MARCH 18, 2013

AUDIT REPORT

OFFICE OF AUDITS

NASA'S PROCESS FOR ACQUIRING INFORMATION TECHNOLOGY SECURITY ASSESSMENT AND MONITORING TOOLS

OFFICE OF INSPECTOR GENERAL

National Aeronautics and
Space Administration

REPORT NO. IG-13-006 (ASSIGNMENT NO. A-11-021-00)

Final report released by:

Paul K. Martin
Inspector General

Acronyms

ACES	Agency Consolidated End-user Services
APM	Application Portfolio Management
AVAR	Agency Vulnerability Assessment and Remediation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DCIO	Deputy Chief Information Officer
ELMT	Enterprise License Management Team
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GRC	Governance, Risk, and Compliance
IT	Information Technology
ITSC	Information Technology Security Center
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OCSO	Organizational Computer Security Official
OIG	Office of Inspector General
OMB	Office of Management and Budget
RMS	Risk Management System

OVERVIEW

NASA'S PROCESS FOR ACQUIRING INFORMATION TECHNOLOGY SECURITY ASSESSMENT AND MONITORING TOOLS

The Issue

NASA's information technology (IT) infrastructure – a complex and diverse array of more than 500 computer systems with 140,000 components spread across numerous locations – plays a critical role in virtually every aspect of the Agency's mission, from controlling spacecraft and processing scientific data to enabling NASA personnel to collaborate with colleagues around the world. At the same time, the Agency's high profile and use of advanced technology coupled with the relatively large size of its networks makes it an attractive target to cyber attackers. To thwart such attacks, NASA must ensure that its IT systems and their associated components are regularly safeguarded, assessed, and monitored. To accomplish this task, the Office of the Chief Information Officer (OCIO) spends at least $58 million annually on IT security, a portion of which is used to acquire and manage security assessment and monitoring tools.

Federal laws and regulations require Federal Government agencies to develop IT security policies and procedures, including Agency-wide IT security programs. In addition, the Information Technology Management Reform Act of 1996 (Clinger-Cohen) requires NASA and other agencies to identify opportunities to achieve efficiencies, improve integration and security, and ensure alignment of IT assets with the agency mission. The Office of Management and Budget (OMB) also requires agencies to coordinate their IT management efforts to eliminate duplicative IT investments, pool purchasing power across respective organizations, drive down costs, and improve IT services.[1] NASA's Strategic Management Council directed the OCIO to implement an application portfolio management (APM) process with the goal of satisfying the greatest number of IT requirements with the fewest applications.[2]

The NASA Office of Inspector General (OIG) initiated this audit to review NASA's policies and procedures related to its acquisition of IT security assessment and monitoring tools. Because the Agency was unable to provide a complete inventory of the tools it purchased to manage nine IT security control areas, we distributed questionnaires to IT security personnel at NASA Headquarters and all Centers. The questionnaire

[1] OMB Memorandum M-11-29, "Chief Information Officer Authorities," August 8, 2011.

[2] APM is a process that provides visibility of IT assets allowing for better decision-making, maintaining a user-friendly inventory of applications (including cost data), and identifying opportunities for reducing duplication among applications.

response rate was 73 percent (111 responses out of 153 questionnaires). See Appendix A for details of the audit's scope and methodology. See Appendix B for information about the questionnaire.

Results

NASA has not fully implemented a process for identifying its IT security assets, a necessity to meet federally mandated requirements and improve IT acquisition outcomes. Lack of such controls result in missed opportunities to capitalize on efficiencies and leverage purchasing power on critical IT security investments. NASA could use two internal management control processes ─ Capital Planning and Investment Control (CPIC) and APM ─ to improve visibility over purchases of IT security assessment and monitoring tools. The CPIC process (mandated by Clinger-Cohen) is intended to capture an agency's major IT investments and achieve cost savings by identifying and eliminating redundant purchases. To facilitate CPIC requirements, NASA uses its IT Investment Management System (ProSight) to collect and aggregate IT investment cost data. However, we found that the ProSight data lacks sufficient detail to identify specific IT security tool requirements, associated maintenance costs, or tools planned for purchase, and therefore cannot be used to prioritize investments or identify potential cost savings. We learned that Marshall Space Flight Center (Marshall) modified ProSight to enable collection of more specific data on IT security assessment and monitoring tools and Marshall IT personnel developed a software application using a commercial off-the-shelf product to provide rapid analysis and review of this data. Both initiatives have enabled Marshall personnel to better document, assess, and prioritize Center-based IT investments.

The APM management control process also developed to meet a Clinger-Cohen requirement) organizes IT applications into relevant portfolio categories to enable performance assessments of individual assets and the portfolio as a whole. Proper use of APM provides visibility of IT assets and enables more informed decision-making, a user-friendly inventory of applications (including cost data), and opportunities for reducing duplication among applications. In April 2007, NASA's Strategic Management Council directed the Chief Information Officer (CIO) to implement the APM process with the goal of satisfying the greatest set of IT requirements using the fewest applications. However, according to Agency officials the APM process was discontinued in June 2011 due to restructuring within the OCIO and the inability to maintain an accurate inventory of application data.

OCIO personnel interviewed as part of this audit stated they were in the process of gathering data on IT security assessment and monitoring tools used Agency-wide. In our judgment, NASA could improve visibility over its IT portfolio and identify opportunities for reducing duplication among all applications by re-instituting the APM process.

In addition to the CPIC and APM processes, NASA's Enterprise License Management Team (ELMT) is responsible for evaluating requirements to determine whether cost savings can be achieved by consolidating purchases. According to Agency officials, the ELMT works with NASA's OCIO and Office of Procurement to increase efficiency in purchasing and utilizing software. ELMT seeks to identify common software requirements and consolidate common software purchases throughout the Agency; conduct market research and business case development; secure appropriate volume discounts for applicable licenses; and distribute unused licenses by negotiating license transferability. To maximize its effectiveness, the ELMT requires comprehensive information on Agency IT technical and purchasing requirements. However, we found that such data is not readily available. Despite this limitation, ELMT officials said they have achieved $5.9 million in reduced software costs by leveraging NASA's purchasing power and by eliminating redundant purchases and related maintenance agreements.

Because NASA does not have a process that captures, consolidates, and assesses IT security tool requirements across the Agency, centralized purchases of tools to meet common IT security tool requirements do not regularly occur. For example, our survey showed that NASA spent $25.7 million on 242 separate purchases of IT security assessment and monitoring tools across nine control areas currently in use as of June 2012 with little or no coordination between IT security officials. This inability to consolidate requirements and centralize purchases limits NASA's efforts to gain efficiencies on critical IT investments.

In addition, NASA's decentralized organizational structure contributes to an ineffective IT investment management process. For example, we identified the following purchases across the Agency:

- NASA OCIO spent $7.3 million to purchase and $1.8 million in annual maintenance costs for Agency-wide IT security assessment and monitoring tools;
- NASA Centers spent $5.9 million to purchase and $2.2 million to annually maintain assessment and monitoring security tools that perform the same or similar IT security management functions; and
- Individual organizations that supported project systems at 10 locations spent $6.7 million to purchase and $1.8 million in annual maintenance costs for additional IT security assessment and monitoring tools with similar functions.

