understanding the ITMB's purpose, who is the responsible party, and what role the subordinate boards played in the IT governance process. Several other ITMB members echoed these comments. Moreover, NASA policy and the charters of the primary boards do not align. For example, the policy purports to define the boards' jurisdictions by reference to criteria in the charters, but the charters do not contain this referenced information.

As a case study, we reviewed the actions of the IT governance boards relating to the Agency's implementation of full disk encryption and found the project circumvented the regular approval process. According to the encryption implementation plan, the IT PMB should have overseen the project. However, the encryption team requested a waiver to designate the ITMB as the governing body because the project was being deployed within the Centers' infrastructure. In the end, neither board approved the project implementation plan. Instead, one of the subsidiary boards – the End User Services Board – provided final approval of the implementation plan. Although the Board's charter states that it was created to address issues like the encryption initiative, the risk, visibility, and complexity of the encryption project far exceeded the Board's established authority. Further, NASA did not follow its governance requirements and began installing encryption software on Agency laptops in March 2012, 3 months before completion of the Operational Readiness Review.[39] Prior to implementation, it was discovered that the encryption software was not compatible with the Agency's personal identity verification cards and the vendor had to modify the software, further delaying implementation. According to the head of the encryption implementation team, properly vetting the encryption software through the governance process may have avoided some of the compatibility issues and challenges encountered during implementation.

Center CIOs, Center CISOs, and Mission Directorate CIOs consistently expressed the opinion that while the boards are great forums for collaboration among peers, important issues and initiatives are not consistently presented to all applicable boards. For example, the Agency CIO established the IT Security Advisory Board (ITSAB) to serve as a resource on information security issues for the NASA IT community. However, members of the ITSAB stated that not all the issues presented to the ITMB were first vetted through the ITSAB. Moreover, board members told us that they were confused about the purpose of the ITSAB, including its authority and integration with other parts

[39] NASA Procedural Requirements (NPR) 7120.7, "NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements," November 3, 2008, defines key decision points and milestones that must be presented to the governance boards prior to continuing a project. The Operational Readiness Review determines that the project is ready to go-live with the system or service; requirements have been met; the functionality, performance, and security controls have been thoroughly tested; procedures are in place for operations; the users have been adequately trained; and the organization responsible for operations and sustaining engineering is ready to assume responsibility. It ensures a security plan is in place and that system authorization has been received.

of the governance structure. These officials said that not involving IT security officials in the initial planning phase of Agency projects means that NASA is often forced to react to security-related issues that arise during implementation rather than planning for them ahead of time. Representatives from the IT Security Division acknowledged these same issues and are currently working to re-charter and improve integration of the ITSAB within the IT governance structure.

Officials we interviewed also expressed concern that there was little to no vertical communication between the boards. For example, several reported that the Agency Deputy CIO for Security was the single point of communication to advocate to the primary boards issues raised by the ITSAB, even though this is not how the process was designed in the ITSAB charter and the Deputy CIO rarely attended ITSAB meetings. Several ITSAB members told us they were not satisfied with the level of communication between the boards. For example, one member commented that "given the lack of IT security participation in the OCIO IT governance model, or outreach from OCIO IT security management, the Center CISOs do not have insight into an Agency/OCIO strategy and priorities for IT security at NASA, if such strategy and priorities exist." Members of the ITSAB also stated that they did not understand how the board fits into the Agency's overall IT governance structure. Specifically, several CISOs stated that it was not clear whether issues discussed at ITSAB meetings were relayed to higher-level boards and noted they often did not receive responses to their input. Overall, we found that the number of boards coupled with confusion over how they interrelate contributes to the ineffectiveness of NASA's IT governance structure.

Moreover, the Mission Directorate CIOs and the Center CIOs told us that the Mission Directorate personnel often work outside of established procedures because of the amount of time it takes a decision to make its way through the current governance process. Mission Directorate CIOs expressed their concerns with the formal governance process citing time constraints, impact of security on the mission, and the potential for nonapproval. One concern is that IT initiatives routed through the IT governance process tend to lag behind Mission Directorate requirements and this makes the process appear nonresponsive or not sufficiently dynamic to meet the Mission Directorates' needs. Another concern is that the Mission Directorates often cannot wait for Agency decisions to occur or be implemented on new IT initiatives. This lack of coordination results in duplication of IT infrastructure and applications as well as restricted information and resource sharing between and across the Agency.

Finally, we found that NASA IT managers tend to rely on informal relationships rather than formalized business processes to make IT decisions. Many Center CIOs attribute the success of IT initiatives at their Centers to strong collaboration between Center IT and Mission Directorate representatives at the local level. The Center CISOs who told us they felt comfortable with the security posture of the Mission Directorate IT assets at their Centers have fostered personal, collaborative relationships with the Mission Directorate representatives at their Centers. For example, the CISO at Johnson Space Center noted that because Mission Directorates answer to a different chain of command, he is not able to make the final decision in matters of design, procurement, and implementation. However, the Center CIO noted that many of the Mission Directorate representatives at Johnson work with him and Center IT security personnel to align their activities with the Center's efforts. In sum, we found that collaboration on IT issues that takes place at the Centers generally is not facilitated by the formal IT governance structure, but rather is a result of the willingness of the parties to work together in the best interests of the Agency.

CIO Cannot Enforce Security Measures over a Majority of IT Assets

Over the past several years, our audits have repeatedly identified poor management processes and inadequate operational and technical controls that affect NASA's ability to protect the information and information systems vital to its mission. Specifically, we have reported on the challenges NASA has implementing a new continuous monitoring methodology, a process for protecting networks from cyber-attacks, a plan for addressing known security weaknesses, and full disk encryption for its tens of thousands of laptop computers.

For example, in 2010 and 2011 we reported shortcomings as NASA moved from a compliance-focused "snapshot" approach for measuring the security of its IT systems to a continuous monitoring approach that seeks to perform real-time security monitoring.[40] Specifically, our audits found that the Agency's continuous monitoring program was ineffective because NASA:

- did not have a complete inventory of the devices connected to its networks and thus could not verify that 100 percent of Agency computers undergo monitoring to ensure they remain securely configured, free of technical vulnerabilities, and adequately patched;
- did not monitor configuration settings of Agency network servers to certify that these critical resources remained securely configured; and
- had not established baselines for securely configuring widely used Agency computer operating systems, including Windows servers.

We concluded that collectively, these issues inhibited the NASA CIO's awareness of the Agency's overall security posture and significantly hindered the Agency's ability to secure its networks and protect sensitive information.

[40] NASA OIG, "Audit of NASA's Efforts to Continuously Monitor Critical Information Technology Security Controls" (IG-10-019, September 14, 2010), and "NASA Faces Significant Challenges Transitioning to a Continuous Monitoring Approach for its Information Technology Systems" (IG-12-006, December 5, 2011).

In March 2011, we reported that NASA needed to improve its processes for protecting Mission networks from Internet-based cyber-attacks.[41] Specifically, we found that six computer servers associated with IT assets that control NASA spacecraft and contain critical data had vulnerabilities that could allow a remote attacker to take control of or render them unavailable. Moreover, once inside the network, the attacker could use the compromised computers to exploit other weaknesses we identified that could severely degrade or cripple NASA operations. We also found network servers were not securely configured and, as a result, exposed encryption keys, encrypted passwords, and user account information to potential attackers.

