NASA
National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

AUDIT OF NASA'S INFORMATION TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT EFFORTS

May 24, 2018

Report No. IG-18-019

Office of Inspector General

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

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

NASA Office of Inspector General
Office of Audits

Results in Brief

Audit of NASA's Information Technology Supply Chain Risk Management Efforts

May 24, 2018

IG-18-019 (A-17-008-00)

Why We Performed This Review

Counterfeit information technology (IT) and communications products represent an increasing threat to nations, governments, and companies around the world. According to industry estimates, 1 in 10 such products sold are counterfeit, equating to approximately $100 billion in counterfeit IT products. NASA spent approximately $1.4 billion in fiscal year 2017 on computer systems, networks, and IT services used to control spacecraft, collect and process scientific data, and provide security for critical Agency infrastructure. The risk that IT and communications products entering the Agency's supply chain could be counterfeit presents a significant threat to NASA operations and could impair the Agency's ability to protect the confidentiality, integrity, and availability of its data, systems, and networks.

In March 2013, Congress directed NASA, the Departments of Commerce and Justice, and the National Science Foundation to conduct a formal assessment of "cyber-espionage or sabotage" risks before acquiring any IT or communication systems. Responding to this mandate, the NASA Office of the Chief Information Officer (OCIO) established a supply chain risk management process to identify, assess, and neutralize cyber-espionage or sabotage risks associated with counterfeit or compromised IT or communication systems that attempt to enter the Agency's supply chain. The OCIO is responsible for performing these assessments in consultation with the Federal Bureau of Investigation (FBI).

This audit examined the effectiveness of NASA's supply chain risk management efforts to protect the confidentiality, integrity, and availability of NASA data, computer systems, and networks. We performed fieldwork at NASA Headquarters, Glenn Research Center, Johnson Space Center, and Kennedy Space Center and interviewed the Agency's Deputy Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO), and other OCIO officials. We also surveyed in writing and interviewed in person Center CIOs and Mission Directorate IT representatives, and analyzed the Agency's listing of IT and communications products and services that had cleared NASA's risk assessment process. Finally, we reviewed public laws, NASA policies, prior audit reports, external reviews, and other information related to supply chain risk management.

What We Found

While NASA has improved its supply chain risk management efforts since the process was first mandated in 2013, we identified pervasive weaknesses in the Agency's internal controls and risk management practices that lead us to question the sufficiency of its current efforts. NASA's risk assessment process, when followed, often consists of a cursory review of public information obtained from Internet searches or unverified assertions from manufacturers or suppliers that the IT and communications products or services being acquired do not pose a risk of cyber-espionage or sabotage. Further, we found NASA does not consistently coordinate with the FBI in its review process. In addition, contrary to best practices the Agency's supply chain risk management practices do not require testing of IT and communication products to determine their authenticity and vulnerability to cyber-espionage or sabotage prior to their acquisition and deployment. Moreover, Agency policy excludes specific IT systems and flight hardware, such as equipment operated on the International Space Station, from risk assessment requirements. Overall, the Agency's weak controls have resulted in the purchase of non-vetted IT and communication assets, some of which we found present significant security concerns to Agency systems and data. In addition to our longstanding concerns about NASA's IT governance and security practices, the Agency compounds its security vulnerabilities by relying on ineffectual processes and information in its efforts to prevent risky IT products from entering its network environment.

What We Recommended

In order to strengthen security controls over the Agency's supply chain risk management, we recommended the NASA Chief Information Officer, in coordination with the Assistant Administrator for Procurement: (1) work with the FBI and NASA Counterintelligence Office to consistently utilize information obtained from the FBI and other Government sources to enable informed IT acquisition and risk management decisions; (2) ensure NASA's assessed and cleared listing (ACL) is updated weekly; (3) revise the NASA Procurement Class Deviation to remove language that exempts certain IT systems from the Agency's supply chain risk management review process; (4) incorporate information regarding the Agency's supply chain risk management requirements into NASA IT security training; (5) review the 7 transactions identified by the Office of Inspector General (OIG) in which IT and communication products were acquired without a supply chain risk assessment; (6) perform a comprehensive risk assessment for the 7 IT and communications products acquired outside the Agency's supply chain risk management process to determine their vulnerability to cyber-espionage and sabotage; and (7) direct all NASA Centers, Mission Directorates, and Program/Project Offices to review and strengthen their current supply chain risk management efforts to ensure only assessed and cleared IT and communications products and services enter the Agency's supply chain.

We provided a draft of this report to NASA management, who concurred with our recommendations and described planned corrective actions. We consider the proposed actions responsive for all seven recommendations and will close them upon verification and completion of those actions.

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

TABLE OF CONTENTS

Acronyms

ACL	Assessed and Cleared List
CBP	Customs and Border Protection
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FY	fiscal year
GAO	Government Accountability Office
ISO	Information System Owner
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OT	Operational Technology
RFI	Request for Investigation
SEWP	Solutions for Enterprise-Wide Procurement
SP	Special Publication
SSP	system security plan

INTRODUCTION

Counterfeit information technology (IT) and communications products represent an increasing threat to nations and economies around the world. According to industry estimates, 1 in 10 IT products sold are counterfeit, equating to approximately $100 billion in counterfeit products.[1,2] NASA spent approximately $1.4 billion in fiscal year (FY) 2017 on IT investments in computer systems, networks, and services used to control spacecraft, collect and process scientific data, and provide security for critical Agency infrastructure. The risk that IT and communications products entering the Agency's supply chain and network environment could potentially be counterfeit presents a significant threat to NASA operations and could impair the Agency's ability to protect the confidentiality, integrity, and availability of its data, systems, and networks.

In March 2013, Congress directed NASA, the Departments of Commerce and Justice, and the National Science Foundation to conduct a formal assessment of "cyber-espionage or sabotage" risks before acquiring any IT or communication systems.[3] Responding to the congressional mandate, in 2013 the NASA Office of the Chief Information Officer (OCIO) established a supply chain risk management process to identify, assess, and neutralize cyber-espionage or sabotage risks associated with counterfeit or compromised IT or communication systems that attempt to enter the Agency's supply chain. The OCIO is responsible for performing these assessments in consultation with the Federal Bureau of Investigation (FBI).

This audit examined the effectiveness of NASA's Supply Chain Risk Management efforts. Specifically, we reviewed whether NASA had implemented controls to meet Federal and Agency IT security requirements to protect the confidentiality, integrity, and availability of NASA data, computer systems, and networks. Details of the audit's scope and methodology are described in Appendix A.

Background

A 2008 criminal investigation involving counterfeit Cisco products underscored the risks posed by counterfeit IT products to the Federal Government's supply chain. In that case, the FBI identified individuals trafficking over $2 million in counterfeit Cisco routers, network switches, and Wide Area Network Interface cards that had fraudulently entered the U.S. Government's IT and communications supply chain. Such counterfeit equipment could cause immediate or premature system failures during use and could allow unauthorized access to otherwise secure computer systems. More recently, the threat of counterfeit and "gray market" IT products entering Federal IT supply chains has gained

[1] Alliance for Gray Market and Counterfeit Abatement and KPMG (2006); AGMA/KPMG White Paper: "Gray Markets: An Evolving Concern," 2016.

[2] The Computing Technology Industry Association, "IT Industry Outlook 2017," January 2017.

[3] Public Law No. 113-6, "Consolidated and Further Continuing Appropriations Act of 2013," March 26, 2013.

increasing prominence.[4] In 2016, the U.S. Customs and Border Protection (CBP) reported the seizure of 31,560 shipments of counterfeit products estimated to be worth $1.3 billion that were being shipped to the United States. According to CBP, 686 of the seizures consisted of counterfeit computers/parts estimated to be worth $19.3 million. Total counterfeit seizures reported by CBP has increased significantly since 2006, when the Agency reported 14,675 seizures of counterfeit products estimated to be worth $155.3 million. According to the Government Accountability Office (GAO), Federal IT supply chains face a variety of threats, including: (1) installation of malicious logic on hardware or software, (2) installation of counterfeit hardware or software, (3) failure or disruption in the production or distribution of a critical product or service, (4) reliance upon a malicious or unqualified service-provider for the performance of technical services, and (5) installation of unintentional vulnerabilities on hardware or software.[5,6]

In 2008, the Federal Government began implementing initiatives designed to improve cybersecurity across Federal agencies by reducing potential vulnerabilities in IT systems; protecting against intrusion attempts; and anticipating future threats through defensive, offensive, educational, research and development, and counterintelligence efforts. One of the initiatives focused on the development of a multipronged approach to global supply chain risk management.[7] According to the initiative, domestic and global supply chains risks must be managed strategically and comprehensively over a product or service's entire life cycle. To accomplish this, the initiative advised agencies that managing their supply chain risk would require:

1. A greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions.

2. The development of tools to mitigate risk across the life cycle of products from design through retirement.

3. The development of new acquisition practices that reflect the complex global marketplace.

4. Partnership with industry to adopt supply chain risk management standards and best practices.

Supply chain risk management is the process of identifying, assessing, and neutralizing risks associated with IT and communication products or services. As discussed above, the 2013 Appropriations Act directed NASA to assess the vulnerability of its IT products or services to cyber-espionage and sabotage. While Congress imposed this requirement on NASA and three other Federal agencies, it provided no additional funding or specific guidance to execute the mandate. Further, the FBI, the entity tasked with assisting agencies in assessing supply chain risks, has limited resources to support NASA's supply chain risk management efforts. Specifically, while the FBI does not have the resources to perform all vendor assessments for NASA, it has made its database containing vendor assessment data available to OCIO

[4] The black market is the trade of illegal and/or stolen goods. The white market is the trade of legitimate goods. The gray market falls somewhere in between and generally refers to a legal product bought and sold outside the manufacturer's authorized trading channels.