NASA's lack of centralized and readily available information on current and planned IT security tool purchases diminishes opportunities to save money by consolidating similar requirements and purchases. In particular, NASA's IT investment management and reporting process has not been tailored to capture the data Agency IT officials need to understand the products the Agency currently owns or plans to purchase. We believe significant opportunities exist for Agency officials to reduce unnecessary or redundant purchases. For example:

- **Vulnerability Management Tools.** In 2008, the OCIO spent $364,973 to purchase McAfee Foundstone/McAfee Vulnerability Manager as the

Agency-wide solution for vulnerability management on NASA's 140,000 system components. The annual maintenance cost for this software exceeds $200,000. Two years later, NASA acquired vulnerability management services through the Consolidated End-user Services (ACES) contract, which duplicates vulnerability management services on 32,200 of NASA's system components.

- **Governance, Risk, and Compliance (GRC) Tools.** NASA acquired three different tools for managing GRC ─ Risk Management System (RMS), Information Technology Security Center (ITSC), and Rsam. These products were developed or purchased to meet Federal Information Security Management Act (FISMA) requirements to manage system security plans, track Plan of Action and Milestones, and monitor the security posture of NASA's systems and associated components. The tools purchased performed the same or similar IT security management functions. The OCIO purchased RMS as an Agency-wide solution for $1.5 million with annual maintenance costs of $273,000. Marshall internally developed ITSC, which has annual maintenance costs of $361,000. Finally, four NASA locations made a combined purchase of Rsam at a total cost of $372,339, with annual maintenance costs of $80,412. The Rsam purchase occurred after the OCIO's RMS purchase and both purchases were made after Marshall's development of ITSC, which was available for use by all NASA organizations.

- **Log Event Management Tools.** The OCIO, Chief Information Security Officers (CISOs), and Organizational Computer Security Officials (OCSOs) reported making 12 separate purchases of Splunk ─ a product used to log details of potential security threats on networks and systems ─ at a cost of $1.3 million with annual maintenance costs of $237,245. Even when organizations were located at the same Center, coordination and consolidation of purchases did not consistently occur. For example, two of these purchases were made separately by projects that resided at Goddard Space Flight Center.

- **Firewall/Boundary Protection Tools.** The OCIO, CISOs, and OCSOs reported making 20 separate purchases of Juniper boundary protection tools at a total cost of $3.1 million with annual maintenance costs of $450,135.[3]

We believe NASA should integrate the processes used by CPIC, APM, and ELMT to obtain more detailed information on IT security assessment and monitoring tool requirements across the Agency. We acknowledge that not all of the purchases we identified created duplication or could have been consolidated; however, in our judgment consolidating Agency requirements will allow NASA to more efficiently manage its widely distributed IT systems and the funds it allocates for IT security. NASA's ability to identify and consolidate IT security tool requirements prior to making purchase

[3] Firewall/boundary protection tools protect against external and internal intrusions of computer networks.

decisions is imperative to achieve cost savings and standardize IT security tools Agency-wide.

Management Action

We recommended that the CIO modify the CPIC process to capture detailed IT security requirements and re-establish the APM process to enable greater visibility over existing inventory and planned acquisition of IT assessment and monitoring tools. Furthermore, NASA should consider routing the captured data acquired from the revised CPIC process to ELMT for review and potential consolidation of IT security tool purchases.

In response to a draft of this report, the CIO concurred with our recommendations and stated that the OCIO plans to complete responsive actions by the end of fiscal year (FY) 2015. We consider the OCIO planned actions responsive and will close the recommendations upon verification that the actions are complete. The Agency's comments in response to a draft of this report are reprinted in Appendix C.

CONTENTS

INTRODUCTION

RESULTS

APPENDIX A

APPENDIX B

APPENDIX C

APPENDIX D

INTRODUCTION

Background

NASA has a diverse information technology (IT) infrastructure that encompasses more than 500 computer systems with 140,000 components distributed across the country. The organizational structure is also complex, with individual NASA Centers and tens of thousands of contractors supporting hundreds of NASA projects, many using NASA's computer networks to process, store, and transmit sensitive information. Concurrently, the large number of NASA systems and importance of the information on these systems makes NASA an attractive target to cyber attackers. To prevent and thwart such attacks, NASA must ensure that its IT systems and their associated components are safeguarded and regularly assessed and monitored. NASA uses a variety of IT security assessment and monitoring tools to respond to ever-evolving IT security threats. However, the decentralized nature of its organizational structure makes implementation of an effective IT security investment management process a continuous challenge.

NASA's Chief Information Officer (CIO) and the Deputy CIO for IT Security (DCIO) are responsible for developing IT security policies and procedures and for implementing an Agency-wide IT security program. The CIO and DCIO work from the Headquarters-based Office of the Chief Information Officer (OCIO). In addition, each Center has a CIO in charge of Center IT operations, and each Center CIO has a Chief Information Security Officer (CISO) responsible for IT security operations. In most cases, the Center CIO also assigns multiple Organizational Computer Security Officials (OCSOs) to the CISO to facilitate implementation and oversight of information security within their organizations. Further, NASA's three Mission Directorates (Aeronautics Research, Science, and Human Exploration and Operations) have IT points of contact who coordinate with the OCIO. All of these individuals play a key role in ensuring the IT security of NASA's networks and components and, therefore, are involved in determining what IT security assessment and monitoring tools the Agency needs.

NASA's CIO has statutory responsibility through the Information Technology Management Reform Act of 1996, also known as the Clinger-Cohen Act, to eliminate duplicative IT investments and applications. In addition, the Office of Management and Budget (OMB) requires that CIOs work with Chief Financial Officers and Chief Acquisition Officers to eliminate duplicative IT investments, pool purchasing power, and improve IT services. To help meet these objectives, NASA developed a Capital Planning and Investment Control (CPIC) process to achieve cost savings by eliminating redundant purchases. Further, NASA's Strategic Management Council directed the NASA CIO to work with the Office of Program Analysis and Evaluation and the Office of the Chief Engineer to develop an Application Portfolio Management (APM) process that organizes the Agency's investments in IT tools and applications to ensure integration and eliminate unnecessary duplication. NASA Procedural Requirements (NPR) 2800.1B, "Managing Information Technology," March 20, 2009, also requires an APM process. Finally, NASA's Enterprise License Management Team (ELMT) evaluates software requirements to determine whether cost savings can be achieved by consolidating purchases.

Objectives

The objective of this audit was to review NASA's policies and procedures related to the acquisition of IT security assessment and monitoring tools. Details of the audit's scope and methodology are in Appendix A.