Lastly and as previously discussed, in December 2012, we reported that issues and challenges associated with the implementation of full-disk encryption on NASA's laptop computers caused NASA to miss its target implementation dates, thereby leaving sensitive operational data vulnerable to theft. Specifically, we found that NASA's full-disk encryption effort was repeatedly delayed due to slow implementation of its computer services contract, the highly decentralized nature of information technology management at the Agency, and a lack of sufficient internal controls. Moreover, the Agency did not have a reliable accounting of the number of laptops in its possession and therefore was not likely to be able to ensure that encryption software was installed on 100 percent of required machines by the deadline.[42]

NASA Culture Inhibits CIO's Ability to Secure Assets. Federal law designates the Agency CIO as the official responsible for developing IT security policies and procedures and implementing an Agency-wide IT security program. However, we found that the NASA CIO is unable to enforce implementation of recommended or mandated IT security programs because of the autonomous nature of NASA operations. NASA's IT environment is diversified with hundreds of networks owned and operated by the Mission Directorates and Centers. Mission Directorates fund their computer networks and Directorate personnel are responsible for IT security, risk determination, and risk acceptance. Moreover, Mission Directorate personnel make the determination on how to secure their networks outside of the Agency CIO's authority. Because there is no one group responsible for securing NASA's networks, there is little standardization across the Agency. NASA's networks include numerous hardware configurations and multiple operating systems at varying version and security levels that make securing the Agency's portfolio of IT assets extremely complex. For example, even though the OCIO manages Web content at the Agency level, the Mission Directorates and Centers operate and fund 3,447 websites.[43] This large number of public-facing websites provides numerous entry

[41] NASA OIG, "Inadequate Security Practices Expose Key NASA Network to Cyber Attack" (IG-11-17, March 28, 2011).

[42] We made five recommendations in this review to help protect NASA's information and prevent unauthorized access to data stored on its laptop computers such as developing a better method to account for laptops and reexamining the role of Agency IT officials for safeguarding mobile IT assets. The Administrator agreed with each of our recommendations and proposed corrective actions.

[43] NASA reported this information in the Agency's Web Improvement Plan provided to OMB in 2011.

points to the Agency's networks potentially allowing unauthorized access to sensitive information and technology.

Further complicating NASA's ability to secure its networks is a lack of a complete inventory of IT assets. Several CISO's we spoke to stated that there is no visibility over the complete inventory of IT assets, and individual organizations often do not have accurate and complete information on their assets, configurations, and security vulnerabilities. We found that this condition persists across the Agency. Five Center CIOs told us they could not account for 100 percent of the IT systems and hardware at their Centers. According to the CISOs, Agency efforts to establish a consistent, consolidated IT security inventory have been thwarted by inconsistent enforcement of the policies and implementation of the tools meant to capture the information, pockets of NASA organizations not agreeing to provide requested information, and inconsistent or lack of guidance from OCIO IT security management. One Center CISO stated that some Mission Directorate personnel at his Center are not diligent in following Agency directed security policy and that in some cases Mission Directorates have attempted to hide assets; thus circumventing Agency requirements.

Governance Model Fails to Adequately Address Security. We have consistently identified the lack of strong governance as an overarching reason for significant and ongoing IT security deficiencies at NASA. In May 2010, we reported that only 24 percent of applicable computers on a network that supports mission-critical spacecraft and science operations were monitored for critical software patches and only 62 percent were monitored for technical vulnerabilities.[44] During detailed control testing, we identified several high-risk vulnerabilities on a system that provided support to manned and unmanned spacecraft. If exploited, these vulnerabilities could allow a remote intruder to gain control of the system or render it unavailable.

These deficiencies occurred because NASA had not put in place an oversight structure to maintain the security of this mission-critical network and to ensure that Agency IT security policies and procedures were followed. In response to our report, the Agency agreed to: (1) designate a NASA Directorate or Center to immediately establish an oversight process to include monitoring of systems for the presence of critical patches and technical vulnerabilities and (2) review all other Agency Mission network IT security programs to determine whether each contains an effective oversight process. However, almost 3 years later these actions have yet to be completed.

In her February 2012 Congressional testimony, the Agency CIO acknowledged that NASA's culture does not support building effective cyber security processes. The Agency CIO stated that the largest impediment to effective IT security is persuading and changing the Mission Directorate culture. Center CISOs we spoke with echoed this sentiment, stating that they do not believe that IT security has been adequately built into the Agency's IT governance model. The consensus during our interviews was that

[44] NASA OIG, "Review of the Information Technology Security of [a NASA Computer Network]" (IG-10-013, May 13, 2010).

security is an afterthought and NASA is operating primarily in a reactive mode to security incidents. In large part, IT personnel believe that this is due to the lack of consideration of IT security when designing and implementing IT initiatives. The Center viewpoint is that the Agency makes decisions without consulting security personnel at the Centers on potential security impacts. For example, several Center IT security representatives stated that security issues are discussed at the higher-level boards without consulting the Center-based CISO community through the ITSAB.

Moreover, we found consensus among the Center CIOs and CISOs that the SOC cannot function effectively because it does not have adequate visibility over NASA's Mission networks. The SOC is the OCIO's central coordination point for Agency-wide security incident detection, response, and reporting and provides centralized, continuous monitoring of computer network traffic entering and leaving NASA Centers and includes an information system for Agency-wide coordination, tracking, and reporting of security incidents. However, the SOC has limited visibility of NASA's Mission networks and no visibility of the Agency's high-performance computing networks (networks with transmission rates of 10Gig +).[45] Under the current design, the Mission Directorates are responsible for implementing their own incident management program. Consequently, NASA relies on Mission Directorates, which control nearly 62 percent of NASA's annual IT spending, to self-report intrusions or other security incidents.

SOC officials told us that the Mission Directorates are reluctant to allow visibility to their networks and that their biggest challenge is changing this culture. The OCIO requested funding in NASA's 2013 budget to extend SOC coverage to identify and include the Mission networks. However, even if NASA were to receive this funding, Mission Directorates may remain reluctant to grant the SOC access and the Agency CIO lacks the authority to force compliance. The inability of the NASA CIO to ensure that all of the Agency's computer networks implement key IT security controls places critical IT assets at risk of compromise. This is particularly troubling given previous findings that Mission Directorates often lack effective IT security and IT assets operated by these Directorates do not consistently implement key IT security controls.[46]

IT Governance across Government

Although NASA's mission is unique, the challenges the Agency faces in managing a decentralized IT environment are not. We examined IT governance at three agencies that like NASA are geographically diverse, independently operated, and support thousands of users – Interior, VA, and the USPS. Each of these organizations has moved away from a decentralized model to a consolidated, centralized structure. The VA and Interior began this process during the past 8 years and these efforts are ongoing. The USPS centralized

[45] NASA OIG, "Review of NASA's Computer Security Incident Detection and Handling Capability" (IG-12-017, August 7, 2012).

[46] NASA OIG, "Review of the Information Technology Security of [a NASA Computer Network]" (IG-10-013, May 13, 2010).

its IT infrastructure in the 1990s, but recently revised its IT governance structure to ensure that all IT activities fall within the purview of the Agency CIO.

