

SEPTEMBER 14, 2010

AUDIT REPORT

OFFICE OF AUDITS

AUDIT OF NASA'S EFFORTS TO CONTINUOUSLY
MONITOR CRITICAL INFORMATION TECHNOLOGY
SECURITY CONTROLS

OFFICE OF INSPECTOR GENERAL



National Aeronautics and
Space Administration

Final report released by:

A handwritten signature in black ink, appearing to read 'PKMJA', written in a cursive style.

Paul K. Martin
Inspector General

Acronyms

CIO	Chief Information Officer
CIS	Center for Internet Security
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IT	Information Technology
NITR	NASA Information Technology Requirement
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

OVERVIEW

AUDIT OF NASA'S EFFORTS TO CONTINUOUSLY MONITOR CRITICAL INFORMATION TECHNOLOGY SECURITY CONTROLS

The Issue

As part of our annual audit of NASA's compliance with the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) evaluated whether NASA had processes in place at selected Centers to continuously monitor critical information technology (IT) security controls. Specifically, we assessed whether NASA had effective processes in place to ensure that its computers remained securely configured and free of vulnerabilities and that software patches were timely and appropriately applied. We also reviewed internal controls as appropriate. We performed our site work at Goddard Space Flight Center, Johnson Space Center, Kennedy Space Center, and Langley Research Center. See Appendix A for details of the audit's scope and methodology.

Results

Continuous monitoring of security controls is an essential element of an organization's IT security program. We found that NASA's processes for continuous monitoring of its operating system configurations, system vulnerabilities, and software patch levels were not fully effective for protecting critical Agency information resources. For example, none of the four Centers we visited monitored operating system configurations on their computer servers to ensure they remained securely configured over time. Although all four Centers had implemented NASA's vulnerability management process that includes automated vulnerability discovery, prioritized remediation, and the quarantine of computers with unmitigated vulnerabilities, we found that this process could be improved by adding a control to provide assurance that 100 percent of the Centers' computer networks are continuously monitored. Similarly, the Centers could improve the implementation of their software patch management process by ensuring that all of the Centers' computers are included in the process.

In a March 2006 OIG audit report, we recommended that Centers establish inventories of their computers.¹ Although the Agency concurred with that recommendation, NASA decided to implement a single Agency-wide inventory instead of Center-level inventories, which delayed implementation until at least September 2010. In this review, we found that the lack of complete and up-to-date inventories is a barrier to effective

¹ "NASA's Implementation of Patch Management Software Is Incomplete" (IG-06-007, March 17, 2006).

monitoring of IT security controls. Accurate inventory lists increase the effectiveness of an IT security program by providing a means to verify that 100 percent of the computers in the Agency's network are subject to configuration, vulnerability, and patch monitoring. Until NASA establishes a complete inventory of its network resources, Centers will be unable to fully implement these key IT security controls and NASA's IT security program will not be fully effective in protecting the Agency's valuable IT resources from potential exploitation.

Management Action

In order to strengthen the Agency's IT security program, we urged NASA to expedite implementation of our 2006 recommendation to establish complete inventories of Agency computer networks – to include computers, firewalls, routers, and switches.² In addition, we recommended that NASA's Chief Information Officer require the Centers to (1) continuously monitor computer server operating system configuration settings and (2) implement a process to verify that vulnerability monitoring includes 100 percent of applicable network devices. We also found that NASA did not require system owners to install NASA's patch management program but made no recommendation concerning this issue because NASA issued corrective policy during the course of our audit.

In response to our July 13, 2010, draft report, the Chief Information Officer (CIO) concurred with our recommendation that NASA establish inventories of the computers connected to its networks. The CIO stated that NASA has developed an inventory system that became operational in July 2010. Our preliminary review of the inventory system found that it contained detailed information on various computers to include Internet protocol address, computer operating system (when appropriate), device type, location, and software patch and vulnerability status. As of September 9, 2010, the inventory system listed more than 163,000 devices that according to NASA management represents a "significant proportion" of the total devices connected to NASA's networks.

The CIO also concurred with our recommendation to monitor computer server configuration settings and stated that a security configuration baseline will be developed for one server operating system (Windows Server 2003) by January 1, 2011, and that guidance requiring monitoring of compliance with this configuration will be issued by August 2011. We do not believe that these actions are fully responsive to our recommendation because they do not apply to all server operating systems used by NASA. In addition, compliance monitoring for this single server operating system will not be implemented until August 2011. Accordingly, we have requested that the CIO further address the scope and timeliness of the Agency's planned action.