[5] GAO Testimony, "IT Supply Chain: Additional Efforts Needed by National Security- Related Agencies to Address Risks," March 27, 2012.

[6] Malicious Logic is hardware, firmware, or software that is intentionally included or inserted into a system for a harmful purpose.

[7] Comprehensive National Cybersecurity Initiative #11, "Develop a multi-pronged approach for global supply chain risk management," January 2008.

staff responsible for supply chain risk assessments. However, much of the investigative information in the FBI database is classified or law enforcement sensitive and cannot be publicly released, thereby complicating NASA's efforts to use the information to help remove itself from ongoing vendor agreements.

These reasons, coupled with the size of NASA's enterprise network and number of associated systems, make supply chain risk management an enormous undertaking for the Agency. Under Federal guidance issued by the National Institute of Standards and Technology (NIST), information systems are classified at a low, moderate, or high impact security level. A security impact level is considered "low" when the loss of confidentiality, integrity, or availability could be expected to have a "limited" adverse effect on organizational operations, assets, or individuals. A security impact level is "moderate" when the loss could be expected to have a "serious" adverse effect and "high" when the loss could be expected to have a "severe or catastrophic" adverse effect.[8] NASA currently operates over 400 individual computer networks and systems to support its varied missions, of which more than 25 are classified as high impact systems under Federal guidelines while more than 290 are deemed moderate impact.

The Agency developed its supply chain risk management process as a collaborative effort among NASA end users, the OCIO, and Center procurement and information security officials after the requirement to assess IT and communication products and services took effect in March 2013. To help facilitate the risk assessment process, NASA developed a "request for investigation" (RFI) form to initiate a request to purchase IT and communication products or services.[9] As of June 2017, the NASA OCIO had processed over 1,600 RFIs from IT personnel at NASA Centers who are responsible for performing supply chain risk management efforts. Of the over 1,600 requests processed, the Agency denied 233 or approximately 15 percent, often citing issues such as missing or incorrect information on the RFI or the product having been manufactured in China.

Federal Information Security Requirements

In response to growing national security concerns, the Federal government developed a series of requirements to help agencies address the reality of a growing global marketplace and the increased risks to their IT and communication supply chains. Because NASA uses commercially supplied IT products and services to operate its complex information systems and networks, a comprehensive supply chain risk management process integrated into the Agency's overall IT security planning and acquisition efforts is needed to provide the first line of defense against malicious actors. Among other requirements, NASA must meet standards imposed by the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) directives, and NIST controls. Each of these requirements is detailed below.

Federal Information Security Modernization Act of 2014

FISMA requires agencies to provide information security protections commensurate with the risks and magnitude of the harm that could result from unauthorized access, disclosure, modification, or destruction of Agency information. The requirements imposed by FISMA seek to help ensure information security management is integrated into agency IT operations and practices.

[8] National Institute of Standards and Technology Federal Information Processing Standards Publications (FIPS PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

[9] Request for Investigation /IT Product Source Assessment Waiver form (NF1823).

Further, agencies are required to perform periodic assessments of their IT security risks and the processes that support the protection of IT operations and assets across the agency. In addition, agencies are required to implement policies that ensure information security is addressed throughout the life cycle of each agency information system. Finally, Agency information systems must undergo at least annual testing and evaluation of the effectiveness of information security.

FISMA also requires agencies to develop agency-wide security awareness training to inform personnel – to include contractors and other users of their information systems – of the need to comply with agency policies designed to reduce information security risks.

Office of Management and Budget Directive

In 2016, OMB revised Circular A-130 to reflect changes in law and advances in technology.[10] As a result, OMB required Federal agencies to develop supply chain risk management plans as described in NIST Special Publication (SP) 800-161 to ensure the integrity of information systems throughout the system development life cycle.[11] Consequently, to improve NASA's supply chain risk management capabilities, the Agency must address the following six requirements:

- Consider supply chain security issues in all resource planning and management activities throughout the system development life cycle;
- Analyze risks (including supply chain risks) associated with potential contractors and the acquisition of IT and communication products and services they provide;
- Allocate risk between the Government and contractor when acquiring IT and communication products and services;
- Develop, implement, document, maintain, and oversee agency-wide information security and privacy programs;
- Implement supply chain risk management principles to protect NASA against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle; and
- Develop supply chain risk management plans as described in NIST SP 800-161 to ensure the integrity, security, resilience, and quality of information systems.

National Institute of Standards and Technology

Since 2009, NIST has emphasized the need for Federal information systems and their related components to be protected throughout their entire life cycle – that is, during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and ultimately retirement.[12] To assist Federal agencies in mitigating supply chain risks, NIST developed guidance and enhanced IT security controls to assist agencies with acquisition strategies, tools, and methodologies for purchasing and testing IT and communication products and services prior to them entering the Agency's network environment. These enhanced controls, when incorporated into agency

[10] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," December 29, 2015.

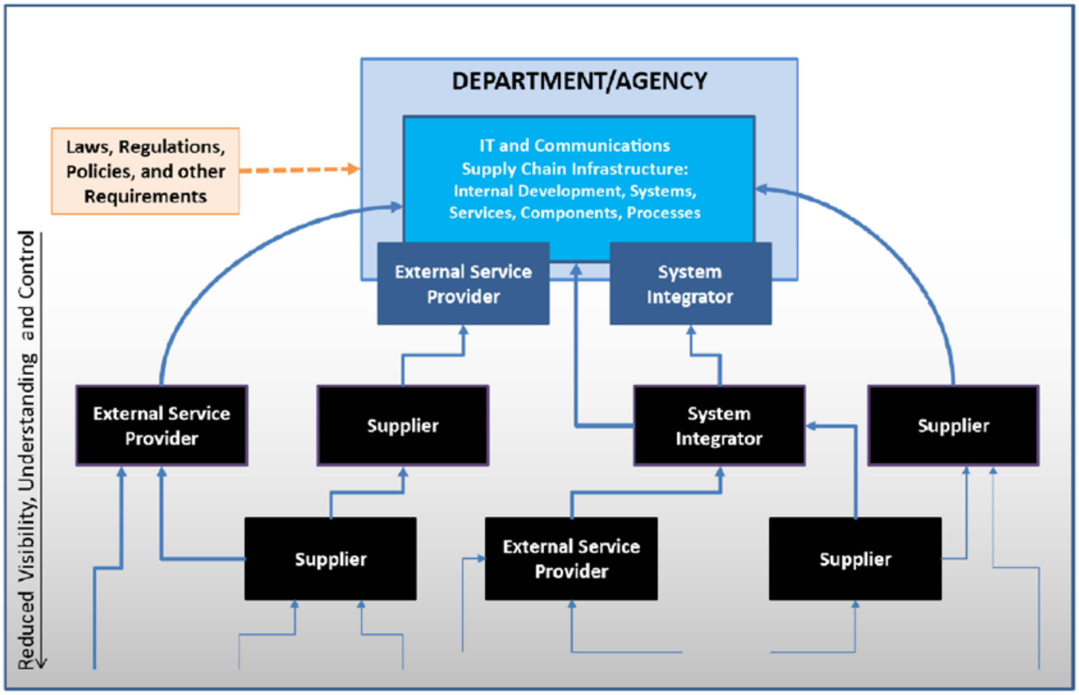
[11] NIST SP 800-161 Guidance, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," April 2015.

[12] NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

information system security plans, provide an assessment of supply chain risks, enabling management to effectively research, identify, and assess the security, integrity, and quality of IT and communication products or services being purchased. NIST also recommends agencies consider creating incentives for suppliers who, for example, implement specific security safeguards or promote transparency into their organizational processes and security practices.

According to NIST, the IT and communication supply chain contains an integrated set of components (hardware, software, and related processes) within an agency that composes the environment in which a system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned.[13] Figure 1 depicts a typical Federal agency's IT and communications supply chain that consists of multiple layers of system integrators, external service providers, and suppliers.

Figure 1: Federal Agency IT and Communications Supply Chain


DEPARTMENT/AGENCY
Laws, Regulations, Policies, and other Requirements
IT and Communications Supply Chain Infrastructure: Internal Development, Systems, Services, Components, Processes
External Service Provider
System Integrator
External Service Provider
Supplier
System Integrator
Supplier
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

Source: NIST SP 800-161.

In addition, NIST promotes best practices for effective IT supply chain risk management, to include:

- Implementing a formal risk management process, including an organization-wide risk methodology for conducting IT and communications risk assessments;
- Establish a formal governance structure that integrates IT and communications supply chain risk management requirements and incorporates these requirements into Agency policies;
- Ensure adequate resources are allocated to information security and IT and communications supply chain risk management to ensure proper implementation of guidance and controls;

[13] NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," April 2015.