Prior to centralization, each of Interior's nine bureaus employed a CIO and technical staff to manage and provide IT services to approximately 70,000 employees at more than 2,400 locations. Both Interior's Inspector General and the GAO repeatedly reported that the Department's IT and cyber security governance was inefficient, wasteful, and lacked accountability. In 2010, the Secretary of the Interior placed the Department's entire IT infrastructure under the purview of the Department's CIO, and all of the IT services, personnel, and infrastructure owned and operated by other offices were transferred to the CIO. The Secretary instructed the Department to complete the transition within 4 years.

Likewise, the VA had a decentralized IT governance structure spread across 3 divisions and more than 1,000 medical centers, clinics, nursing homes, and veterans' centers. In 2005, in response to a statutory directive, the VA moved to a centralized model under which the Agency CIO has control over all IT resources.[47] This was a multi-year effort centralizing all IT budgeting, planning, and development, including full control of the VA's IT budget and staff, under the Agency CIO.

Officials at these organizations told us that based on their experience, unless the Agency CIO has the full support of the head of the organization and is given the ultimate decision and enforcement authority over all areas of IT in the organization, the CIO would not be able to implement an effective and successful IT governance structure. The Interior CIO said he believed none of the changes at his Department could have taken place without the full support of the Secretary.

Another key aspect of the transformation at these organizations was eliminating the confusion about "who was in charge" by ensuring that all personnel with CIO responsibilities report to the Agency CIO and by reserving the title of CIO solely for that official. Each of the organizations we met with revised their governance structure to employ only one CIO who reported to the head of the organization and who had authority and responsibility over all IT resources and budgets. This change helped clearly delineate the CIO as the ultimate decision authority over IT matters. Prior to centralization, Interior employed more than 30 individuals with the CIO title. Similarly, USPS revised the job titles of all CIOs in its organizational units to clarify that the Agency CIO has ultimate decision authority for IT matters. According to the VA and Interior CIOs, the reorganization of IT functions under one official responsible for IT across their organizations resulted in increased efficiency and security, as well as lower operating costs.

We also found that centralization of the IT function at these organizations resulted in improved control over IT funding and expenditures. At USPS, all IT purchases go through a single purchasing unit. At Interior, the CIO must approve all IT purchases that

[47] H.R. 4061, ''Department of Veterans Affairs Information Technology Management Improvement Act of 2005."

exceed $2,500.[48] In addition, all major IT procurements are routed through a Department-level management board of contracting officers with specialized IT procurement experience. According to the Interior CIO, he has the authority to remove the warrant of any contracting officer that authorizes purchases outside of this approval system. According to Interior's CIO, the Department's bureaus initially were not receptive to turning over control of their funding to a Department CIO. However, Interior adopted the approach that having funding does not constitute the right to proceed with an IT initiative.

Prior to centralization, the VA CIO had direct control over only 3 percent of the Department's overall IT budget and 6 percent of the Department's IT personnel. With support from the Secretary of Veterans Affairs and Congress, the VA centralized all IT budgeting, planning and development, and placed full control of the VA's IT budget and staff under the Assistant Secretary for Information and Technology (the CIO for the Agency). According to the VA CIO, the transition was not easy or quick – it took more than 2 years to identify all of the IT money and resources from the various parts of the agency. Prior to this transition, individual medical directors in the field had virtually complete control over decisions about IT investments, which had resulted in an ad hoc and disjointed IT system. The VA CIO told us that consolidating IT Department-wide resulted in a savings of $1.7 billion over 4 years; a successful, on-time IT product development rate of 90 percent compared to 30 percent prior to consolidation; and a 40 percent increase in IT services provided without an increase in cost (no budget increase in the prior 3 years).

According to the VA and Interior CIOs and the USPS CISO, restructuring the management of IT at these agencies has also improved the function of their governance boards and the security of their IT networks. At the VA, charters clearly explain the jurisdictions of the various boards and how they interact with one another. Similarly, vertical and horizontal coordination, reporting, and critical information flow between VA's IT governance boards allows for more transparent communication and decision making between them. All of the IT executives stressed the importance of having IT security representatives involved throughout the IT governance process to ensure that appropriate security measures are implemented from the initial stages of development of any IT project. At USPS, the CISO is involved in the planning phase of any new initiative and is an active participant in the IT governance process. With regard to security, the VA CIO stated that since consolidation the VA centrally monitors all systems, affording a comprehensive view of threats. Similarly, USPS reduced its operational networks from 18 to 1, and the consolidated network falls under the purview of the OCIO where it is monitored for security threats. Any security incidents identified at USPS flow through a centralized, security office.

Interior, VA, and USPS officials told us that centralizing IT management across their agencies was a political, painful, and time-consuming process. At Interior, the

[48] This threshold contrasts rather sharply with the $400 million on IT expenditures discussed previously that the NASA CIO admitted no awareness of until a year after the money was spent.

transformation was a multi-year initiative that required cooperation from each bureau and office, and Interior officials spent over a year just planning the process. According to a Department report, the consolidation will result in approximately $500 million in cost savings, increased employee efficiency, and elimination of waste. Moreover, in 2011 for the first time in nearly a decade the Interior's OIG did not identify IT or IT security as a top management challenge for the Department.

With mission critical assets at stake and IT budgets shrinking, NASA must take a holistic approach to operating its vast portfolio of IT systems. In our judgment, centralization of the Agency's IT framework under a Headquarters-based CIO would improve NASA's overall management of IT, including planning, acquisition, and security, while increasing control over IT expenditures and accountability. Because of the integrated nature of IT infrastructure throughout the Agency's operations, spreading oversight of and authority over IT assets among the Agency CIO, the Mission Directorate CIOs, and the Center CIOs has led to a governance structure that is overly complex and ineffective. Although coordination and collaboration between these entities will always be necessary, we believe that both NASA's history and the experience of the other agencies supports a recommendation that NASA move to a more centralized approach to IT governance.

Recommendations, Management's Response, and Evaluation of Management's Response

For almost 2 decades, the OIG and GAO have reported on a variety of issues related to NASA's decentralized IT operations, the limited authority of the Agency CIO, and significant lapses in IT security. However, during this time NASA has made only incremental changes in its approach to IT governance. In our judgment, NASA must make fundamental changes to its IT governance model and significantly strengthen the Agency CIO's authority in order to address serious IT challenges. The retirement of the Agency CIO in April 2013 presents NASA with an opportunity to reevaluate its IT organizational structure and personnel resources.

The NASA Administrator must be the driving force behind this effort and ensure that the Agency has the leadership in place not only in the OCIO but also at the Centers and in the Mission Directorates to transform NASA's IT management culture. To overcome the barriers that have resulted in inefficient and ineffective management of the Agency's IT assets and operations, we recommend that the NASA Administrator:

Recommendation 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.

Management's Response. The Administrator concurred with our recommendation, stating that the OCIO will implement the IT Governance model approved by the Mission Support Council (MSC) in November 2011 and will further adapt implementation to address the issues identified in our report. The Administrator stated that as the model is phased in it will provide the OCIO with greater visibility into both institutional and Mission IT investments and assets and lead to greater accountability and integration. The Agency plans to have the model in place by May 30, 2014.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved. We will close the recommendation upon verification that the MSC model provides the OCIO with adequate visibility, accountability, and integration into Mission-related IT assets and activities.