NASA NEEDS TO IMPROVE ITS PROCESS FOR ACQUIRING INFORMATION TECHNOLOGY SECURITY ASSESSMENT AND MONITORING TOOLS

NASA's IT investment management process does not fully capture, assess, and consolidate IT security tool requirements across the Agency and therefore misses opportunities to capitalize on efficiencies and leverage purchasing power on critical IT security investments. NASA officials reported spending $25.7 million on 242 separate purchases of IT security assessment and monitoring tools currently in use as of June 2012. We found that officials made these purchases with little or no coordination and identified specific purchases that could have been consolidated to better leverage the Agency's purchasing power. With improved awareness of its IT portfolio and visibility over its purchases, NASA could reduce its costs for IT security assessment and monitoring tools and potentially save millions of dollars annually in maintenance costs.

NASA's IT Investment Management and Reporting Process Could be Tailored to Capture and Review IT Security Investment Data

Despite federally mandated requirements, NASA has not fully implemented a coordinated approach to identifying its IT requirements and improving IT acquisition outcomes. The Clinger-Cohen Act and OMB require agencies to review IT investments to identify opportunities to achieve efficiencies and pool their purchasing power across entire organizations to drive down costs and improve IT services. NASA created the ELMT in April 2008 to help the Agency determine whether it could achieve cost savings by consolidating IT purchases. In addition, the Agency has two internal management control processes ─ CPIC and APM ─ that are intended to identify NASA's IT investments and eliminate redundant purchases to achieve cost savings. However, NASA has not used these processes to capture detailed IT security assessment and monitoring tool investment data. If NASA standardized the CPIC process and implemented the IT application data capture functionality for all users, the Agency could gain a better understanding of its IT portfolio and greater visibility over its purchases. Moreover, the resulting data could help the ELMT negotiate more cost-effective purchase agreements.

Capital Planning and Investment Control. The Clinger-Cohen Act mandates that each Federal agency have a CPIC process to improve IT management through reductions in IT operations and maintenance costs and increased efficiency of operations. CPIC is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and management of IT in support of agency missions and business needs. NASA's IT Investment Management System (ProSight), managed by the OCIO, collects and aggregates IT investment cost data as part of the CPIC process.

However, we found that the CPIC process is not consistently implemented at each Center and there is little collaboration between Centers.

NASA's CPIC process captures cost data on high value IT investments (major commodities) and generally focuses little on the details of low-value purchases (non-major commodities such as IT security tools). Further, the data collected in ProSight is not sufficiently detailed to identify specific IT security tool requirements, maintenance costs, or tools planned for purchase. Although the functionality exists to capture most IT application data, ProSight is used primarily to capture cost information on major commodities. As a result, aggregate data in ProSight does not provide enough detail to identify purchase and maintenance costs associated with IT security tools or information about planned IT security purchases.

Although NASA is not using ProSight to collect data on all IT security purchases, officials at Marshall have modified the system to collect detailed IT application data at their location. Marshall personnel also developed a software application using a commercial off-the-shelf product to facilitate rapid analysis and review of IT investment data contained within ProSight. Marshall's IT security staff have used the modified program to better document and catalog a detailed assessment of existing IT investments, establish an inventory of applications for internal and external stakeholders, and identify opportunities to reprioritize and rebalance IT assets and investments in response to changing needs and demand. Currently, only Marshall personnel use this capability although it is available to other Centers.

Application Portfolio Management (APM). The primary objective of an APM process is to provide an overall view of existing IT application assets to improve the performance of individual assets within the portfolio as well as the performance of the portfolio as a whole.[4] In April 2007, NASA's Strategic Management Council, consistent with Federal requirements established in the Clinger-Cohen Act, directed the NASA CIO to develop an APM process that organizes the Agency's investments in IT tools and applications to ensure integration and eliminate unnecessary duplication.[5] However, use of APM was discontinued as part of an OCIO reorganization in June 2011 and the OCIO's inability to maintain a reliable inventory of IT applications.

NASA's APM goals were to develop and maintain a user-friendly inventory of NASA applications with cost data; identify opportunities for reducing duplication among applications; reduce future duplication by providing increased visibility into how existing NASA applications could meet mission and business needs; and enable stakeholders to assess how well IT applications are performing. During the course of our review, OCIO personnel stated that they were gathering data on IT security assessment and monitoring

[4] A comprehensive APM program would include all IT software assets owned by the Agency. These assets would include widely used software such as Microsoft's SQL, Project, and SharePoint, Oracle applications, and internally developed software applications.

[5] The Strategic Management Council, chaired by the NASA Administrator, serves as the Agency's senior decision-making body for strategic planning. The NASA CIO is also a member of this Council.

tools used Agency-wide, but these efforts to date were incomplete. We believe NASA could improve visibility over its IT portfolio and identify opportunities for consolidating and reducing duplication among all applications by reestablishing an APM process.[6]

Enterprise License Management Team (ELMT). NASA has previously consolidated software purchases to leverage its purchasing power. In 2008, the Agency established the ELMT at the NASA Shared Service Center to work with the OCIO and the Headquarters Office of Procurement to increase efficiency in purchasing and utilizing software applications. ELMT seeks to identify widespread common software requirements, reduce software and maintenance costs on initial purchase through consolidation, reduce the number of procurements, and encourage common software versions and configurations throughout the Agency. The team maintains an enterprise license database, and all NASA Centers are encouraged to consult with the ELMT to determine whether existing agreements can fulfill their software needs before making a new purchase. ELMT also conducts market research to reduce overall license and maintenance costs and to secure volume discounts for applicable licenses. ELMT also distributes unused licenses by negotiating license transferability into purchase agreements. Transferability is important for large organizations like NASA where similar software is used often across various programs and projects. For example, when a project ends and no longer needs specific software, transferability allows other units to take ownership without added purchase expenses.

From fiscal year 2009 through 2011, ELMT was involved in the purchase of seven software applications that initially cost $27.3 million but were negotiated down to $19.1 million. After accounting for ELMT costs of $2.4 million, NASA achieved a net savings of $5.9 million through consolidations. Despite this success, we found that widespread use of ELMT was minimal due to the limited availability of IT procurement requirement and purchasing data in ProSight. Such information, if available and tailored appropriately, could allow ELMT to review portfolio management information and consolidate IT security assessment and monitoring tool requirements.

NASA Could Leverage its Purchasing Power by Consolidating IT Security Assessment and Monitoring Tool Requirements and Purchases

Because NASA's IT investment process does not adequately track technology requirements and purchases, the Agency was unable to provide complete information in support of our review. Accordingly, to determine the IT security assessment and monitoring tools in use at NASA, we distributed questionnaires to the DCIO, 12 CISOs, and 140 OCSOs. The questionnaire asked these officials to identify the IT security assessment and monitoring tools they had procured to manage the following nine IT security control areas common across all information systems: Intrusion Detection;

[6] To help NASA reestablish an APM process, we provided the OCIO with the data on IT security assessment and monitoring tools gathered during this audit.

Network Traffic Monitoring; Log Event Management; Malware and Antivirus Protection; Vulnerability Management; Patch Management; Firewall/Boundary Protection; Configuration Management; and Governance, Risk, and Compliance (GRC).