² As we noted in our March 2006 report, "NASA's Implementation of Patch Management Software Is Incomplete" (IG-06-007), an ideal inventory would consist of a current, complete listing of all NASA computers, by Center, maintained in one location. The inventory would ideally include the computer identification number, Internet protocol address (when appropriate), operating system, and location.

The CIO partially concurred with our recommendation concerning the monitoring of devices connected to NASA's networks, stating that, in her view, it is impossible to ensure that 100 percent of devices are monitored for vulnerabilities. Although we agree that NASA's vulnerability management program may never attain 100 percent coverage of all network devices, we believe that NASA can take steps to move toward this goal. Accordingly, we are requesting that NASA implement processes to measure current vulnerability scanning coverage and to increase that coverage over time.

Finally, the CIO requested that we remove our finding that NASA's process for monitoring software patches was not effective because the CIO issued a policy to address this issue during the course of our audit. As discussed in the report, at the time of our site visits to the Centers NASA did not require owners of Agency information systems to implement NASA's patch monitoring and reporting solution (PatchLink) and, as a result, NASA did not have assurance that all applicable systems were at the correct software patch level. After we notified Agency managers of our preliminary finding and indicated that we intended to recommend that the Agency require system owners to implement Patchlink, the CIO issued a policy requiring Patchlink implementation. In the draft report, we acknowledged that this policy should address our finding and, therefore, did not recommend further action. We believe it is appropriate to discuss the issue and NASA's corrective action in the final public version of our report.

See Appendix B for the full text of management's comments.

CONTENTS

INTRODUCTION

Background _____	1
Objectives _____	2

RESULTS

NASA Did Not Monitor Its Computer Servers to Ensure They Remained Securely Configured _____	3
NASA's Vulnerability Management Program Could Be Improved _	6
NASA's Process for Monitoring Agency IT Systems for Software Patches Was Not Effective _____	8

APPENDIX A

Scope and Methodology _____	11
Review of Internal Controls _____	12
Prior Coverage _____	12

APPENDIX B

Management Comments _____	13
---------------------------	----

APPENDIX C

Report Distribution _____	16
---------------------------	----

INTRODUCTION

Background

As part of our Federal Information Security Management Act (FISMA) audit for fiscal year (FY) 2009, we assessed NASA processes for meeting the continuous security control monitoring requirement defined in the National Institute of Standards and Technology Special Publication 800-37.³ Specifically, we reviewed Center processes for maintaining the security of their systems by continuously monitoring key controls related to computer server operating system configuration, vulnerability detection and remediation, and software patching. We conducted our review at four Centers: Goddard Space Flight Center, Johnson Space Center, Kennedy Space Center, and Langley Research Center. Computer systems at these Centers support operations that span all of NASA's primary mission areas: Aeronautics Research (Langley), Space Exploration and Space Operations (Johnson and Kennedy), and Science (Goddard).

In general, configuration management is the process of assessing and, if necessary, modifying settings to ensure that critical network resources including computer servers remain in a secure state and are not vulnerable to exploitation. Often, operating systems on computer servers are configured by the vendor for ease-of-deployment and ease-of-use rather than for security, leaving them exploitable in their default state. To address this issue, the Center for Internet Security (CIS) has published recommended configuration settings, called benchmarks, for securing a wide variety of computer operating systems. NASA has adopted the CIS benchmarks as a best practice for the secure configuration of operating systems on its computer servers.

Unfortunately, initializing a computer server's operating system to a secure state is not sufficient to ensure ongoing protection against exploitation. Because operating system configurations can change when software patches are applied or when computers are upgraded, it is necessary to monitor operating systems on a continuous basis to ensure they remain securely configured.

Accordingly, continuous monitoring of security controls is an essential element of an organization's information technology (IT) security program. The goal of continuous monitoring is to determine whether a system's key security controls continue to be effective over time in light of changes to hardware or software. A well-designed and well-managed continuous monitoring program can transform an otherwise static security control assessment and risk determination process to a dynamic process that provides essential information about a system's security status. This, in turn, enables officials to

³ "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004.

take timely risk mitigation actions and make risk-based decisions regarding the operation of the information system.