Recommendation 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.

Management's Response. The Administrator concurred with our recommendation and stated that the OCIO will work with the Office of the Chief Financial Officer and the Office of Procurement to develop process improvements and implement any required financial system changes. In addition, through the Enterprise Architecture program the OCIO will define and document a technical baseline to make it easier to align procurements with Agency strategic direction. The Agency plans to complete these actions by December 31, 2013.

Evaluation of Management's Response. Management's proposed actions are responsive. We will close the recommendation upon verification that the Agency established an approval threshold that captures the majority of IT expenditures.

Recommendation 3. Reevaluate the relevancy, composition, and purpose of the existing boards in light of changes made to the Agency's IT governance structure.

Management's Response. The Administrator concurred with our recommendation, stating that the incoming Agency CIO will evaluate the composition, roles, responsibilities, reporting structure, and processes of the Agency's IT governing boards. In addition, as an immediate step the Acting CIO has implemented an I3P Organizational Assessment that includes a review of I3P governance and the roles, responsibilities, and decision rights of the Program Office, each Service Office, and the Center CIOs. The Agency plans to complete its assessment of the Boards within 180 days of appointment of a new Agency CIO.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 4. Require the use of governance boards for all major IT decisions and investments, including those made by Mission Directorates.

Management's Response. The Administrator concurred with our recommendation, stating that although programs and projects will continue to have the ability to manage highly specialized Mission IT, under the MSC-approved governance model the Agency CIO will have approval rights over institutional and non-highly specialized Mission IT investments. Additionally, the Agency CIO will direct Center CIOs to work with Center Directors to ensure that IT funds are used in alignment with IT priorities. In the same way, the Agency CIO will ensure that IT governance boards used for major IT decisions and investments are responsive to Mission and Center requirements. This action will be completed by May 30, 2014.

Evaluation of Management's Response. While the Administrator concurred with our recommendation, he indicated that highly specialized IT – defined by NASA as IT that is a part of, internal to, or embedded in a Mission platform – will continue to be managed by program or project managers and not be subject to approval by the Agency CIO. It is not clear to us based on this response whether the Agency will require the use of IT governance boards for all major NASA IT investments or whether it will waive this requirement for highly specialized Mission IT. We encourage the Mission Directorates to work with the Agency CIO to develop a process that increases the Agency CIO's oversight and input into all Mission IT investments to ensure that highly specialized Mission IT investments are not excluded from the Agency's IT Governance process. The recommendation is resolved and will be closed upon completion and verification that NASA's IT governance boards play a substantive oversight role in all major Agency IT investments.

Recommendation 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.

Management's Response. The Administrator concurred with our recommendation, stating that the OCIO will review and revise as necessary all board charters to improve their effectiveness. Furthermore, the OCIO will establish governance thresholds that clearly define the scope and authority of each board following the example of the Agency's governing council thresholds. Finally, the OCIO will implement a plan to increase governance awareness. The Agency plans to complete these actions within 180 days after appointment of a new Agency CIO.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

Recommendation 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.

> **Management's Response.** The Administrator partially concurred with our recommendation, stating that NASA will revise the current reporting structure to make the Agency CIO a direct report to the Administrator and revise the job title of Mission Directorate CIOs. In addition, the OCIO will work to better define the roles and responsibilities of Center and Mission Directorate CIOs. The Agency plans to complete these actions by September 30, 2013. However, the Agency declined to revise the job title of Center CIOs explaining that they have a policy-making role analogous to Center Chief Financial Officers.
>
> **Evaluation of Management's Response.** The Agency's proposed actions are responsive to our recommendations regarding the reporting relationship of the NASA CIO and the job title of the Mission CIOs. Although we believe that revising the job title of the Center CIOs would help delineate their roles and responsibilities more clearly, we acknowledge that there are other ways by which the Agency can accomplish this goal. Therefore, the recommendation is resolved and will be closed upon verification that NASA has adequately defined the roles and responsibilities of Center CIOs.

Recommendation 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.

> **Management's Response.** The Administrator partially concurred with our recommendation, stating that NASA agrees that the Mission Directorates require a principal advocate for their IT needs who is also responsive to the Agency CIO. He stated that the OCIO and Mission Directorates will work together to define the roles, responsibilities, and reporting structures of the Mission Directorate CIOs to ensure consistency and accountability. However, the Administrator declined to make the Mission Director CIOs a direct report to the Agency CIO.
>
> **Evaluation of Management's Response.** Although we continue to believe that making the Mission Directorate CIOs report directly to the Agency CIO would improve the CIO's visibility over Mission IT assets and activities, we acknowledge that there are other ways by which the Agency can accomplish this goal. Therefore, the recommendation is resolved and will be closed upon verification that the Agency has taken adequate steps to define the roles, responsibilities, and reporting structures of the Mission Directorate CIOs so as to ensure consistency and accountability.

Recommendation 8. In light of the changes recommended in this report, reevaluate the resources of the OCIO to ensure that the Office has the appropriate number of personnel with the appropriate capabilities and skill sets.

Management's Response. The Administrator concurred with our recommendation, stating that the new Agency CIO will conduct an organizational assessment to identify the resources and skill sets necessary to support the IT governance improvements and expanded responsibilities for the OCIO and Center CIO organizations. This action will be completed 180 days after a new CIO is appointed.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the proposed actions.

APPENDIX A

Scope and Methodology

We performed this audit from April 2012 through April 2013 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 accomplish our objective, we interviewed 53 individuals from both inside and outside NASA. We conducted interviews with the NASA CIO, Center CIOs, Mission Directorate CIOs, and the Agency and Center CISOs. We also surveyed the Center and Mission Directorate CIOs and CISOs to gain an understanding of each stakeholders' perspective on the current state of IT governance at NASA. Additionally, we interviewed the Associate CIO for Capital Planning and Governance, Deputy CIO for IT Reform, ACES End User Services Office, representatives from the Data-At-Rest Implementation Team, Chief of Data Center Consolidation, and representatives from the Security Operations Center to discuss the operational effectiveness of the current IT governance structure and its impact on Agency-wide initiatives.

We conducted interviews with the Department of Veterans Affairs CIO, the Department of the Interior CIO, and the United States Postal Service CISO to discuss the design of their current IT governance structure and to identify lessons learned for benchmarking purposes that relate to NASA.

Federal Laws, Regulations, Policies, and Guidance. We reviewed the following in the course of our audit work:

- 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"
- NPD 2800.1B, "Managing Information Technology," March 21, 2008
- NPR 2800.1B, "Managing Information Technology," March 20, 2009

- NPR 7120.7, "NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements," November 3, 2008
- NPD 2810.1D, "NASA Information Security Policy," May 9, 2009
- NPR 2810.1A, "Security of Information Technology," May 16, 2006
- NPD 1000.3D, "The NASA Organization with Change 37," May 25, 2012

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

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, and project approvals. The control weaknesses we identified are discussed in the Results section of this report. Our recommendations, if implemented, will correct the identified control weaknesses.

Prior Coverage

The NASA OIG has issued 10 reports of particular relevance to the subject of this report and GAO has issued 3. Unrestricted reports can be accessed at http://oig.nasa.gov/audits/reports/FY13 and http://www.gao.gov, respectively.