Based on questionnaire responses received through June 2012 (73 percent), we found that NASA spent $25.7 million on IT security assessment and monitoring tools across all levels of the organization. Our results indicated that the OCIO, CISOs, and OCSOs at NASA locations, Mission Directorates, programs, and projects made 242 separate purchases of IT security assessment and monitoring tools at a cost of $19.9 million and an additional $5.8 million in annual maintenance costs. Specifically, the OCIO spent $7.3 million to purchase and $1.8 million annually to maintain IT security assessment and monitoring tools while CISOs similarly spent $5.9 million to purchase and $2.2 million annually to maintain IT security assessment and monitoring tools. OCSOs supporting project systems spent $6.7 million to purchase and $1.8 million annually to maintain IT security assessment and monitoring tools. Table 1 shows the combined OCIO, CISO, and OCSO IT security tool purchases and expenditures within the nine IT security control areas.

Table 1. NASA Security Tool Purchases and Expenditures

IT Security Control Area	Number of Separate Purchases	Purchase Costs	Annual Maintenance Costs	Totals
Intrusion Detection	23	$ 3,033,215	$ 713,926	$ 3,747,141
Network Traffic Monitoring	34	2,869,551	541,707	3,411,258
Log Event Management	41	4,514,070	834,939	5,349,009
Malware and Antivirus Protection	32	541,929	221,599	763,528
Vulnerability Management	32	1,659,297	636,562	2,295,859
Patch Management	11	1,324,467	1,121,812	2,446,279
Firewall/Boundary Protection	43	3,650,492	732,298	4,382,790
Configuration Management	17	442,276	266,727	709,003
Governance, Risk, and Compliance (GRC)	9	1,899,645	734,012	2,633,657
Totals	**242**	**$ 19,934,942**	**$ 5,803,582**	**$ 25,738,524**

Source: Based on OIG analysis of NASA reponses to survey questionnaire.

We determined that in multiple instances, the OCIO, CISOs, and OCSOs purchased the same or similar tools for the nine IT security control areas, thereby indicating potential missed opportunities for consolidation.

Intrusion Detection Tools. Intrusion detection tools monitor networks or systems for malicious activities or policy violations. According to our survey, NASA made 23 separate purchases of 20 different intrusion detection tools at a cost of $3 million with annual maintenance costs of $713,926. A NASA CISO and OCSO made two separate purchases of the Basic Analysis and Security Engine Intrusion Detection Tools at a cost of $85,000 and annual maintenance costs of $15,000. Another CISO and OCSO made two separate purchases of the Forensic Access Data and Storage Intrusion Detection Tools at a cost of $318,000 and annual maintenance costs of $29,000. Additionally, the OCIO, CISOs, and OCSOs made 19 additional purchases of 18 other intrusion detection tools at a cost of $2.6 million with annual maintenance costs of $669,926.

Network Traffic Monitoring Tools. Network traffic monitoring examines network performance and user behavior to help security program managers identify areas in need of improvement. This information can be correlated with other sources of information to create a comprehensive security picture. According to our survey, NASA made 34 purchases of 24 different tools to monitor network traffic at a cost of $2.9 million with annual maintenance costs of $541,707. One of the tools purchased was Q-Radar, for which the OCIO and IT security personnel at three locations made four separate purchases for $1.2 million and annual maintenance costs of $139,605. In addition, IT security personnel at four locations made six purchases of Solar Winds tools for $99,500, with annual maintenance costs of $59,559. The remaining 24 purchases involved 22 individual tools to perform network traffic monitoring at a cost of $1.6 million with annual maintenance costs of $344,563.

Log and Event Management Tools. Log and event management tools alert system administrators to potential security or other events on Agency networks and systems. Third party assessments reported that NASA systems were lacking sufficient log management capability in the past and that system administrators needed to better monitor and maintain logs related to alerts generated by potential security events. NASA made 41 separate purchases of 20 different log and event management tools at a cost of $4.5 million with annual maintenance costs of $834,939. For example, the OCIO, CISOs, and OCSOs made 12 separate purchases of Splunk to document what events had occurred on a system and identify potential security threats at a cost of $1.3 million and annual maintenance costs of $237,245. Two of the 12 purchases were made by large projects located at the same NASA Center, and Agency officials told us there was no coordination or consolidation of these purchases. Additionally, NASA CISOs and OCSOs made 8 separate purchases of another product called Net IQ for $1 million and annual maintenance costs of $159,384. Agency personnel made 21 additional purchases of 18 other log event and management tools at a cost of $2.2 million with annual maintenance costs of $438,310.

Malware and Antivirus Tools. Malware and Antivirus Tools protect against software installed without the users knowledge designed to harm the computer or steal information. The requirement for antivirus and malware protection is common to all NASA information systems. We identified 32 separate purchases of malware and antivirus tools at a cost of $541,929 with annual maintenance costs of $221,559. For example, NASA CISOs and OCSOs made 19 separate purchases of Symantec Malware and Antivirus protection tools at a cost of $486,703 and annual maintenance costs of $129,128. In addition, in December 2010, NASA awarded the Agency Consolidated End-user Services (ACES) contract that includes Symantec Antivirus tools for all ACES end-users.

Vulnerability Management Tools. NASA employs vulnerability scanning tools to scan IT assets at every NASA location to detect and mitigate vulnerabilities. According to our survey, NASA made 32 separate purchases of vulnerability management tools at a cost of $1.7 million with annual maintenance costs of $636,562. To centrally manage vulnerability mitigation efforts, in 2005 the CIO launched the Agency Vulnerability Assessment and Remediation (AVAR) program and purchased McAfee Foundstone/McAfee Vulnerability Manager as the Agency-wide solution at a cost of $364,973 and with annual maintenance costs of $234,057. While NASA uses McAfee Vulnerability Manager to scan its approximately 140,000 system components, such scanning is also being performed under the Agency's ACES contract.

While the ACES contract was developed to consolidate NASA's IT services, we identified duplication of efforts in its vulnerability management services. Specifically, ACES uses Retina Network Security Scanner to perform scans on approximately 32,200 of NASA's 140,000 system components. While the contractor is performing scans and mitigating findings on those components, NASA's AVAR is also performing vulnerability scans on those same 32,200 system components. The OCIO could not provide cost data associated with the ACES vulnerability management services. We also identified 30 additional purchases of vulnerability management tools, which included 11 purchases of NESSUS, four purchases of IBM App Scan, two purchases of HailStorm WebApp Scanner, and 13 purchases of various other tools at a cost of $1.4 million and with annual maintenance costs of $402,505.

Patch Management Tools. Patch management is the process for identifying, acquiring, installing, and verifying patches for IT products and systems to correct software security and functionality problems. To implement patch management, NASA made 11 purchases of 9 different tools for $1.3 million with annual maintenance costs of $1.1 million. According to our survey, the NASA OCIO purchased KACE for $1.2 million and annual maintenance costs of $424,000. At the same time, one CISO and seven OCSOs purchased eight different tools to perform patch management functions for $98,467 with annual maintenance cost of $697,812.