Remediating system vulnerabilities and applying software patches also help prevent the exploitation of vulnerabilities within an organization's information systems. Vulnerabilities are software flaws or system misconfigurations that can be exploited to gain access to or control of an information system. Vulnerability scanners are specialized commercial software programs that automate the vulnerability detection process. Vulnerability scanners search large databases of known vulnerabilities associated with commonly used computer operating systems and software applications. When a match is found in the database, the scanner alerts the operator to a possible vulnerability. The scanners rank vulnerabilities according to their potential to harm the system, allowing organizations to prioritize and address their most critical vulnerabilities. Most vulnerability scanners also generate reports to help system administrators fix discovered vulnerabilities. System administrators commonly remediate vulnerabilities by applying a software patch, by updating a system's configuration, or by adding a compensating control such as encryption to ensure data integrity.⁴

NASA's Chief Information Officer (CIO) is responsible for developing and overseeing Agency-wide, risk-based, and cost-effective policies and procedures for safeguarding NASA's IT resources. Center CIOs and Center Information Technology Security Managers are responsible for enforcing security policies and procedures by identifying potential risks and implementing operational and technical controls that cost-effectively mitigate the identified risks. These officials are also responsible for implementing measures to continuously monitor key security controls to ensure the availability, confidentiality, and integrity of Agency IT resources.

Objectives

We examined whether NASA had effective processes for continuously monitoring key IT security controls at four of its Centers. Specifically, we assessed whether NASA had processes in place for

- ensuring computer server operating systems remain securely configured (configuration management);
- detecting and remediating system technical vulnerabilities (vulnerability management); and
- ensuring that systems are at the correct software patch level (patch management).

We also reviewed internal controls as appropriate. See Appendix A for details of the audit's scope and methodology.

⁴ Software patches are pieces of computer code developed to address problems in computer software. The patches enable new functionality or address security flaws in the software.

NASA DID NOT MONITOR ITS COMPUTER SERVERS TO ENSURE THEY REMAINED SECURELY CONFIGURED

Although NASA requires Agency-wide use of CIS operating system configuration settings for securing Agency computer servers, the four Centers we visited did not have effective processes in place to ensure their computer servers remained securely configured over time. This occurred because NASA did not require Centers to continuously monitor their computer servers against the respective CIS benchmarks. Further, because Centers did not have complete inventories of their computers, they could not confirm that the applicable benchmarks had been applied to all equipment.

Regular monitoring of server configurations is essential for maintaining the security of NASA's computer systems and networks. For example, improperly configured and unmonitored computer servers are susceptible to compromise and thus may be used by intruders to gain access to NASA's computer network. Once inside, the intruder can use the compromised server to exploit other weaknesses, which could result in the loss or impairment of Agency IT resources.

Centers Need to Monitor Their Computer Server Configurations

Since 2004, the NASA Office of the Chief Information Officer (OCIO) has required the Agency-wide use of applicable CIS-recommended benchmarks for the secure configuration of computer server operating systems. In addition, OCIO recommended using an automated scoring tool developed by CIS (the CIS Configuration Assessment Tool) as a way for Centers to validate implementation of the benchmarks. In 2007, OCIO updated its policy for configuration management by establishing a timeframe for meeting performance targets, by operating system, for different benchmarks. For example, by FY 2007 Centers should have met 100 percent of benchmark settings for all Windows-based servers and 80 percent of benchmark settings for all other computer server platforms.

Although Center employees responsible for IT security were aware of the requirement to configure server operating systems according to the applicable benchmarks, none of the four Centers we visited had a process in place for monitoring their computer servers to ensure that they remained securely configured over time. Indeed, Center employees stated that such monitoring was not required. We also found that none of the Centers we visited regularly used the OCIO-recommended CIS Configuration Assessment Tool to test their computer server configurations against the related benchmarks.

Computer Servers Were Not Securely Configured

We tested the configuration settings of selected computer servers at the Centers we visited to determine whether they met OCIO-required performance standards. We grouped the servers by operating system: servers that used Microsoft Windows and servers that did not. We then tested the servers' compliance with the appropriate CIS benchmarks. We tested 15 Windows-based servers and 7 Unix- and Linux-based servers. The Windows servers that we tested met an average of 68 percent of the benchmarks while the Unix and Linux servers that we tested met an average of 46 percent of the benchmarks.