NASA Office of Inspector General

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

"NASA's Effort to Encrypt its Laptop Computers (Special Report, December 17, 2012)

"Review of NASA's Computer Security Incident Detection and Handling Capability" (IG-12-017, August 7, 2012)

"NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems" (IG-12-006, December 5, 2011)

"Inadequate Security Practices Expose Key NASA Network to Cyber Attack" (IG-11-017, March 28, 2011)

“Preparing for the Space Shuttle Program’s Retirement: A Review of NASA’s Disposition of Information Technology Equipment” (IG-11-009, December 7, 2010)

“Audit of NASA’s Efforts to Continuously Monitor Critical Information Technology Security Controls” (IG-10-019, September 14, 2010)

“Review of the Information Technology Security of a [a NASA Computer Network]” (IG-10-013, May 13, 2010)

“Final Memorandum of NASA’s Information Technology Capital Planning and Investment Control” (IG-06-017, September 14, 2006)

“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)

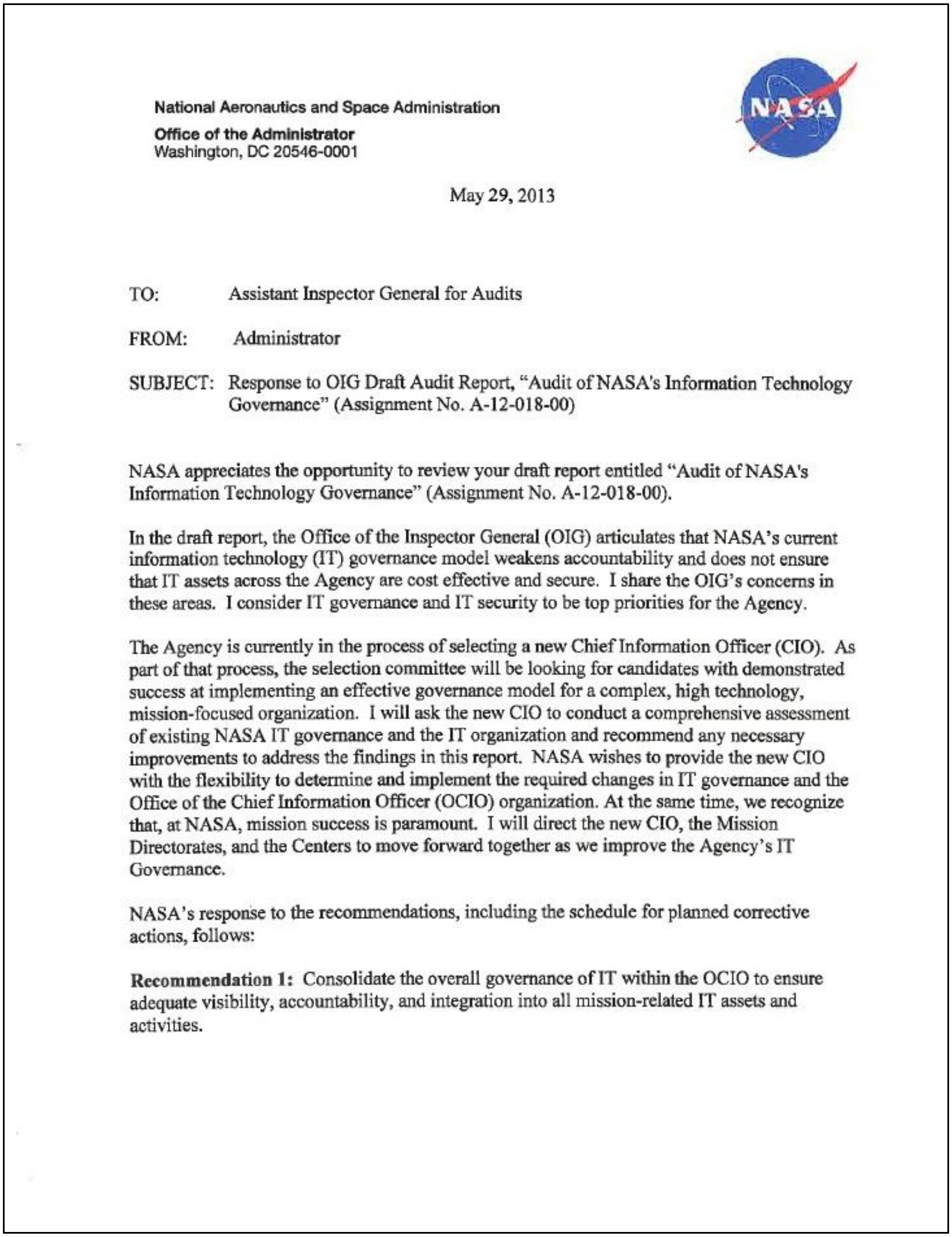
Government Accountability Office

“Information Technology: DHS Needs to Further Define and Implement Its New Governance Process” (GAO-12-818, July 25, 2012)

“Information Technology: NASA Needs to Remedy Vulnerabilities in Key Networks” (GAO-10-4, October 15, 2009)

“NASA Chief Information Officer: Opportunities to Strengthen Information Resources Management” (GAO/AIMD-96-78, August 1996)

MANAGEMENT COMMENTS



National Aeronautics and Space Administration
Office of the Administrator
Washington, DC 20546-0001

May 29, 2013

TO: Assistant Inspector General for Audits

FROM: Administrator

SUBJECT: Response to OIG Draft Audit Report, "Audit of NASA's Information Technology Governance" (Assignment No. A-12-018-00)