- Develop and implement consistent, well-documented, repeatable processes for system engineering, IT and communications security practices, and acquisition; and

- Establish internal controls to assure compliance with security and quality requirements.

Governance over Supply Chain Risk Management

For supply chain risk management to be effective, agencies must exercise strong IT governance practices, including organizational oversight over the acquisition, security, and use of IT and communication products and services. Without such controls in place, agencies increase the risk of introducing IT and communications products or services into their network environments that could compromise their systems and data.

Establishment of NASA's Supply Chain Risk Management Process

Even before 2013's congressional supply chain risk management directive, NASA performed information system security assessments pursuant to FISMA, NIST guidance, and Agency policies. However, the NASA Office of Inspector General (OIG) previously identified concerns with the sufficiency of these efforts, including how the Agency addressed material risks to its supply chain. Further, NASA Information System Owners (ISO) were responsible for determining the security categorizations of their systems and ensuring they adhered to Federal IT requirements for Low, Moderate, or High potential impacts on Agency missions, assets, legal responsibilities, functions, or individuals, although little was done to ensure the integrity of IT and communications products or their respective supply chains.[14]

In response to the 2013 mandate, the NASA OCIO established a supply chain risk management work flow with the goal of performing risk assessments of IT and communications products and services prior to their purchase and deployment into the Agency's network environment. In addition, the Agency developed an Assessed and Cleared List (ACL) of IT and communications products and services that have cleared the Agency's risk assessment process to enter NASA's supply chain and network environment. Inclusion of a specific product or service on NASA's ACL would determine whether an RFI was necessary prior to acquisition. NASA's current ACL includes over 1,400 IT and communication products and services ranging from specific computers to the blanket approval of all products from companies like Cisco Systems, Dell, and Hewlett Packard meaning any products or service regardless of make or model produced by those companies are cleared to enter the Agency's supply chain.

In June 2013, NASA provided Congress with a draft proposal outlining the Agency's plan for implementing the requirements of the 2013 mandate. The proposal committed NASA to updating the ACL on a weekly basis, completing the Agency's final supply chain risk management framework and guidance by July 2013, and integrating counterintelligence information into its risk management process. NASA also committed to providing Congress with quarterly reports describing any reviews and assessments performed as well as the corresponding determinations made pursuant to the 2013 mandate.

[14] NIST FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

NASA Supply Chain Risk Management Standards

While the NASA OCIO has issued numerous policy directives, requirements, handbooks, and memoranda regarding information security, it has not issued guidance specifically addressing IT supply chain risk management procedures. In 2016, NASA's Office of Procurement issued a Procurement Class Deviation that provided supply chain risk management guidance to Agency contracting officers and purchase card holders as part of its discussion on restrictions when acquiring moderate or high-impact IT systems.[15] The Deviation also contained information about security-related contract clauses that may be included in solicitations or contracts for the acquisition of IT and communication products and services.[16,17] Lastly, the Deviation further defined moderate or high-impact IT systems by categorizing items such as embedded IT (used as an integral part of another product), flight hardware (including equipment operated on the International Space Station), and prototypes used to test, troubleshoot, and refine air and spacecraft hardware and software that does not fall within the definition of an IT system.[18]

Prior Office of Inspector General Audits

Over the last 7 years, the OIG has issued over 30 audit reports containing more than 100 recommendations designed to improve the Agency's IT security, including two audits specifically addressing NASA's IT governance.[19] Specifically, our 2017 audit of NASA's IT governance found that the OCIO's insight into and control over the bulk of the Agency's nearly $1.4 billion annual IT spending remains limited, with the Mission Directorates and Centers controlling $739 million (53 percent) and $311 million (22 percent), respectively, in FY 2017. The audit found that the OCIO has made insufficient progress to improve NASA's IT governance since our 2013 review, casting doubt on the office's ability to effectively oversee the Agency's IT investments. In addition, we found the OCIO continues its decade-long struggle to establish an effective enterprise architecture and that its current iteration is immature.

Our FY 2017 FISMA review noted that information security remains a significant challenge for NASA.[20] Specifically, the audit found that while NASA continues to make progress in implementing IT security initiatives, its cybersecurity program remains ineffective when evaluated against OMB's model that requires agencies to achieve a maturity level of 4 (on a 1-5 scale) to be considered effective. This year, NASA achieved a maturity level of 2 in the five functional areas examined, indicating the Agency's information systems remain vulnerable to serious security threats.

[15] NASA Procurement Class Deviation 15-03A, April 28, 2016. At NASA, Procurement Class Deviations are deviations from established FAR requirements deemed necessary by the Agency and approved by the Assistant Administrator for Procurement.

[16] NASA Federal Acquisition Regulation (FAR) Supplement 1852.239-73, "(Deviation), Review of the Offeror's Information Technology Systems Supply Chain," April 2016.

[17] NASA FAR Supplement 1852.239-74, "(Deviation), Information Technology System Supply Chain Risk Assessment," April 2016.

[18] NASA Federal Acquisition Regulation Supplements 1839 and 1852.

[19] NASA OIG, "NASA's Information Technology Governance," (IG-13-015, June 5, 2013) and "NASA's Efforts to Improve the Agency's Information Technology Governance," (IG-18-002, October 19, 2017).

[20] NASA OIG, "Final Memorandum, Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation (IG-18-003, November 6, 2017).

In a February 2017 report on the security of NASA cloud computing, we found that several of the cloud services in use at the Agency lacked authorizations to operate, were not covered by an IT system security plan, and had not been tested for appropriate security controls. We also identified numerous instances in which Agency personnel acquired cloud services using contracts that lacked provisions to address key business and IT security risks associated with cloud environments. As a result, we found that NASA needed to continue strengthening its risk management and governance practices to safeguard its information.[21]

Similarly, in a February 2017 report on industrial control system security at NASA, we found that the Agency had not developed a centralized inventory of Operational Technology (OT) systems or established a standard protocol to protect systems that contain OT components. We also found that NASA lacked an integrated approach to managing cyber security risks associated with critical infrastructure. Finally, we noted that the Agency had inadequate guidance and oversight, coupled with insufficient funding and record keeping that limited visibility over critical infrastructure protection processes, which impaired the Agency's ability to protect vital critical infrastructure assets.[22]

[21] NASA OIG, "Security of NASA's Cloud Computing Services," (IG 17-010, February 7, 2017).

[22] NASA OIG, "Industrial Control System Security Within NASA's Critical and Supporting Infrastructure," (IG-17-011, February 8, 2017).

Weaknesses in NASA's Supply Chain Risk Management Place Agency Data, Systems, and Networks at Risk

While NASA's supply chain risk management efforts have improved since the process was first mandated in 2013, we identified pervasive weaknesses in the Agency's internal controls and risk management practices that lead us to question the sufficiency of its current efforts. NASA's risk assessment process, when followed, often consists of a cursory review of public information obtained from Internet searches or unverified assertions from manufacturers or suppliers that the IT and communications products or services being acquired do not pose a risk of cyber-espionage or sabotage. Further, we found NASA does not consistently coordinate with the FBI in this review process. In addition, the Agency's supply chain risk management practices do not require testing of IT and communication products to determine their authenticity and vulnerability to cyber-espionage or sabotage prior to their acquisition and deployment. Moreover, Agency policy excludes specific IT systems and flight hardware, such as equipment operated on the International Space Station, from risk assessment requirements. Overall, the Agency's weak controls have resulted in the purchase of non-vetted IT and communication assets, some of which we found present significant security concerns to Agency systems and data. In addition to our ongoing concerns over NASA's IT governance, the sufficiency of Agency IT security practices, and the OCIO's limited visibility into Agency-wide IT purchases, NASA further compounds its security vulnerabilities by relying on ineffectual supply chain risk management processes and information to prevent risky IT products from entering its network environment.

NASA Internal Control Process Fails to Adequately Address Supply Chain Risk

Changes to NASA's risk assessment practices developed in response to the 2013 mandate remain immature four years after implementation; consequently, NASA continues to rely on pre-existing internal control processes to mitigate supply chain risks and protect its network environment. Further, the Agency's existing policy does not incorporate current supply chain risk management processes or requirements, and the policy appears to contradict, in part, the intent of the mandate.

NASA Has Limited the Scope and Impact of Supply Chain Risk Management

Too often, NASA's current supply chain risk assessment practices rely solely on a cursory review of public information obtained from Internet searches or on assertions from manufacturers or suppliers that the IT and communications products being purchased does not contain components produced, manufactured, or assembled by entities identified by the U.S. Government as posing a risk of cyber-espionage or sabotage. The initial review of public-facing information confirmations from manufacturers and suppliers is performed by Center-based supply chain risk management representatives in advance of the RFI being sent to Headquarters for final review and approval. The Centers' current risk assessment practices do not require testing of IT and communication products or services to determine their authenticity and vulnerability to cyber-espionage or sabotage. Further, NASA has made little effort over the past 4 years to utilize FBI information in its risk assessment process as required by the 2013 mandate. The few times NASA has engaged with the FBI on these issues, NASA was not able to fully incorporate the information it received into its overall risk assessment process due to the sensitivity of the information. Moreover, because these risk assessments typically occur concurrent with the procurement process, the Agency is often too far along in the process to cancel the procurement without conveying a clear justification to the vendor, a justification that may only be supported by law enforcement sensitive information that is not publicly releasable.