Firewall/Boundary Protection Tools. Firewall/boundary protection tools protect against internal or external intrusion of computer networks and are ubiquitous throughout NASA's networks to monitor and control access. According to our survey, NASA made 43 separate purchases of firewall/boundary protection tools at a cost of $3.7 million with annual maintenance costs of $732,298. Specifically, the

OCIO, CISOs, and OCSOs made 20 separate purchases of Juniper boundary protection tools at a cost of $3.1 million and annual maintenance costs of $450,135. In addition, the CIO, OCSOs, and CISOs made 19 separate purchases of CISCO/Check Point boundary protection devices at a cost of $577,000 with annual maintenance costs of $353,000. Agency personnel also purchased four additional firewall/boundary protection tools at a cost of $50,460.

Configuration Management Tools. Configuration management is a collection of activities that seeks to establish and maintain the integrity of IT products and systems through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. According to our survey, NASA made 17 purchases of 15 different tools for configuration management of NASA systems at an initial cost of $442,276 with annual maintenance costs of $266,727.

Governance, Risk, and Compliance (GRC) Tools. FISMA mandates common GRC requirements to manage system security plans, track the status and corrective actions for deficiencies identified on NASA systems, and monitor the security posture of its systems and associated components. NASA made 14 purchases of 12 different tools to perform GRC activities at NASA locations at a cost of $1.7 million and annual maintenance costs of $704,012. The following are four examples of GRC expenditures at NASA:

- ITSC, a software suite that Marshall developed internally in 2003 and has annual maintenance costs of $361,000. Although this product is available to all NASA locations, only Marshall currently uses it.

- RMS from SecureInfo cost NASA $1.5 million and has annual maintenance costs of $273,000. The OCIO purchased RMS in July 2005 as the Agency-wide risk management software solution. Prior OIG reviews have noted that RMS was not user-friendly and contained incomplete information; therefore, the Agency is evaluating other solutions as potential replacements.

- Rsam was purchased by four Centers in August 2008 to meet many of the same FISMA requirements as the RMS and ITSC tools. Rsam cost $372,339 with annual maintenance costs of $80,412. Despite knowledge that RMS was the required Agency-wide solution, Centers purchased Rsam to help satisfy their FISMA requirements.

- The Information Technology Security Data Base was deployed in June 2000 at the Jet Propulsion Laboratory to meet many of the same FISMA IT security requirements that similar tools are meeting at other Centers.

Although there are information systems at NASA with unique security requirements, the nine control areas can be assessed and monitored using a common set of tools. We believe that uncoordinated purchases causes NASA to spend more than necessary on IT security software because many of the software requirements are procured individually each year versus leveraging economy of scale purchases through an enterprise purchase agreement. Such purchases by individual NASA entities may also result in redundant efforts by procurement and contract management staff and result in higher per license cost and increased maintenance due to limited quantity procurements. Furthermore, maintenance costs are often based on vendor resources used in maintaining individual maintenance agreements and are typically calculated as a percentage of the initial software purchase costs. By consolidating its requirements, reducing separate purchases, and negotiating volume discounts, NASA could have further reduced the associated annual maintenance costs.

We acknowledge that not all of the purchases identified in the nine IT security control areas created duplication or could have been consolidated. However, we believe NASA could more efficiently manage its widely distributed IT security systems by consolidating requirements. NASA IT security, procurement, and capital planning officials acknowledge overlap in the purchase of IT security tools across the Agency and agree that NASA could benefit by consolidating efforts to leverage its buying power.

Conclusion

To achieve cost savings and standardize IT resources across the Agency, NASA needs to consolidate IT security assessment and monitoring tool requirements prior to making purchasing decisions. Full implementation of two current NASA systems could assist in the effort to make more effective use of IT security funds by: 1) expanding the CPIC process to capture detailed IT security application and cost data; and 2) revitalizing the APM program to gain a better understanding of the Agency's IT security assessment and monitoring tool environment. Using this data, the ELMT could identify IT security assessment and monitoring tools for consolidation. Our survey found that NASA's DCIO, CISOs, and OCSOs spent $25.7 million for tools that are either the same or performed similar IT security management functions as other available software. We believe NASA could have reduced its purchase costs and the associated annual maintenance costs with a more effective IT investment management process that captures, consolidates, and assesses IT security tool requirements across the Agency.

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

To improve NASA's process for acquiring Agency-wide IT security assessment and monitoring tools, we made the following recommendations to the Chief Information Officer:

Recommendation 1. Ensure that IT application data capture is available to all NASA IT Investment Management System (ProSight) users.

Management's Response. The CIO concurred with our recommendation, stating that the OCIO is in the process of migrating from ProSight to a new CPIC management tool, eCPIC, and will utilize the Federal eCPIC Steering Committee to leverage ideas regarding identifying and collecting data associated with investments and for tracking and reducing spending in commodity IT areas, including for security tools. The OCIO plans to complete the migration to eCPIC in April 2013, and will develop a plan to implement the data collection process as part of the CPIC meeting scheduled for October 2013 and implement that plan by the end of FY 2014. In addition, work is underway to define the current and target state of IT security tools and to develop a transition plan to achieve the target state. This effort should be complete by the end of FY 2014.

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

Recommendation 2. Require, as part of the CPIC process, that all Agency activities identify their IT security assessment and monitoring tools and associated purchase and maintenance costs in ProSight.

Management's Response. The CIO concurred with our recommendation stating that as part of a new OMB initiative, PortfolioStat, the OCIO is assessing data requirements to support effective reporting and decision making. PortfolioStat includes an assessment of the IT security tools budget and whether opportunities exist for consolidation to eliminate duplication. The OCIO has requested data from the Centers and Mission Directorates and also plans to use data provided by the OIG during this review. Furthermore, the OCIO is working with the Chief Financial Officer to determine if changes can be made to the Agency's financial system that will provide enhanced granularity into IT spending throughout the Agency and therefore enable decision makers to identify potential investment/portfolio areas for consolidation. The OCIO is planning to complete these actions by the end of FY 2015, assuming adequate resources are available to make any necessary modifications to the financial system.

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

Recommendation 3. Ensure that the captured data is routed through the ELMT for review and consolidation of IT security assessment and monitoring tools.

Management's Response. The CIO concurred with our recommendation stating that the OCIO will establish accounts for the ELMT team in eCPIC in April 2013 when migration and training activities are complete. The OCIO will also recommend that the ELMT be represented on the CPIC Working Group and participate in working sessions to improve CPIC activities.

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

Recommendation 4. Once the above recommendations are implemented, determine if other non-major commodity IT application data could be captured using the same process in an effort to reestablish an overall APM program.

Management's Response. The CIO concurred with our recommendation, stating OMB's PortfolioStat process is providing a framework to collect data on high priority IT spending areas. In the interim, the OCIO will continue to implement the annual PortfolioStat processes and prioritize the highest value areas for consolidation to eliminate duplication. The OCIO will also continue to identify candidates for applications license consolidation in the Agency. The OCIO is planning to complete this action by the end of FY 2015.

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

APPENDIX A

Scope and Methodology

We performed this audit from October 2011 through January 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 assess NASA's ability to gather and consolidate requirements for IT security assessment and monitoring tools, we analyzed data obtained from the DCIO, CISOs, and OCSOs though questionnaires and interviews. We also interviewed personnel from ACES, AVAR, ELMT, and procurement across all NASA Centers about IT security assessment and monitoring tools and acquisition processes, CPIC, and APM.