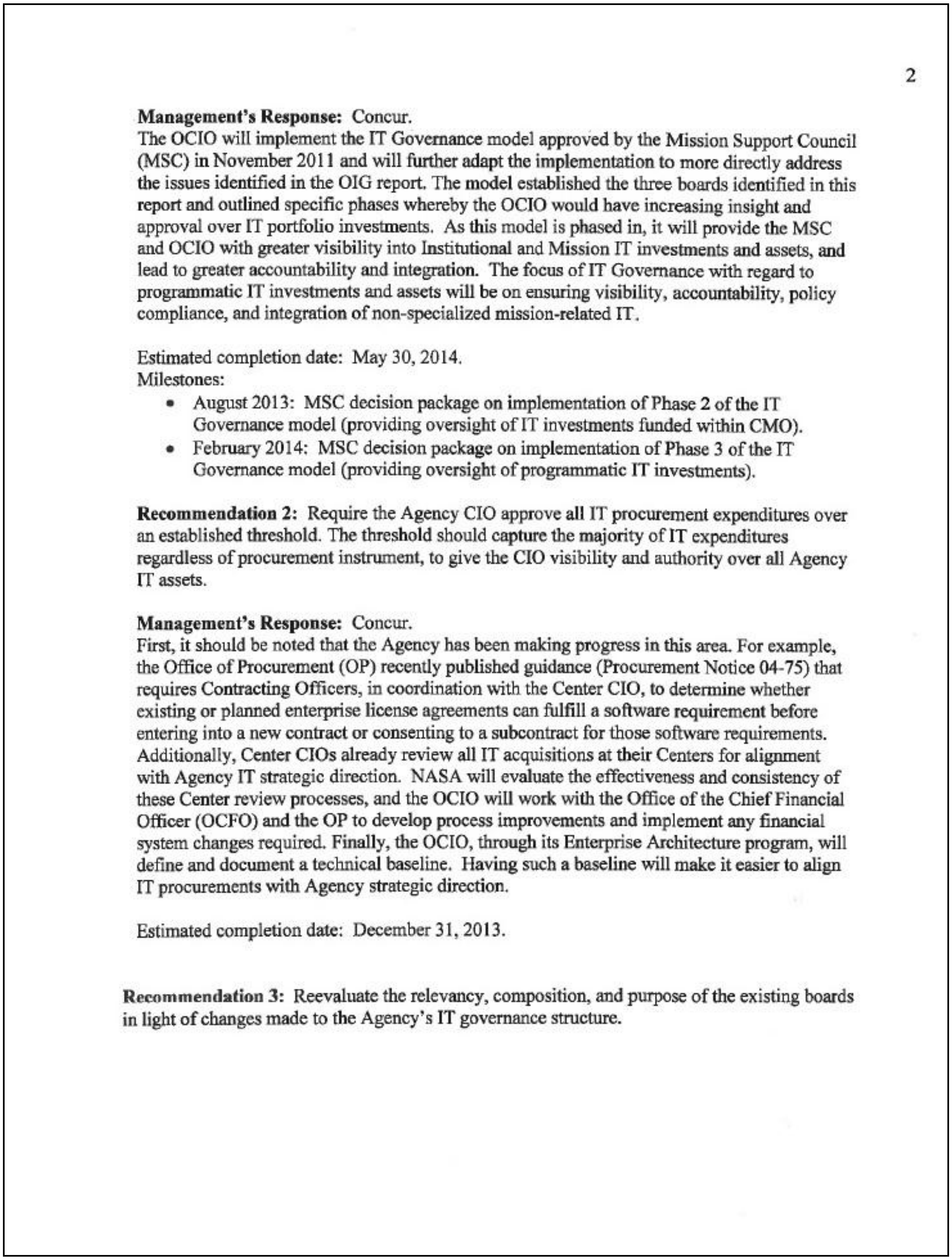
NASA appreciates the opportunity to review your draft report entitled "Audit of NASA's Information Technology Governance" (Assignment No. A-12-018-00).

In the draft report, the Office of the Inspector General (OIG) articulates that NASA's current information technology (IT) governance model weakens accountability and does not ensure that IT assets across the Agency are cost effective and secure. I share the OIG's concerns in these areas. I consider IT governance and IT security to be top priorities for the Agency.

The Agency is currently in the process of selecting a new Chief Information Officer (CIO). As part of that process, the selection committee will be looking for candidates with demonstrated success at implementing an effective governance model for a complex, high technology, mission-focused organization. I will ask the new CIO to conduct a comprehensive assessment of existing NASA IT governance and the IT organization and recommend any necessary improvements to address the findings in this report. NASA wishes to provide the new CIO with the flexibility to determine and implement the required changes in IT governance and the Office of the Chief Information Officer (OCIO) organization. At the same time, we recognize that, at NASA, mission success is paramount. I will direct the new CIO, the Mission Directorates, and the Centers to move forward together as we improve the Agency's IT Governance.

NASA's response to the recommendations, including the schedule for planned corrective actions, follows:

Recommendation 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.



Management's Response: Concur.
The OCIO will implement the IT Governance model approved by the Mission Support Council (MSC) in November 2011 and will further adapt the implementation to more directly address the issues identified in the OIG report. The model established the three boards identified in this report and outlined specific phases whereby the OCIO would have increasing insight and approval over IT portfolio investments. As this model is phased in, it will provide the MSC and OCIO with greater visibility into Institutional and Mission IT investments and assets, and lead to greater accountability and integration. The focus of IT Governance with regard to programmatic IT investments and assets will be on ensuring visibility, accountability, policy compliance, and integration of non-specialized mission-related IT.

Estimated completion date: May 30, 2014.
Milestones:

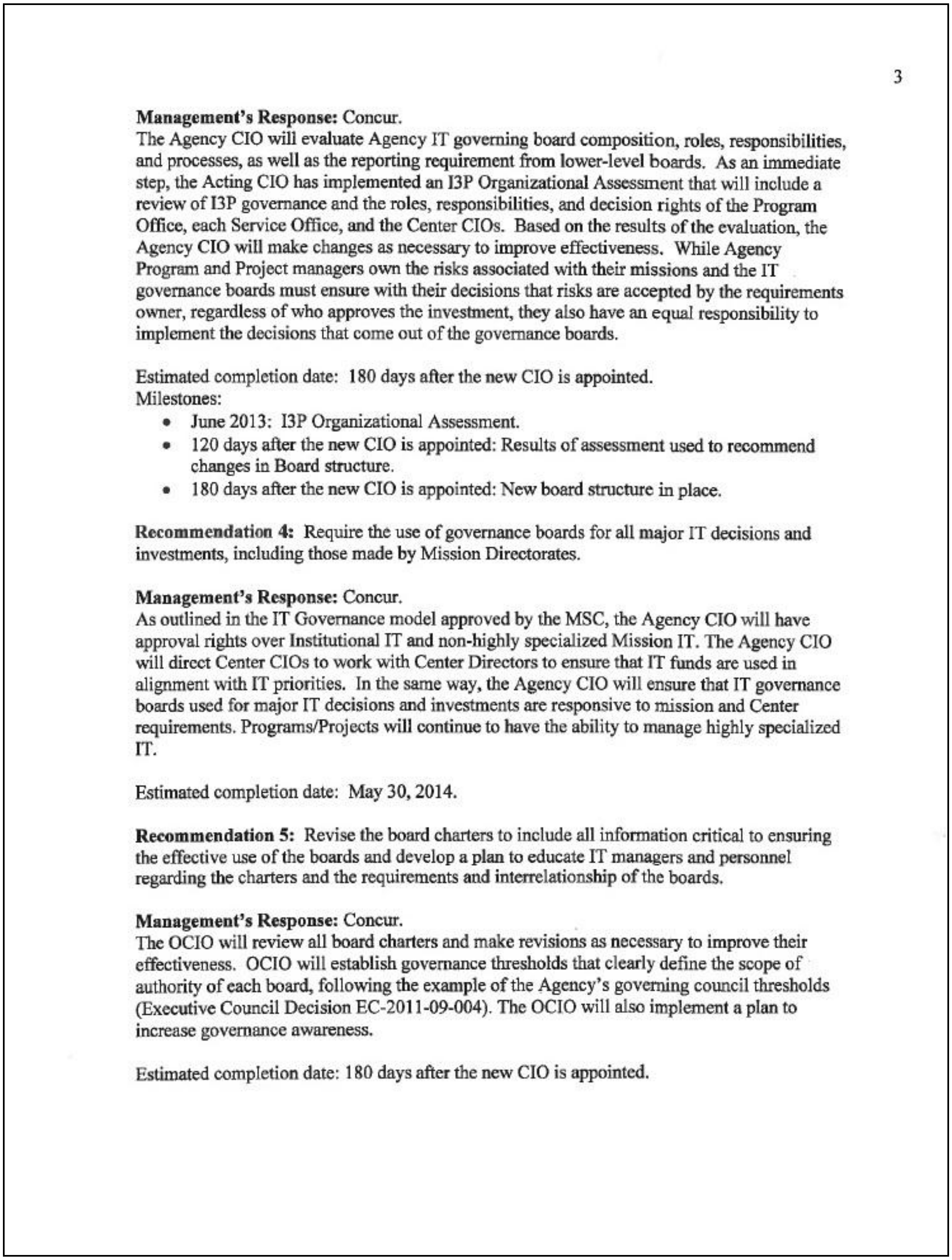
- August 2013: MSC decision package on implementation of Phase 2 of the IT Governance model (providing oversight of IT investments funded within CMO).
- February 2014: MSC decision package on implementation of Phase 3 of the IT Governance model (providing oversight of programmatic IT investments).