Ideally, products sought to be acquired by the Agency would go through the supply chain risk assessment process prior to initiating the acquisition. However, OCIO officials explained that time-sensitive procurements need to proceed concurrently with the risk assessment process. From time to time, instances have arisen where an asset already deployed on the network was later identified as a security risk. However, according to OCIO officials, replacing the product is not often an option due to funding restraints so the Agency attempts to mitigate the risks through other controls or processes.

Limited Policy Appears to Contradict Congressional Intent

NASA security officials have issued limited guidance addressing supply chain risk management. For example, while the OCIO has established numerous policies related to information security, the Office has not issued guidance specifically addressing IT and communications supply chain risk management requirements. However, NASA's Assistant Administrator for Procurement – the Agency's senior official responsible for adherence to the Federal Acquisition Regulation – issued a Procurement Class Deviation in 2016 that addresses supply chain risk management requirements for Agency contracting officers and purchase card holders when acquiring moderate or high-impact IT systems.[23,24,25] While this guidance is helpful, the Deviation exempts a large segment of IT and communications products from review based on NASA's definition of an IT system.

[23] The Federal Acquisition Regulation is the primary regulation that guides Federal Executive agencies in their acquisition of supplies and services.

[24] At NASA, Procurement Class Deviations are deviations from established FAR requirements deemed necessary by the Agency and approved by the Assistant Administrator for Procurement.

[25] NASA Procurement Class Deviation 15-03A, April 28, 2016. NASA originally issued this same guidance through Procurement Information Circulars 15-03, 14-03, and 13-04.

The Deviation excludes the following:

1. Systems acquired by a contractor incidental to a contract and not directly charged to the contract, such as a contractor's payroll and personnel management system;

2. Systems that do not process NASA information, i.e., any data collected, generated, maintained, or controlled on behalf of the Agency;

3. Imbedded IT that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where IT is integral to its operation are not considered IT systems;

4. Services in support of IT systems, such as help desk services; and

5. Flight hardware, including aircraft, spacecraft, artificial satellites, launch vehicles, balloon systems, sounding rockets, on-board instrument and technology demonstration systems; equipment operated on the International Space Station; and prototypes and engineering or brass boards created and used to test, troubleshoot, and refine air- and spacecraft hardware, software and procedures.[26]

In our view, exclusions 3 and 5 above create a narrower definition of an "IT system" compared to the definition in the 2013 mandate. Specifically, the Act states that none of the funds appropriated or otherwise made available under the Act may be used to acquire any information technology unless an assessment of any associated risk of cyber-espionage or sabotage including any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China has been performed. Our review of NIST definitions of "Information System" and "Information Technology" leads us to conclude that it was not the intent of the legislation to exclude such critical components as imbedded IT, where such technology is integral to the system or component's operation. Further, the NASA Administrator or his designee (in this case, the Assistant Administrator for Procurement) may not issue a FAR deviation that contradicts express provisions of an applicable statute. The FAR is intended to implement and at times interpret Federal acquisition statutes but cannot overrule a statute. Thus, where a FAR provision (or in this case a FAR Deviation) is contrary to an applicable statute, it is invalid.

When we raised this matter during the audit, NASA OCIO and procurement managers explained the Deviation was not intended to exclude any IT systems from review; rather, in their view the systems already undergo a thorough review through existing procurement, security, and mission operational practices and as such any supplemental review provided through the supply chain risk management process would result in a duplication of efforts. However, these officials were unable to explain what specific activities are performed that equate to an adequate risk assessment. Further, given the weaknesses identified during our prior audits, we are concerned that reliance on existing information security controls without implementing a comprehensive supply chain risk management program could unnecessarily expose NASA data and networks to risk of cyber-espionage or sabotage.

[26] A brass board is an experimental or demonstration test model intended for field testing outside the laboratory environment.

Centers Develop Guidance but Lack Training

In the absence of guidance from the NASA OCIO about conducting supply chain risk assessments, several NASA Centers developed their own guidance and established intranet websites to disseminate information about supply chain risk management requirements. Specifically, Langley Research Center and Armstrong Flight Research Center both issued formal policies governing supply chain risk management requirements for their Centers, while Glenn Research Center and Goddard Space Flight Center both maintain Center-wide intranet websites that contain supply chain risk management information and guidance to help Center employees understand the requirements for acquiring IT and communications products and services. We consider these policies and intranet websites examples of best practices even though their impact is limited to individual Centers rather than Agency-wide.

Although several Centers have developed guidance for managing the supply chain risk assessment process, Center personnel we spoke with who are responsible for supply chain risk management expressed concern about their lack of formal training. Specifically, these personnel told us that training was minimal at best and did not specifically address their responsibilities for performing their supply chain risk management duties. One employee we spoke with expressed his apprehension in his role, citing the lack of training, his engineering background, and lack of knowledge about specific IT risk management concerns. In addition, while purchase card holders receive training regarding supply chain risk management requirements surrounding IT procurements, the Agency's annual mandatory IT security training for all employees fails to address supply chain risk management requirements or responsibilities. Given the Agency's responsibility to conduct IT supply chain risk assessments, developing detailed guidance and providing training on that guidance are key controls to help protect the Agency's networks and assets from harm.

Minimal Interaction with FBI

During our review, we found that NASA had only minimal interaction with the FBI concerning supply chain risk assessments even though the Agency is required by law to use the organization as a resource for vetting IT vendors and products. According to NASA officials, one of the key factors discouraging coordination are limitations on the use of FBI intelligence.

According to the 2013 mandate, none of the funds appropriated or otherwise made available under the Appropriations Act were to be used by NASA to acquire a high-impact or moderate-impact information system, as defined for security categorization in the NIST Federal Information Processing Standard Publication 199, ''Standards for Security Categorization of Federal Information and Information Systems'' unless the Agency performed specific risk assessment processes to include:

1. Reviewing the supply chain risk from the presumptive awardee against available and relevant threat information provided by the FBI and other appropriate agencies; and

2. In consultation with the FBI or other appropriate Federal entity, conducting an assessment of any risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured, or assembled by one or more entities identified by the United States Government as posing a cyber-threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China.

As of July 2017, NASA had engaged with the FBI less than 10 times since 2013 to discuss supply chain concerns despite having processed over 1,600 RFIs during that same period. Agency officials told us that the classified and law enforcement sensitive nature of the information the FBI makes available to NASA to assist in risk assessments impairs the Agency's ability to disclose specific reasons why a vendor or product may not be suitable for NASA procurement. For example, Agency officials learned from the FBI that security software from Kaspersky had vulnerabilities that could be exploited. In response to an Agency-wide data call, NASA identified over 1,000 instances of the software deployed in the Agency's network environment.[27] However, the Agency could not officially disclose the information because of its classified nature and continued to use the software until intelligence community officials publicly expressed concerns regarding the vendor.

Further, because the Agency's supply chain risk assessment is often performed concurrently with the procurement process, NASA is at times too far along in the process to cancel the procurement without conveying to the vendor or supplier a clear reason for its withdrawal. As such, the Agency does not consistently utilize FBI information in its risk assessment process. In our view, to meet the intent of the mandate NASA should not move forward with an IT-related procurement without first having obtained and reviewed relevant supply chain information.

Assets Elude Risk Assessment Process

A major challenge facing Federal agencies in today's interconnected world is the identification of "shadow IT" or IT on an agency's network that the CIO or Chief Information Security Officer did not purchase or authorize for use. Often purchased using a government credit card and downloaded directly through a web browser, employees can acquire IT and communication products or services that could be counterfeit, tampered with, or otherwise vulnerable to cyber-espionage and sabotage without the involvement or awareness of the information system owner or information system security officer. Acquisition of IT and communication products or services that have not been cleared by the OCIO may expose NASA data, systems, and networks to significant risks, including loss, theft, or destruction of Agency data and networks.

To examine this potential vulnerability, we tested 36 IT procurements to determine whether Agency IT security officials were aware of and had approved use of the items.

Testing of Select IT Purchases

During the audit, we reviewed a judgmentally selected sample of 18 IT and communication products acquired and deployed into the Agency's network environment between January 2013 and June 2017, including 9 purchase card transactions and 9 transactions from NASA's Solutions for Enterprise-Wide Procurement (SEWP) contract.[28] The audit sample was based on several criteria, to include a range in value of purchases and purchase methods, and focused on equipment that posed particular vulnerability to the supply chain. We found 7 of the 18 IT and communication products (41 percent) totaling $142,875 entered the Agency's network environment without undergoing the required supply chain risk review and approval process. We examined these 7 transactions to determine whether the products were supported by a completed RFI or were listed on the ACL before they were acquired and found that

[27] According to Agency officials, the number of instances identified could relate to multiple computer systems with one IP address or multiple IP addresses on one system.