The questionnaires focused on tools purchased to manage nine IT security control areas – intrusion detection, network traffic monitoring, log event management, malware and antivirus, vulnerability management, patch management, firewall/boundary protection, configuration management, and GRC. We requested information for purchases and the associated maintenance costs for tools currently in use.

We used three different questionnaires, with the questionnaire sent to the DCIO asking specifically about tools purchased for an Agency-wide solution and additional questions for the CISOs and OCSOs to identify the systems for which they were responsible. We distributed 12 CISO questionnaires and 140 OCSO questionnaires, which included the responsible IT security official for most of the Agency's computer systems as identified in the system inventory. We distributed the questionnaires in October 2011. We received responses from the DCIO, the CISOs, and 98 of the OCSOs by June 2012 – overall, a 73 percent response rate. Our analysis of questionnaire responses identified what IT security assessment and monitoring tools the DCIO, CISOs, and OCSOs purchased and the number of purchases that were made in the nine IT security control areas.

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

- Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)
- Executive Order 13589, "Promoting Efficient Spending," November 9, 2011
- OMB Memorandum M-11-29, "Chief Information Officer Authorities," August 8, 2011
- OMB Memorandum M-12-10, "Implementing PortfolioStat," March 30, 2012
- OMB Memorandum M-12-12, "Promoting Efficient Spending to Support Agency Operations," May 11, 2012
- NASA Policy Directive (NPD) 1000.0A, "NASA Governance and Strategic Management Handbook," August 13, 2008
- NPR 2800.1B, "Managing Information Technology," March 20, 2009
- NPR 2810.1A, "Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)"
- NPR 7120.7, "NASA Information Technology and Institutional Infrastructure Program and Project Manager Requirements," November 3, 2008
- NASA OCIO Information Resources Management Strategic Plan, June 2011
- NASA Memorandum, "Solutions for Enterprise-Wide Procurement (SEWP) Contract," August 15, 2011
- NASA Memorandum, "FY09 Acquisition of IT Products and Service Guidance," March 27, 2008

Use of Computer-Processed Data. We did not use computer-processed data in the performance of this audit. However, we did obtain information from the OCIO that was a result of data manually entered into a spreadsheet to report NASA's System Inventory and individuals (CISOs and OCSOs) responsible for the security of the systems included in the inventory. This information was verified during the distribution of questionnaires to all CISOs and OCSOs.

Review of Internal Controls

We examined internal controls that would allow NASA to acquire IT security assessment and monitoring tools, achieve efficiencies, improve integration and security, and ensure alignment of IT with mission. We discussed the control weaknesses identified in the Results section of this report. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

During the past five years, the NASA Office of Inspector General (OIG) issued one report of particular relevance to the subject of this report: "Final Memorandum on Review of NASA's Consolidation of Information Technology Purchases under the Outsourcing Desktop Initiative" (IG-09-001-R, November 6, 2008). Unrestricted reports can be accessed over the Internet at http://oig.nasa.gov/audits/reports/FY13/index.html.

QUESTIONNAIRES

To collect information on IT security assessment and monitoring tools in use across the Agency, we developed three different questionnaires: one for the DCIO, which focused on tools purchased as Agency-wide solutions; one for CISOs; and one for OCSOs, which included a section to identify the systems for which they were responsible.

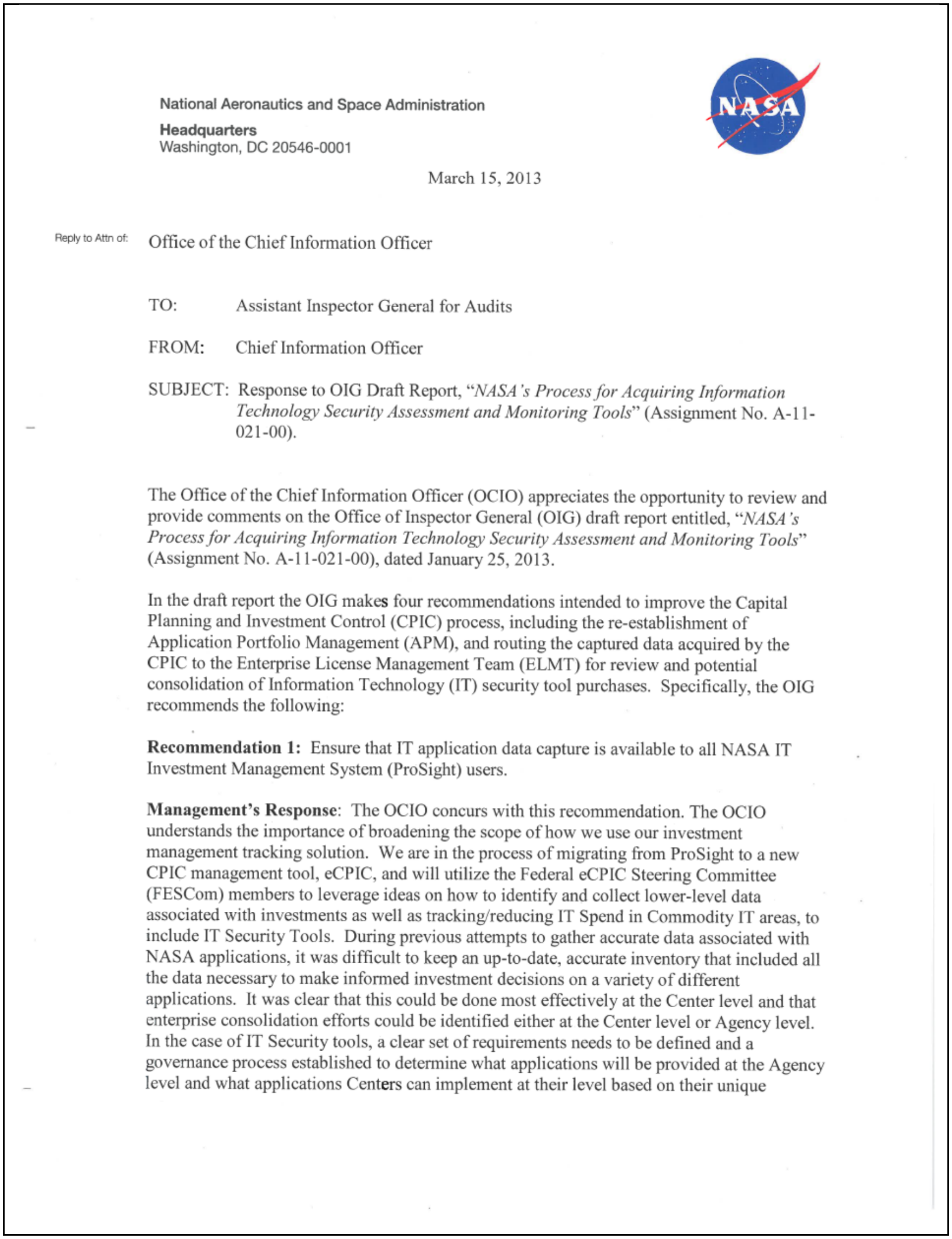
Between October 19 and December 6, 2011, we distributed the questionnaires to the DCIO, 12 CISOs, and 140 OCSOs. We received the DCIO's response January 4, 2012. We received responses from all 12 CISOs by June 25, 2012. The last of the 98 responses from OCSOs was received January 25, 2012. Overall, the response rate was 73 percent (153 distributed and 111 returned).