Recommendation 2: Require the Agency CIO 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.

Management's Response: Concur.
First, it should be noted that the Agency has been making progress in this area. For example, the Office of Procurement (OP) recently published guidance (Procurement Notice 04-75) that requires Contracting Officers, in coordination with the Center CIO, to determine whether existing or planned enterprise license agreements can fulfill a software requirement before entering into a new contract or consenting to a subcontract for those software requirements. Additionally, Center CIOs already review all IT acquisitions at their Centers for alignment with Agency IT strategic direction. NASA will evaluate the effectiveness and consistency of these Center review processes, and the OCIO will work with the Office of the Chief Financial Officer (OCFO) and the OP to develop process improvements and implement any financial system changes required. Finally, the OCIO, through its Enterprise Architecture program, will define and document a technical baseline. Having such a baseline will make it easier to align IT procurements with Agency strategic direction.

Estimated completion date: December 31, 2013.

Recommendation 3: Reevaluate the relevancy, composition, and purpose of the existing boards in light of changes made to the Agency's IT governance structure.



Management's Response: Concur.
The Agency CIO will evaluate Agency IT governing board composition, roles, responsibilities, and processes, as well as the reporting requirement from lower-level boards. As an immediate step, the Acting CIO has implemented an I3P Organizational Assessment that will include a review of I3P governance and the roles, responsibilities, and decision rights of the Program Office, each Service Office, and the Center CIOs. Based on the results of the evaluation, the Agency CIO will make changes as necessary to improve effectiveness. While Agency Program and Project managers own the risks associated with their missions and the IT governance boards must ensure with their decisions that risks are accepted by the requirements owner, regardless of who approves the investment, they also have an equal responsibility to implement the decisions that come out of the governance boards.

Estimated completion date: 180 days after the new CIO is appointed.
Milestones:

- June 2013: I3P Organizational Assessment.
- 120 days after the new CIO is appointed: Results of assessment used to recommend changes in Board structure.
- 180 days after the new CIO is appointed: New board structure in place.

Recommendation 4: Require the use of governance boards for all major IT decisions and investments, including those made by Mission Directorates.

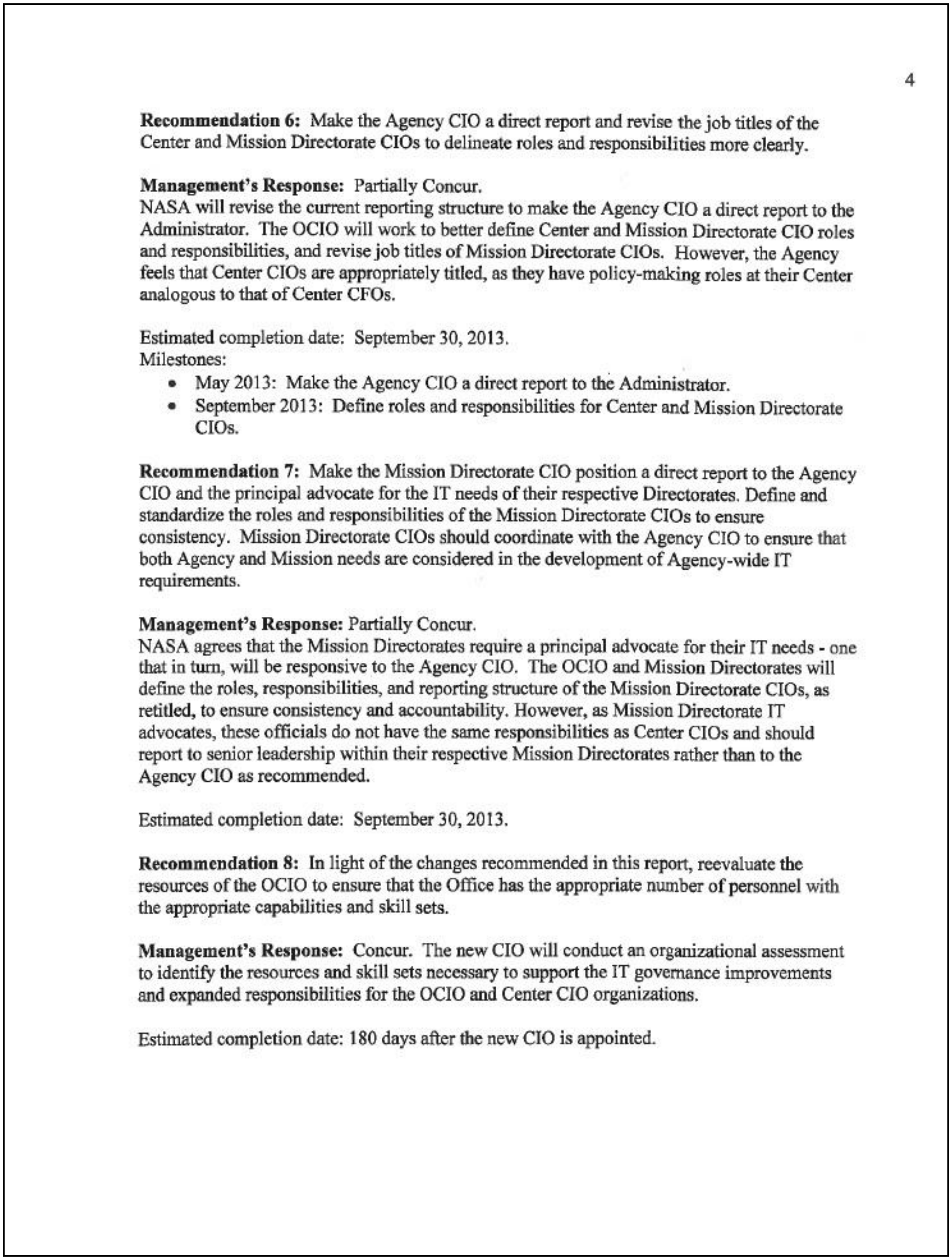
Management's Response: Concur.
As outlined in the IT Governance model approved by the MSC, the Agency CIO will have approval rights over Institutional IT and non-highly specialized Mission IT. The Agency CIO will direct Center CIOs to work with Center Directors to ensure that IT funds are used in alignment with IT priorities. In the same way, the Agency CIO will ensure that IT governance boards used for major IT decisions and investments are responsive to mission and Center requirements. Programs/Projects will continue to have the ability to manage highly specialized IT.

Estimated completion date: May 30, 2014.

Recommendation 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.