[28] The NASA SEWP (Solutions for Enterprise-Wide Procurement) consists of over 140 pre-competed prime contract holders, including more than 110 small businesses that provide IT products and services for Federal agencies and their approved contractors.

none were identified on either of the listings. Upon deeper examination (including accessing law enforcement information), 4 of the 7 purchases identified suppliers that raised potential red flags, to include a Chinese technology company of concern (we subsequently notified the Agency of this concern during the audit). The acquisition and deployment of IT products that have not been assessed or cleared to enter the Agency's supply chain and network environment, and without approval from the Chief Information Officer, presents a material threat to NASA's data, systems, and networks, because the Agency is unable to determine whether the products are counterfeit, free from malicious computer code, or other issues that could place the product at risk to cyber-espionage or sabotage.

In addition to the security implications of these questionable transactions, we are concerned that the purchase of at least one of these items – the IT product from the Chinese technology company – violated the intent of the 2013 law and constitutes, in our view, an Anti-Deficiency Act violation. Further, given the high percentage of unallowable costs identified in our small sample, we are concerned that additional, questionable purchases likely exist in the universe of Agency purchase card transactions.[29] See Appendix C for a complete list of the questioned costs identified.

System Security Plan Testing

We also selected 18 IT and communications products from NASA's list of RFIs for substantive testing. These products were examined in NASA's risk assessment process and were approved entry into NASA's supply chain and network environment. As part of our detailed testing, we selected a sample of IT controls that NIST classifies as "directly relevant" to supply chain security such as Developer Security Testing and Evaluation (SA-11) and Supply Chain Protection (SA-12), including 13 information security controls from the Systems and Services Acquisition control family. We reviewed these controls to determine whether they were included in the information system security plans (SSP) on NASA's RFI form.[30] For the 18 IT and communications products reviewed, we received 14 system security plans; 2 other products selected were identified as having a "low" system categorization and were subsequently not associated with specific SSPs. For the 2 remaining IT and communications products selected, we did not receive their associated SSPs despite multiple requests.

Of the 14 system security plans reviewed, 10 were missing one or more of the information security controls identified by NIST as needed for the effective mitigation of supply chain risks and threats. While NASA's system security plans include many NIST-recommended controls, the 13 controls considered by NIST to be relevant for supply chain risk management were not present within the SSPs and NASA officials could not explain why these controls were not specifically addressed. A well-crafted SSP should help protect NASA's network environment and data by incorporating administrative, technical, and physical standards and guidance for information security controls for the cost-effective security and privacy of data in Federal information systems. A description of the recommended System and Services Acquisition Control Family and Enhancement controls for supply chain risk management can be found in Appendix B.

[29] Because our sample was judgmentally selected, we cannot project the results to the total universe of transactions. That said, the findings may be indicative of additional transactions of concern.

[30] NIST defines an SSP as a formal document prepared by information system owners that provides an overview of the information security requirements and describes security controls established or planned to meet these requirements.

Finally, of the 18 IT and communications products tested, we found inaccuracies and missing information in each of the RFIs reviewed, including 12 missing information in required data fields. Accurate and complete RFI information is necessary to ensure that appropriate determinations on vendor risk are made so that products of concern do not enter NASA's supply chain and network environment. Additionally, we were unable to trace 11 of the RFIs to the specific procurement vehicles used to acquire the IT products to ensure the contracts contained required IT security information. Further, 18 of the 36 total transactions tested that were acquired using Agency purchase cards or through NASA's SEWP contract were governed by the standard terms of agreement between NASA and the vendor and do not contain any FAR or NASA provisions governing information security requirements.

During our discussion of the issues and findings identified during the audit, OCIO personnel acknowledged that certain IT and communication products or services might escape the supply chain risk assessment process and enter the Agency's network environment without the appropriate clearance. However, OCIO personnel told us these risks are mitigated by existing information security controls and practices, including the scanning of Agency networks for vulnerabilities and the monthly review of purchase card transactions by Agency staff to ensure IT and communication products or services are not being acquired without undergoing the supply chain risk assessment. In our view, these mitigation activities are occurring once the assets are already on the network, placing the Agency's data and systems at risk. Further, as our testing has shown, the Agency has not been successful in independently identifying these unapproved purchases outside the supply chain process.

The threats to NASA data, systems, and networks are not limited to unapproved or unauthorized IT and communications products and services. During our audit, NASA officials identified an instance where a computer router included on the Agency's ACL was deployed into NASA's network environment and subsequently was found to be counterfeit after the device failed and Agency representatives filed warranty claims with the manufacturer.[31] In another instance, a computer router connected to a classified NASA network was subsequently identified by the manufacturer as having issues regarding the device's country of origin. While the device was not deemed counterfeit, it was identified as having previously been sold in another country, thereby interrupting the chain of custody and presenting potential "gray market" concerns. In light of these examples, strengthening internal and information security controls over supply chain risk management is an important tool to help protect NASA's networks against counterfeit or suspicious products.

[31] A router is a network device that forwards data from one computer network to another.

CONCLUSION

As the globalization of vendors and suppliers of IT and communications products and services continues to expand, so do the risks and vulnerabilities associated with counterfeit or sabotage products entering Federal supply chains. While NASA's supply chain risk management efforts have improved since 2013, weaknesses in the Agency's IT risk management and governance practices continue to impede NASA's progress in establishing secure IT and communications product and service supply chains. Moreover, these weaknesses place Agency information, systems, and networks at risk. With NASA's increasing use of commercially-supplied IT and communications products and services, it is imperative the Agency strengthen its supply chain risk management and assessment practices to safeguard its data, systems, and networks.

Recommendations, Management's Response, and Our Evaluation

To strengthen security controls over the Agency's supply chain risk management, we recommended that the NASA Chief Information Officer, in coordination with the Assistant Administrator for Procurement:

1. Work with the FBI and NASA Counterintelligence Office to develop methods for the consistent utilization of information obtained from the FBI and other Government sources to enable informed acquisition and risk management decisions regarding IT and communications products and services and the risk they may be vulnerable to cyber-espionage or sabotage.
2. Ensure NASA's assessed and cleared listing (ACL) is updated weekly and that it contains a selection of cleared IT and communications products and services sufficient to meet Agency needs.
3. Revise the NASA Procurement Class Deviation to remove language that exempts IT systems from the Agency's supply chain risk management review process.
4. Incorporate information regarding the Agency's supply chain risk management requirements into NASA IT security training to highlight the threats, vulnerabilities, and consequences associated with IT and communications products and services.
5. Review the 7 transactions identified by the OIG in which IT and communication products were acquired without a supply chain risk assessment and establish whether the acquisition violated the Anti-Deficiency Act.
6. Perform a comprehensive risk assessment, using information obtained from FBI and NASA Counterintelligence, for the 7 IT and communications products acquired outside the Agency's supply chain risk management process to determine their vulnerability to cyber-espionage and sabotage.
7. Direct all NASA Centers, Mission Directorates, and Program/Project Offices to review and strengthen their current supply chain risk management efforts to ensure only assessed and cleared IT and communications products and services enter the Agency's supply chain.

We provided a draft of this report to NASA management, who concurred with our recommendations and described planned corrective actions. We consider the proposed actions responsive for all seven recommendations and will close them upon verification and completion of those actions.

Management's comments are reproduced in Appendix D. Technical comments have been incorporated, as appropriate.

Major contributors to this report include Laura B. Nicolosi, Mission Support Director; Joseph A. Shook, Project Manager; Sashka Mannion; Christopher Reeves; Matt Ward; Jaye Bupp; and Earl E. Baker.

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

Paul K. Martin
Inspector General

APPENDIX A: SCOPE AND METHODOLOGY

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

To answer our objective and gain an understanding of the Agency's information security controls relating to the administration and management of its Supply Chain Risk Management efforts, we performed fieldwork at NASA Headquarters, Glenn Research Center, Johnson Space Center, and Kennedy Space Center. Further, we interviewed the Agency Deputy CIO, SAISO, and many IT officials across the OCIO. We also surveyed in writing and interviewed in person the Center CIOs, and Mission Directorate IT Representatives. We analyzed the Agency's assessed and cleared listing and its listing of approved requests for investigation. Additionally, we interviewed other Agency officials to gain an understanding of how NASA manages the supply chain risk management efforts for IT and communications products and services across the Agency. Finally, we reviewed public laws and requirements, NASA policies, prior audit reports, external reviews, and various other documents related to supply chain risk management.