NASA could have detected and corrected these security weaknesses if it had processes in place to monitor servers to ensure they remained securely configured in accordance with recognized best practices and Agency IT security requirements. Because Centers did not monitor the configuration of their computer servers, Agency systems contained improperly configured servers, which are susceptible to exploitation and loss or impairment of mission-critical IT resources.

As noted above, the Centers did not have complete inventories of the computers linked to their networks. Accordingly, we were unable to quantify the number of Agency computer servers that were not being adequately monitored for compliance with the applicable benchmarks.

In a March 2006 review, we recommended that Centers establish inventories of the computers connected to their networks. However, the Agency has not yet developed these inventories.⁵ Until NASA establishes an inventory of all computers connected to its networks, the Agency's IT security program will not be fully effective in protecting its IT resources from potential exploitation.

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

In order to strengthen the Agency's IT security program, we reiterate our 2006 recommendation that NASA establish inventories of the computers connected to its networks. Moreover, we urge NASA to expedite implementation of this recommendation. We also made the following recommendation.

Recommendation 1. The NASA CIO should require Centers to monitor computer server operating system configuration for compliance with CIS benchmarks and related OCIO-mandated performance targets.

⁵ NASA decided to implement a single Agency-wide inventory instead of separate Center inventories, which NASA officials said has delayed the process.

Management's Response. The CIO concurred, stating that an Agency-wide inventory of computers connected to NASA networks, the IT Security Enterprise Data Warehouse, became operational in July 2010. Information for the inventory comes from network vulnerability scans, NASA's patch management and reporting system (PatchLink), and other sources. In addition, the CIO stated that NASA is developing security configuration baselines for computer server operating systems and is implementing tools that can monitor compliance with these baselines. OCIO plans to publish a baseline for the Windows 2003 server operating system by January 1, 2011, and will require monitoring for compliance with the baseline by August 1, 2011.

Evaluation of Management's Response. Management's comments are not fully responsive to the intent of the recommendation. First, management's proposed actions are not comprehensive because they only address the Windows 2003 server, just one of the many computer server operating systems used by the Agency. Second, monitoring of just this single computer server operating system will not begin until August 2011, a year from the date of our recommendation. Office of Management and Budget Circular No. A-123, "Management's Responsibility for Internal Control," revised December 2004, requires that managers take timely and effective actions to address issues, such as OIG recommendations. Circular A-123 also states that correcting issues is an integral part of management accountability and must be considered a priority by the Agency. Therefore, we are requesting that the CIO provide additional comments to address the above issues in response to this final report.

NASA'S VULNERABILITY MANAGEMENT PROGRAM COULD BE IMPROVED

Although all four Centers that we visited regularly monitored their computer networks for technical vulnerabilities using a vulnerability scanning tool, none of the Centers could demonstrate that this monitoring process provided complete coverage of the Center's computer networks. This occurred because, as noted earlier, the Centers did not have complete computer inventories and therefore could not ensure that their vulnerability detection and mitigation process had been applied to 100 percent of the computers connected to their networks. As a result, some computers may not undergo vulnerability scanning and thus may contain undetected and uncorrected vulnerabilities.

NASA Should Verify that All Applicable Network Devices Undergo Vulnerability Monitoring

None of the Centers that we visited could demonstrate that their vulnerability monitoring processes provided complete coverage of all applicable devices (e.g., computers, routers, and firewalls) connected to their networks. Verifying that all applicable devices connected to Center networks undergo regular vulnerability monitoring is necessary because vulnerability scanning tools, including the tool NASA uses, cannot scan devices for vulnerabilities if those devices are positioned behind internal firewalls or are turned off.

Vulnerability scanners function by attempting to communicate with all applicable devices connected to the network or network segment that is being scanned by sending a message to each device and waiting for a reply. When a reply is received, communication is established and that device can be scanned for potential vulnerabilities. Firewalls, however, block messages from reaching devices that are positioned behind the firewall, preventing a vulnerability scanner from scanning those devices. Similarly, devices that are connected to the network but are not turned on will not respond to a communication request from the scanner and will therefore not be scanned for vulnerabilities.