Table 2 below summarizes the survey results.

Table 2. Summary of Responses to Questionnaires

Questionnaire Recipient	Return Rate	Purchase Costs of IT Tools	Annual Maintenance Costs
DCIO	100% (1 of 1)	$ 7,340,973	$1,762,057
CISOs	100% (12 of 12)	5,882,553	2,278,892
OCSOs	70% (98 of 140)	6,711,416	1,762,633
Total	**73% (111 of 153)**	**$19,934,942**	**$5,803,582**

MANAGEMENT COMMENTS



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

March 15, 2013

Reply to Attn of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

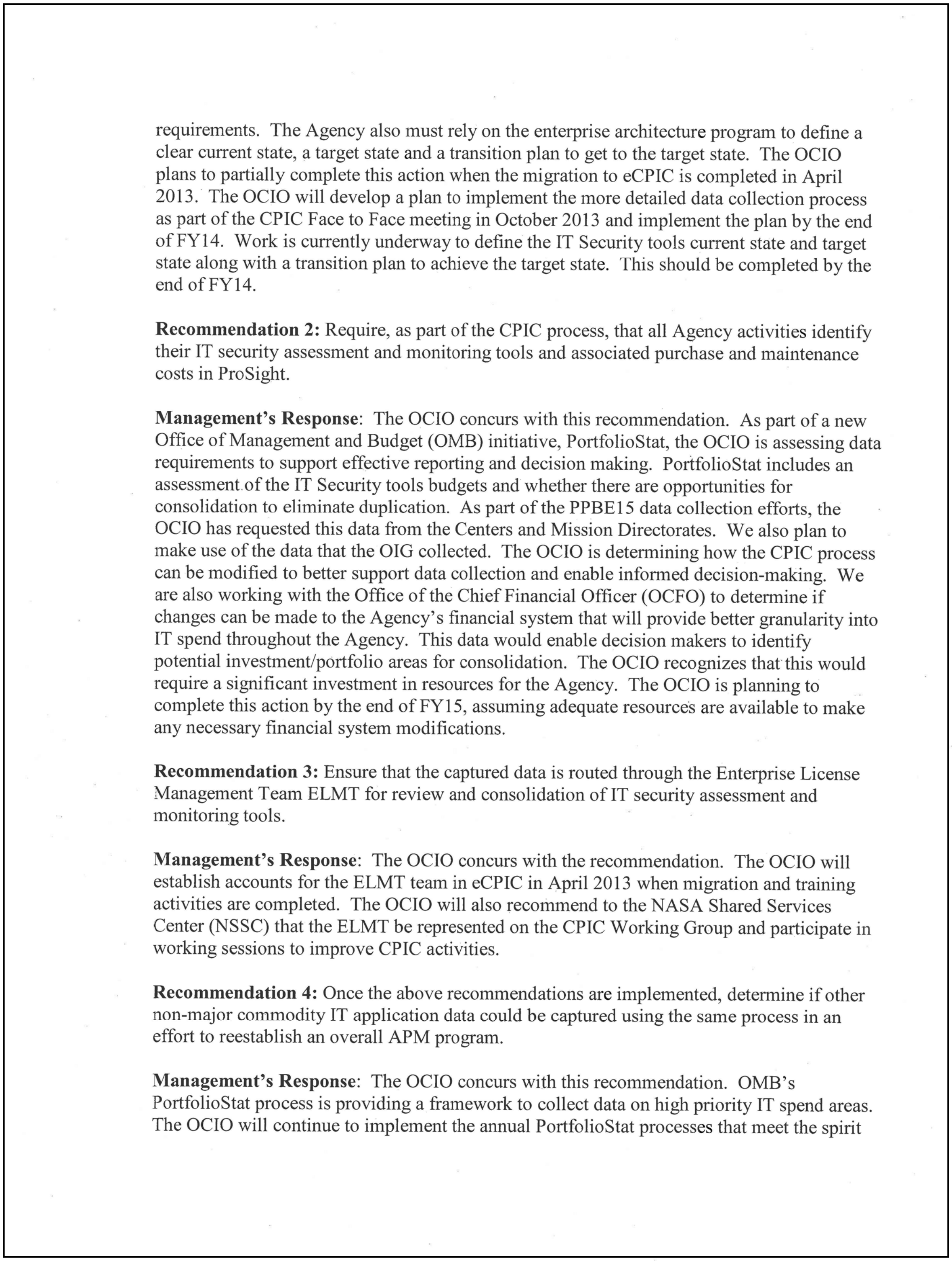
SUBJECT: Response to OIG Draft Report, "*NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools*" (Assignment No. A-11-021-00).

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to review and provide comments on the Office of Inspector General (OIG) draft report entitled, "*NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools*" (Assignment No. A-11-021-00), dated January 25, 2013.

In the draft report the OIG makes four recommendations intended to improve the Capital Planning and Investment Control (CPIC) process, including the re-establishment of Application Portfolio Management (APM), and routing the captured data acquired by the CPIC to the Enterprise License Management Team (ELMT) for review and potential consolidation of Information Technology (IT) security tool purchases. Specifically, the OIG recommends the following:

Recommendation 1: Ensure that IT application data capture is available to all NASA IT Investment Management System (ProSight) users.

Management's Response: The OCIO concurs with this recommendation. The OCIO understands the importance of broadening the scope of how we use our investment management tracking solution. We are in the process of migrating from ProSight to a new CPIC management tool, eCPIC, and will utilize the Federal eCPIC Steering Committee (FESCom) members to leverage ideas on how to identify and collect lower-level data associated with investments as well as tracking/reducing IT Spend in Commodity IT areas, to include IT Security Tools. During previous attempts to gather accurate data associated with NASA applications, it was difficult to keep an up-to-date, accurate inventory that included all the data necessary to make informed investment decisions on a variety of different applications. It was clear that this could be done most effectively at the Center level and that enterprise consolidation efforts could be identified either at the Center level or Agency level. In the case of IT Security tools, a clear set of requirements needs to be defined and a governance process established to determine what applications will be provided at the Agency level and what applications Centers can implement at their level based on their unique



requirements. The Agency also must rely on the enterprise architecture program to define a clear current state, a target state and a transition plan to get to the target state. The OCIO plans to partially complete this action when the migration to eCPIC is completed in April 2013. The OCIO will develop a plan to implement the more detailed data collection process as part of the CPIC Face to Face meeting in October 2013 and implement the plan by the end of FY14. Work is currently underway to define the IT Security tools current state and target state along with a transition plan to achieve the target state. This should be completed by the end of FY14.

Recommendation 2: Require, as part of the CPIC process, that all Agency activities identify their IT security assessment and monitoring tools and associated purchase and maintenance costs in ProSight.