Federal Laws, Regulations, Policies, and Guidance

- Pub. L. No. 114-113, "Consolidated Appropriations Act, 2016," December 18, 2015
- Pub. L. No. 113-283, "Federal Information Security Modernization of 2014," December 18, 2014
- Pub. L. No. 113-235, "Consolidated and Further Continuing Appropriations Act, 2015," December 16, 2014
- Pub. L. No. 113-76, "Consolidated and Further Continuing Appropriations Act, 2014," January 17, 2014
- Pub. L. No. 113-6, "Consolidated and Further Continuing Appropriations Act of 2013," March 26, 2013
- Pub. L. No. 107-347, "E-Government Act of 2002," December 17, 2002
- 48 Code of Federal Regulations Part 1852.204-76, "Security Requirements for Unclassified Information Technology Resources," October 2017 Edition
- 48 Code of Federal Regulations Part 1852.204-75, "Security Classification Requirements," October 2017 Edition

Office of Management and Budget

- OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," July 28, 2016

Federal Information Processing Standards Publications

- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

National Institute of Standards and Technology

- NIST SP 800-160, "Systems Security Engineering," November 2016
- NIST SP 800-161 Guidance, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," April 2015
- NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013
- NIST SP 800-53A, Revision 4, "Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans," December 2014
- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments," September 2012
- NIST SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011
- NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010

NASA Policy Directives and Procedural Requirements

- NPD 2800.1B, “Managing Information Technology," March 21, 2008
- NPR 2800.1B, “Managing Information Technology," March 20, 2009
- NPD 2810.1E, “NASA Information Security Policy," July 14, 2015
- NPR 2810.1A, “Security of Information Technology," May 16, 2006
- NPD 7500.1D, “Program and Project Life-Cycle Logistics Support Policy,” March 2, 2015
- NPD 8730.2C, “NASA Parts Policy (Revalidated 12/6/13),” November 3, 2008
- NPR 8735.1C, Procedures for Exchanging Parts, Materials, Software, and Safety Problem Data Utilizing the Government-Industry Data Exchange Program (GIDEP) and NASA Advisories, February 13, 2013
- NASA Procurement Class Deviation 15-03A, “Class deviation to NFS 1839 and 1852, Restrictions on Acquiring Moderate or High-Impact Information Technology Systems,” April 28, 2016

- NASA Procurement Information Circular (PIC) 15-03, “Class Deviation to NFS 1839 and 1852, Restrictions on Acquiring Moderate or High-Impact Information Technology Systems for FY2015,” April 1, 2015

NASA Information Technology Security Handbooks

- NASA IT Security Handbook 2810.14-01, "System and Information Integrity," December 1, 2014
- NASA IT Security Handbook 2810.05-01, "Systems and Service Acquisition," May 2, 2017
- NASA IT Security Handbook 2810.04-01A, "Risk Assessment: Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching, & Organizationally Defined Values," October 12, 2012
- NASA IT Security Handbook 2810.02-02E, "Security Assessment and Authorization," November 29, 2016
- NASA IT Security Handbook 2810.02-05A, "Security Assessment and Authorization: External Information Systems," October 11, 2016
- NASA IT Security Handbook 2810.02-04-A, "Security Assessment and Authorization: Continuous Monitoring Security Control Ongoing Assessments and Authorization," March 18, 2014
- NASA IT Security Handbook 2810.16-01, "Audit and Accountability," May 2, 2017
- NASA IT Security Handbook 2810.06-01, "Security Awareness and Training, " May 2, 2017
- NASA IT Security Handbook 2810.12-01, "Physical and Environmental Protection," May 2, 2017

Use of Computer-Processed Data

We used computer-processed data to perform this audit, and that data was used to materially support findings, conclusions, and recommendations. In order to assess the quality and reliability of the data, we verified the information through independent calculations and corroboration with Program documents and the input of various Program officials. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

Review of Internal Controls

Based on the work performed during this analysis, we reviewed internal controls as they relate to NASA’s information technology supply chain risk management efforts and identified weaknesses that could potentially impact the confidentiality, integrity, and availability of NASA data, systems, and networks. We discussed the control weaknesses identified in the body of this report. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

During the last 6 years, the NASA OIG and the Government Accountability Office (GAO) have issued 21 audit reports and the U.S. House of Representatives, Permanent Select Committee on Intelligence has issued 1 report that are significant relevance to the subject of this report. Unrestricted reports can be accessed at http://oig.nasa.gov/audits/reports/FY17 , http://www.gao.gov, and http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf, respectively.

NASA Office of Inspector General

Industrial Control System Security within NASA's Critical and Supporting Infrastructure (IG-17-011, February 8, 2017)

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

Final Memorandum, Federal Information Security Modernization Act: Fiscal Year 2016 Evaluation (Full Report) (IG-17-002, November 7, 2016)

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

Final Memorandum, Review of NASA's information Security Program (IG-16-016, April 14, 2016)

Final Memorandum, Federal Information Security Management Act: Fiscal Year 2015 Evaluation (IG-16-002, October 19, 2015)

Final Memorandum, Federal Information Security Management Act: Fiscal Year 2014 Evaluation (IG-15-004, November 13, 2014)

Federal Information Security Management Act: Fiscal Year 2013 Evaluation (IG‐14‐004, November 20, 2013)

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

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

Federal Information Security Management Act: Fiscal Year 2012 Evaluation (IG-13-001, October 10, 2012)

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

Federal Information Security Management Act: Fiscal Year 2011 Evaluation (IG-12-002, October 17, 2011)

Government Accountability Office

Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs (GAO-15-714, September 29, 2015)

Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems (GAO-15-573T, April 22, 2015)

Information Technology: Additional OMB and Agency Actions Needed to Ensure Portfolio Savings Are Realized and Effectively Tracked (GAO-15-296, April 16, 2015)

Information Technology: OMB and Agencies Need to Focus Continued Attention on Eliminating Duplicative Investments (GAO-13-685T, June 11, 2013)

IT Supply Chain, National Security-Related Agencies Need to Better Address Risks, (GAO-12-361, March 23, 2012)

Information Technology: OMB Needs to Improve Its Guidance on IT Investments, (GAO-11-826, September 29, 2011)

Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management (GAO-11-634, September 15, 2011)

Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings (GAO-11-565, July 19, 2011)

Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices (GAO-17-549, September 28, 2017)

U.S. House of Representatives, Permanent Select Committee on Intelligence

Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (U.S. House of Representatives, 112th Congress, October 8, 2012)

Appendix B: NIST Recommended System and Services Acquisition Control Family Controls and Enhancements

Table 1 below describes the System and Services Acquisition information security controls recommended by NIST to address supply chain risk management threats.

Table 1: Supply Chain Risk Management Threats

Number	Control ID	Control Name and Description	Moderate Systems	High Systems
1	SA-1	System and Services Acquisition Policy and Procedures This control addresses the development, documentation, and dissemination of system and services acquisition policy's that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in addition to procedures to facilitate the implementation of the system and services acquisition policies and associated system and services acquisition controls that reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.	SA-1	SA-1
2	SA-2	Allocation of Resources This control addresses information security requirements for information systems or information system services in mission/business process planning. This control further addresses how an Agency documents, and allocates the resources required to protect information systems or information system services as part of its capital planning and investment control process; and establishes a discrete line item for information security in organizational programming and budgeting documentation.	SA-2	SA-2

Number	Control ID	Control Name and Description	Moderate Systems	High Systems
3	SA-3	System Development Life Cycle This control addresses the definition and documentation of information security roles and responsibilities throughout the system development life cycle. The control further identifies individuals having information security roles and responsibilities; and integrates Agency information security risk management processes into system development life cycle activities that provide the foundation for the successful development, implementation, and operation of organizational information systems and requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions.	SA-3	SA-3
4	SA-4	Acquisition Process This control addresses requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
5	SA-5	Information System Documentation This control addresses the implementation and operation of security controls associated with information systems, system components, and information system services. This includes establishing specific measures to determine the quality/completeness of the information system documentation content along with the level of protection for selected information systems, components, or services to ensure that documentation is commensurate with the security category or classification of the system.	SA-5	SA-5
6	SA-8	Security Engineering Principles This control addresses information system security engineering principles in the specification, design, development, implementation, and modification of information systems. These principles apply primarily to the development of new information systems or information systems undergoing major upgrades.	SA-8	SA-8

Number	Control ID	Control Name and Description	Moderate Systems	High Systems
7	SA-9	External Information System Services This control addresses external information system services that are implemented outside of Agency information systems and includes services that are used by but are not part of Agency information systems. FISMA requires that Agencies using external service providers that process, store, or transmit federal information or information systems operated on behalf of the federal government meet the same security requirements that federal agencies are required to meet.	SA-9 (2)	SA-9 (2)
8	SA-10	Developer Configuration Management This control addresses Agencies that conduct internal information systems development and integration and requires Agencies consider the quality and completeness of configuration management activities conducted by developers as evidence of applying effective security safeguards such as protecting data from unauthorized modification or destruction. Further the control addresses that Agencies maintain the integrity of changes to information systems, components, or services throughout the system development life cycle and that authorized changes are tracked to prevent unauthorized changes.	SA-10	SA-10
9	SA-11	Developer Security Testing and Evaluation This control addresses the implementation of a security assessment plan; the performance of testing and the results of the security testing. This control also requires that Agencies implement a verifiable process to address and correct flaws identified during security testing performed during all phases of the system development life cycle that may adversely affect previously implemented security controls.	SA-11	SA-11
10	SA-12	Supply Chain Protection This control addresses supply chain threats to the information system, system components, or information system services by employing a comprehensive, defense-in-breadth information security strategy and that information systems be protected throughout the system development life cycle.		SA-12

Number	Control ID	Control Name and Description	Moderate Systems	High Systems
11	SA-15	Development Process, Standards, and Tools This control addresses development of information systems, system components, or information system services to ensure that documented development process is followed that addresses security requirements, identifies the standards and tools used in the development process, documents the specific tool options and tool configurations used in the development process, and documents, manages, and ensures the integrity of changes to the process and/or tools used in development to maintain the integrity of changes throughout the systems development life cycle and to track authorized changes and prevent unauthorized changes.		SA-15
12	SA-16	Developer-Provided Training This control addresses the development of information systems, system components, or information system services to provide training on the correct use and operation of implemented security functions, controls, and/or mechanisms. This applies to external and internal (in-house) developers and is an essential element to ensure the effectiveness of security controls implemented within Agency information systems.		SA-16
13	SA-17	Developer Security Architecture and Design This control addresses the requirement that developers of information systems, system components, or information system services produce a design specification and security architecture that is consistent with and supportive of the Agency's security architecture and is an integrated part of the Agency's enterprise architecture. This control is primarily directed at external developers, although it may also be used for internal (in-house) development.		SA-17

Appendix C: Summary of Costs Questioned by the OIG

Table 2 below summarizes the questioned costs identified during our audit and discussed in this report (see discussion of questioned costs starting on page 13). These costs are questioned due to acquisitions that did not follow NASA's supply chain risk management process. Given the nature in which these costs are questioned, the dollars are not recoverable.