Management's Response: Concur.
The OCIO will review all board charters and make revisions as necessary to improve their effectiveness. OCIO will establish governance thresholds that clearly define the scope of authority of each board, following the example of the Agency's governing council thresholds (Executive Council Decision EC-2011-09-004). The OCIO will also implement a plan to increase governance awareness.

Estimated completion date: 180 days after the new CIO is appointed.



Recommendation 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.

Management's Response: Partially Concur.
NASA will revise the current reporting structure to make the Agency CIO a direct report to the Administrator. The OCIO will work to better define Center and Mission Directorate CIO roles and responsibilities, and revise job titles of Mission Directorate CIOs. However, the Agency feels that Center CIOs are appropriately titled, as they have policy-making roles at their Center analogous to that of Center CFOs.

Estimated completion date: September 30, 2013.
Milestones:

- May 2013: Make the Agency CIO a direct report to the Administrator.
- September 2013: Define roles and responsibilities for Center and Mission Directorate CIOs.

Recommendation 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.

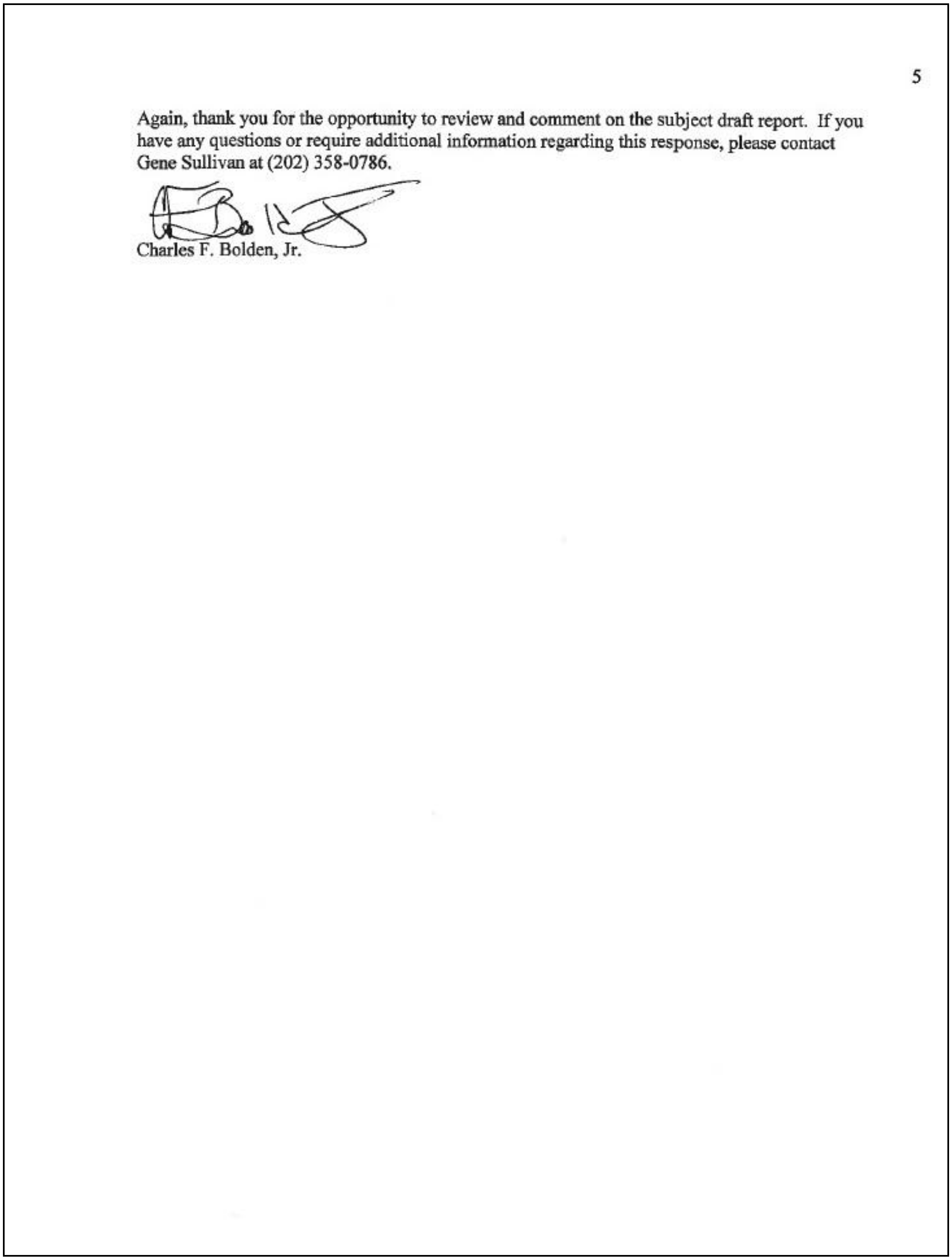
Management's Response: Partially Concur.
NASA agrees that the Mission Directorates require a principal advocate for their IT needs - one that in turn, will be responsive to the Agency CIO. The OCIO and Mission Directorates will define the roles, responsibilities, and reporting structure of the Mission Directorate CIOs, as retitled, to ensure consistency and accountability. However, as Mission Directorate IT advocates, these officials do not have the same responsibilities as Center CIOs and should report to senior leadership within their respective Mission Directorates rather than to the Agency CIO as recommended.

Estimated completion date: September 30, 2013.

Recommendation 8: In light of the changes recommended in this report, reevaluate the resources of the OCIO to ensure that the Office has the appropriate number of personnel with the appropriate capabilities and skill sets.

Management's Response: Concur. The new CIO will conduct an organizational assessment to identify the resources and skill sets necessary to support the IT governance improvements and expanded responsibilities for the OCIO and Center CIO organizations.

Estimated completion date: 180 days after the new CIO is appointed.



5

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 Gene Sullivan at (202) 358-0786.

Charles F. Bolden, Jr.

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Associate Administrator
Chief of Staff
Acting Chief Information Officer
Associate Administrator for Aeronautics Research
Associate Administrator for Science
Associate Administrator for Human Exploration and Operations
Associate Administrator for Space Technology
Associate CIO for Capital Planning and Governance
NASA Advisory Council's Audit, Finance, and Analysis Committee

Non-NASA Organizations and Individuals

- Office of Management and Budget
  - Deputy Associate Director, Energy and Science Division
    - Branch Chief, Science and Space Programs Branch
- Government Accountability Office
  - 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 Science and Space
- 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

Major Contributors to the Report:

Laura B. Nicolosi, Director, Mission Support Directorate
Raymond Tolomeo, Director, Science and Aeronautics Research Directorate
Julia K. Eggert, Project Manager
Scott A. Riggenbach, Lead Auditor
Jason D. Hensley, Auditor

JUNE 5, 2013

REPORT NO. IG-13-015

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit http://oig.nasa.gov/audits/reports/FY13/ to obtain additional copies of this report, or contact the Assistant Inspector General for Audits at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Mr. Laurence Hawkins, Audit Operations and Quality Assurance Director, at Laurence.B.Hawkins@nasa.gov or call 202-358-1543.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Audits. Ideas and requests can also be mailed to:

Assistant Inspector General for Audits
NASA Headquarters
Washington, DC 20546-0001

NASA HOTLINE

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