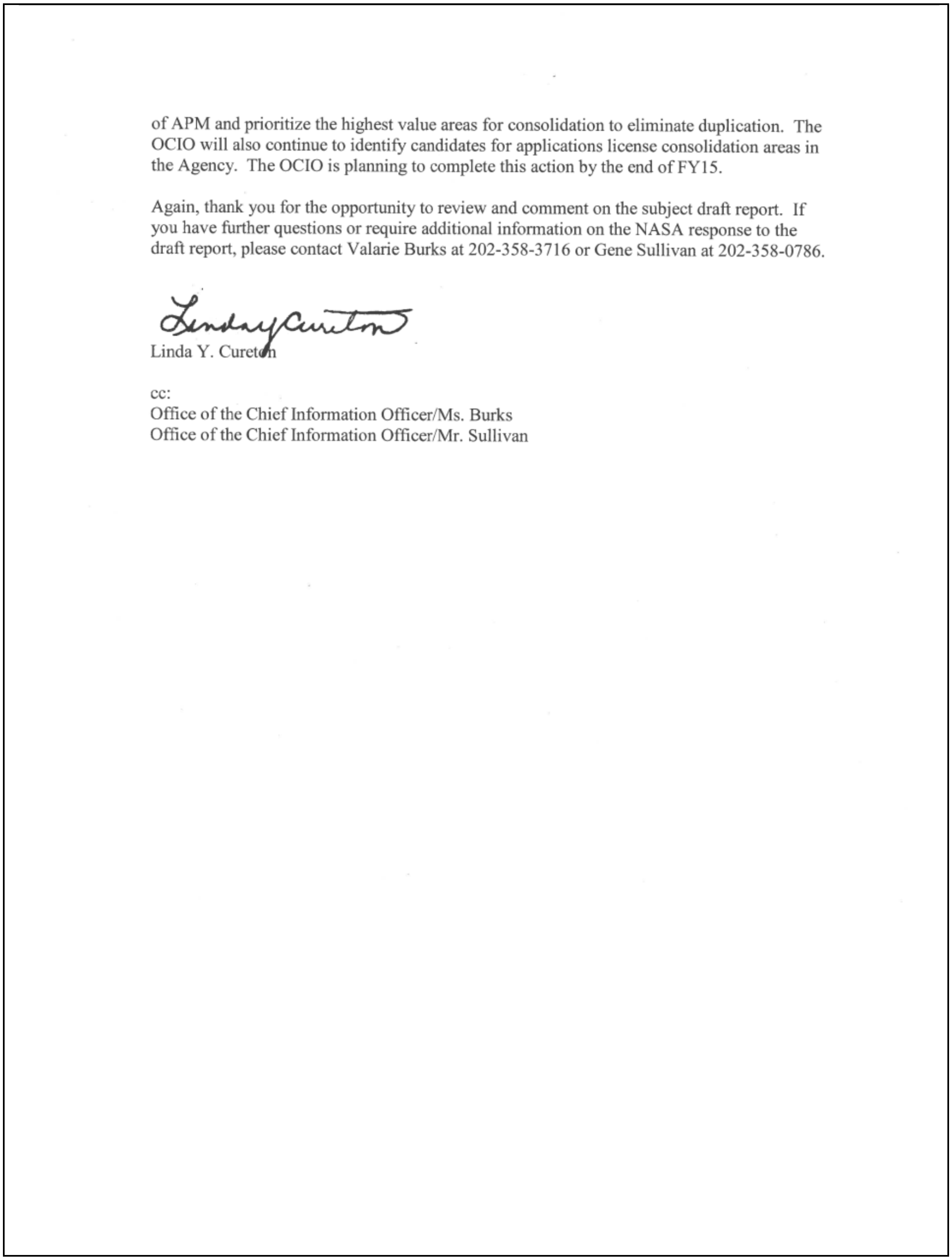
Management's Response: The OCIO concurs with this recommendation. As part of a new Office of Management and Budget (OMB) initiative, PortfolioStat, the OCIO is assessing data requirements to support effective reporting and decision making. PortfolioStat includes an assessment of the IT Security tools budgets and whether there are opportunities for consolidation to eliminate duplication. As part of the PPBE15 data collection efforts, the OCIO has requested this data from the Centers and Mission Directorates. We also plan to make use of the data that the OIG collected. The OCIO is determining how the CPIC process can be modified to better support data collection and enable informed decision-making. We are also working with the Office of the Chief Financial Officer (OCFO) to determine if changes can be made to the Agency's financial system that will provide better granularity into IT spend throughout the Agency. This data would enable decision makers to identify potential investment/portfolio areas for consolidation. The OCIO recognizes that this would require a significant investment in resources for the Agency. The OCIO is planning to complete this action by the end of FY15, assuming adequate resources are available to make any necessary financial system modifications.

Recommendation 3: Ensure that the captured data is routed through the Enterprise License Management Team ELMT for review and consolidation of IT security assessment and monitoring tools.

Management's Response: The OCIO concurs with the recommendation. The OCIO will establish accounts for the ELMT team in eCPIC in April 2013 when migration and training activities are completed. The OCIO will also recommend to the NASA Shared Services Center (NSSC) that the ELMT be represented on the CPIC Working Group and participate in working sessions to improve CPIC activities.

Recommendation 4: Once the above recommendations are implemented, determine if other non-major commodity IT application data could be captured using the same process in an effort to reestablish an overall APM program.

Management's Response: The OCIO concurs with this recommendation. OMB's PortfolioStat process is providing a framework to collect data on high priority IT spend areas. The OCIO will continue to implement the annual PortfolioStat processes that meet the spirit



of APM and prioritize the highest value areas for consolidation to eliminate duplication. The OCIO will also continue to identify candidates for applications license consolidation areas in the Agency. The OCIO is planning to complete this action by the end of FY15.

Again, thank you for the opportunity to review and comment on the subject draft report. If you have further questions or require additional information on the NASA response to the draft report, please contact Valarie Burks at 202-358-3716 or Gene Sullivan at 202-358-0786.

Linda Y. Cureton

cc:
Office of the Chief Information Officer/Ms. Burks
Office of the Chief Information Officer/Mr. Sullivan

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Associate Administrator for Aeronautics Research
Associate administrator for Science
Associate Administrator for Human Exploration and Operations
Chief Information Officer
Associate Chief Information Officer for Capital Planning and Governance
Deputy Chief Information Officer for Information Technology Security
Chief Acquisition Officer/Assistant Administrator for Procurement
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 Organization, Efficiency, and Financial Management
House Committee on Science, Space, and Technology
  Subcommittee on Oversight
  Subcommittee on Space

Major Contributors to the Report:

Wen Song, Director, Information Technology Directorate
Vincent Small, Project Manager
Bret Skalsky, Team Lead
Bessie Cox, Auditor
Chris Reeves, Information Technology Specialist
Mike Beims, Computer Engineer

MARCH 18, 2013

REPORT NO. IG-13-006

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit http://oig.nasa.gov/audits/reports/FY12/ 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.