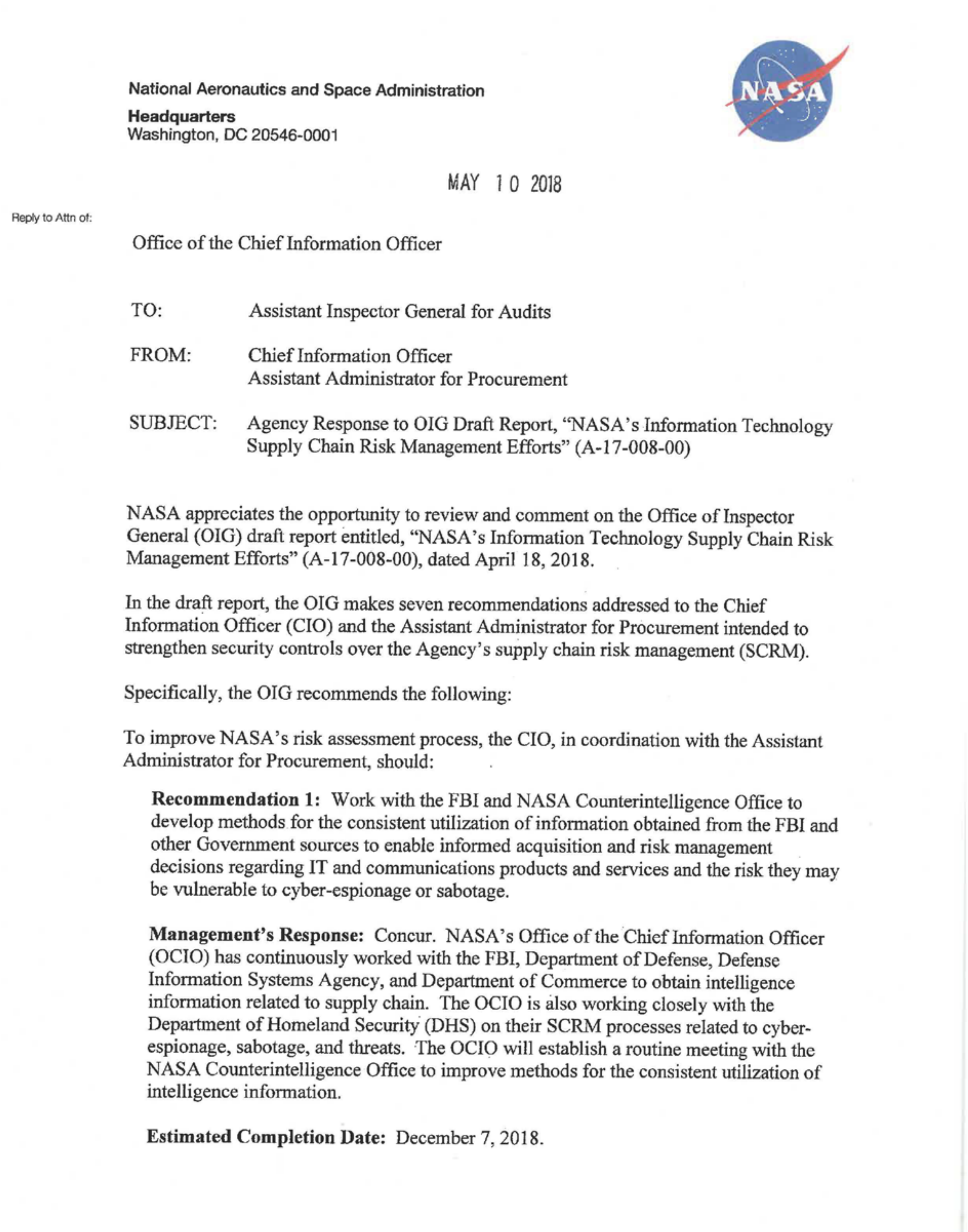
Table 2: Questioned Costs

IT and Communications Product	Number of IT and Communications Products Acquired	Amount Questioned by OIG[a]
BEAM PROFILER	1	3,307
80" Television/Monitor	1	3,500
3D Printer	1	3,500
C2U Server	1	6,385
4K UHD LCD Monitor	15	20,802
88GB Cache, Switch x2	2	94,389
4K Ultra HD LED-Lit Monitor	5	10,992
Total		**$142,875**

Source: NASA Purchase Card and SEWP Transactions

[a] Questioned costs are expenditures that are questioned by the Office of Inspector General because of an alleged violation of legal, regulatory, or contractual requirements, are not supported by adequate documentation at the time of the audit, or are unallowable, unnecessary, or unreasonable.

Appendix D: Management's Comments



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

MAY 10 2018

Reply to Attn of:

Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer
Assistant Administrator for Procurement

SUBJECT: Agency Response to OIG Draft Report, "NASA's Information Technology Supply Chain Risk Management Efforts" (A-17-008-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "NASA's Information Technology Supply Chain Risk Management Efforts" (A-17-008-00), dated April 18, 2018.

In the draft report, the OIG makes seven recommendations addressed to the Chief Information Officer (CIO) and the Assistant Administrator for Procurement intended to strengthen security controls over the Agency's supply chain risk management (SCRM).

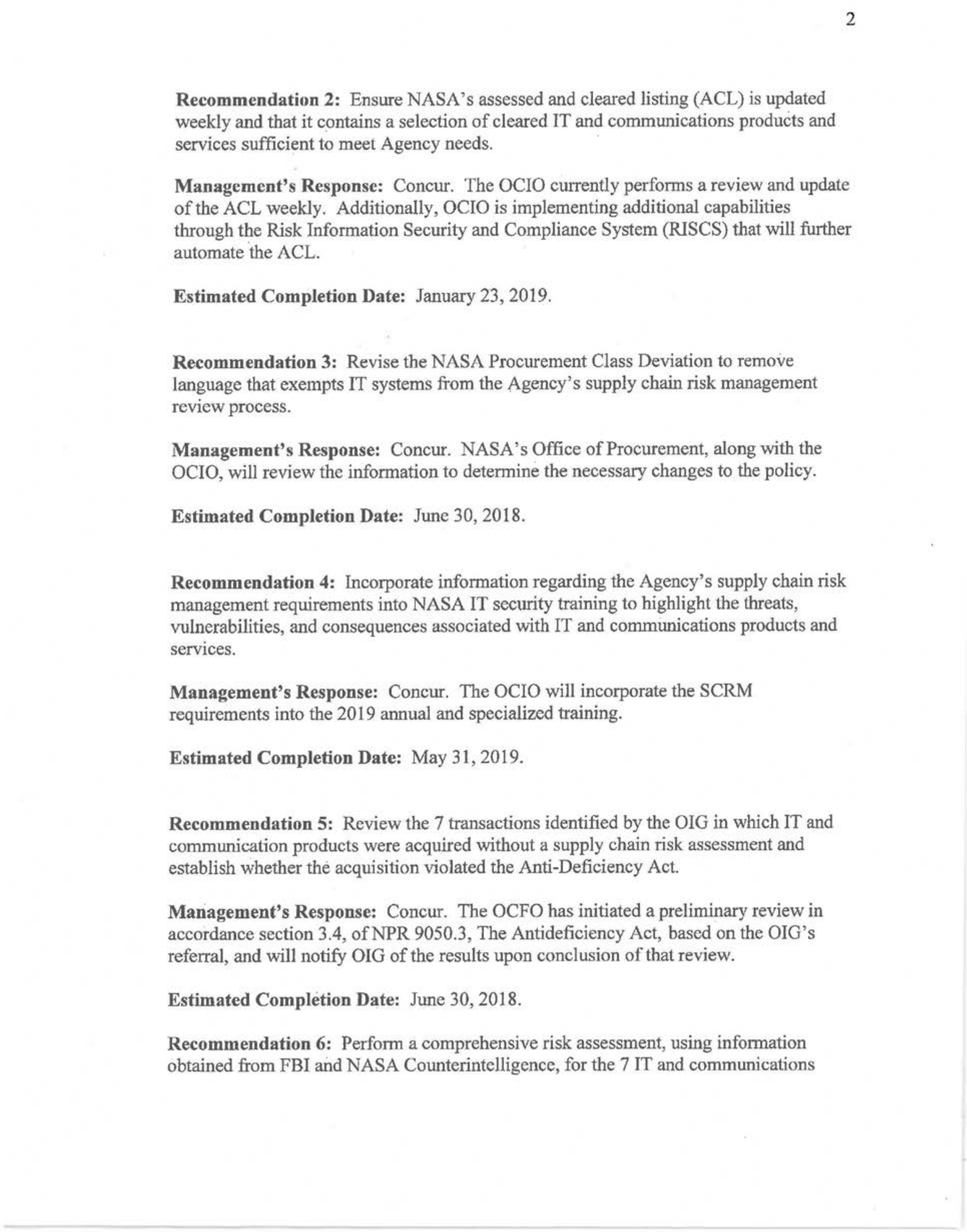
Specifically, the OIG recommends the following:

To improve NASA's risk assessment process, the CIO, in coordination with the Assistant Administrator for Procurement, should:

Recommendation 1: Work with the FBI and NASA Counterintelligence Office to develop methods for the consistent utilization of information obtained from the FBI and other Government sources to enable informed acquisition and risk management decisions regarding IT and communications products and services and the risk they may be vulnerable to cyber-espionage or sabotage.

Management's Response: Concur. NASA's Office of the Chief Information Officer (OCIO) has continuously worked with the FBI, Department of Defense, Defense Information Systems Agency, and Department of Commerce to obtain intelligence information related to supply chain. The OCIO is also working closely with the Department of Homeland Security (DHS) on their SCRM processes related to cyber-espionage, sabotage, and threats. The OCIO will establish a routine meeting with the NASA Counterintelligence Office to improve methods for the consistent utilization of intelligence information.

Estimated Completion Date: December 7, 2018.



Recommendation 2: Ensure NASA's assessed and cleared listing (ACL) is updated weekly and that it contains a selection of cleared IT and communications products and services sufficient to meet Agency needs.

Management's Response: Concur. The OCIO currently performs a review and update of the ACL weekly. Additionally, OCIO is implementing additional capabilities through the Risk Information Security and Compliance System (RISCS) that will further automate the ACL.

Estimated Completion Date: January 23, 2019.

Recommendation 3: Revise the NASA Procurement Class Deviation to remove language that exempts IT systems from the Agency's supply chain risk management review process.

Management's Response: Concur. NASA's Office of Procurement, along with the OCIO, will review the information to determine the necessary changes to the policy.

Estimated Completion Date: June 30, 2018.

Recommendation 4: Incorporate information regarding the Agency's supply chain risk management requirements into NASA IT security training to highlight the threats, vulnerabilities, and consequences associated with IT and communications products and services.

Management's Response: Concur. The OCIO will incorporate the SCRM requirements into the 2019 annual and specialized training.

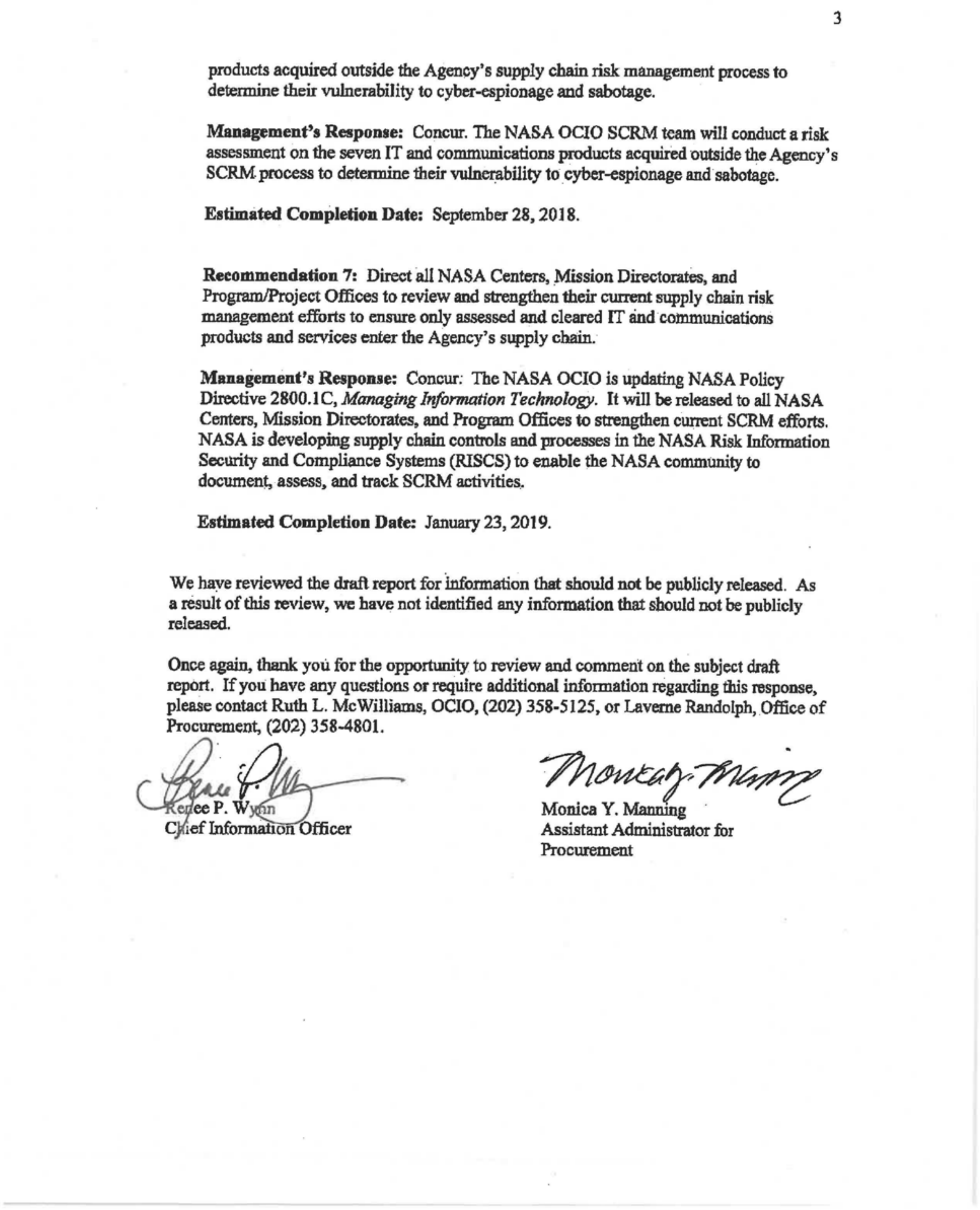
Estimated Completion Date: May 31, 2019.

Recommendation 5: Review the 7 transactions identified by the OIG in which IT and communication products were acquired without a supply chain risk assessment and establish whether the acquisition violated the Anti-Deficiency Act.

Management's Response: Concur. The OCFO has initiated a preliminary review in accordance section 3.4, of NPR 9050.3, The Antideficiency Act, based on the OIG's referral, and will notify OIG of the results upon conclusion of that review.

Estimated Completion Date: June 30, 2018.

Recommendation 6: Perform a comprehensive risk assessment, using information obtained from FBI and NASA Counterintelligence, for the 7 IT and communications



products acquired outside the Agency's supply chain risk management process to determine their vulnerability to cyber-espionage and sabotage.

Management's Response: Concur. The NASA OCIO SCRM team will conduct a risk assessment on the seven IT and communications products acquired outside the Agency's SCRM process to determine their vulnerability to cyber-espionage and sabotage.

Estimated Completion Date: September 28, 2018.

Recommendation 7: Direct all NASA Centers, Mission Directorates, and Program/Project Offices to review and strengthen their current supply chain risk management efforts to ensure only assessed and cleared IT and communications products and services enter the Agency's supply chain.

Management's Response: Concur. The NASA OCIO is updating NASA Policy Directive 2800.1C, *Managing Information Technology*. It will be released to all NASA Centers, Mission Directorates, and Program Offices to strengthen current SCRM efforts. NASA is developing supply chain controls and processes in the NASA Risk Information Security and Compliance Systems (RISCS) to enable the NASA community to document, assess, and track SCRM activities.

Estimated Completion Date: January 23, 2019.

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

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Ruth L. McWilliams, OCIO, (202) 358-5125, or Laverne Randolph, Office of Procurement, (202) 358-4801.

Renee P. Wynn
Chief Information Officer

Monica Y. Manning
Assistant Administrator for
Procurement

Appendix E: Report Distribution

National Aeronautics and Space Administration

Administrator
Associate Administrator
Deputy Associate Administrator
Acting Chief of Staff
Chief Information Officer
Assistant Administrator for Procurement
Director, Glenn Research Center
Director, Johnson Space Center
Director, Kennedy Space Center

Non-NASA Organizations and Individuals

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

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 Space, Science, and Competitiveness

Senate Committee on Homeland Security and Governmental Affairs

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

House Committee on Oversight and Government Reform
Subcommittee on Government Operations

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

(Assignment No. A-17-008-00)