Because Centers did not verify the completeness of their vulnerability scans, high-risk vulnerabilities could go undetected during scanning and uncorrected during the mitigation process. This creates an environment where risk cannot be accurately measured and increases the possibility that vulnerabilities will be exploited through attacks. Exploitation of NASA's high-risk systems can have severe consequences on NASA assets, operations, or personnel. For example, in January 2009 an intrusion resulting from an undetected vulnerability (in this case a server misconfiguration) resulted in the theft of 22 gigabytes of sensitive program data from a NASA Center.

We believe that NASA can improve its vulnerability management program and prevent future exploitations by adding a “completeness check” to verify that all applicable devices connected to its networks are actually scanned. For example, matching entries from a Center-wide inventory of network devices to corresponding entries in a vulnerability scanning report is one way Centers could verify whether all applicable network devices undergo regular vulnerability monitoring.

Recommendation, Management’s Response, and Evaluation of Management’s Response

To reduce the risk of undetected and uncorrected vulnerabilities, we made the following recommendation.

Recommendation 2. The NASA CIO should require that Centers implement a process to validate that 100 percent of applicable network devices, including computers, routers, and firewalls, undergo regular monitoring for technical vulnerabilities.

Management’s Response. The CIO partially concurred, stating that NASA Information Technology Requirement (NITR) 2810-24, January 2010, requires that all IT devices connected to NASA networks be subjected to monthly network-based vulnerability scans. In addition, NITR 2810-24 requires that Center IT Security Managers oversee vulnerability scanning, reporting, and mitigation activities at their respective Centers to ensure that all requirements are met. Although OCIO strongly agreed that all applicable network devices should undergo regular vulnerability scanning, OCIO stated that ensuring 100 percent of devices are actually monitored was not possible.

Evaluation of Management’s Response. While we agree that ensuring 100 percent of applicable devices connected to NASA’s networks are monitored for vulnerabilities is probably an unattainable goal, OCIO needs to take some action toward meeting the intent of this recommendation. In our judgment, NASA could implement processes to measure the vulnerability scanning coverage of its computer networks and, over time, increase that coverage. Therefore, we request that the CIO provide additional comments that describe actions NASA can take to incrementally increase vulnerability scanning coverage of devices connected to Agency computer networks.

NASA'S PROCESS FOR MONITORING AGENCY IT SYSTEMS FOR SOFTWARE PATCHES WAS NOT EFFECTIVE

Ensuring that all computers connected to a NASA network have received the most current software updates is not only required by Agency policy, but is essential to maintaining the security of Agency computer systems and networks. Unpatched computers may contain vulnerabilities that, if exploited, could adversely affect the availability, confidentiality, and integrity of Agency systems and data. As part of its effort to monitor and report the software patch status of its computers, NASA uses a commercial patch management program called PatchLink. PatchLink requires the installation of software “agents” (programs) that communicate with a PatchLink server to determine, based on security policy, what patches need to be installed on the host computer to maintain effective network security. However, we found that at the time of our site visits (March through June 2009), NASA did not require system owners to implement NASA’s software patch monitoring and reporting solution (PatchLink).

NASA Did Not Require System Owners to Implement PatchLink

NASA policy requires that all computer systems connected to an Agency network implement an effective software patch management program that includes verification that patches have been properly applied.⁶ As noted above, NASA uses PatchLink to satisfy this requirement. However, we found that at the time of our site visits, NASA did not require system owners to install PatchLink on their network-connected devices. One reason commonly given by Center IT security personnel for why they did not install PatchLink was that PatchLink sometimes adversely affected their IT system’s performance. However, Center IT personnel did not provide evidence to back up this assertion.

We communicated to OCIO our preliminary findings related to Centers’ patch management practices and indicated that we would recommend that OCIO require system owners to implement NASA’s patch monitoring program.

⁶ NASA Interim Technical Requirement 2810.1A, “Security of Information Technology,” May 2006.

In January 2010, OCIO issued policy⁷ requiring system owners to implement a comprehensive patch monitoring program:

To fulfill patch reporting requirements, all NASA IT devices and all devices on a NASA non-guest network shall either:

- a. Have the Agency patch management/reporting software agent installed. The software agent automatically reports patch status to the ITSEC-EDW. This requirement is applicable to all devices that can execute the Agency patch management/reporting software agent; or
- b. Be registered in the ITSEC-EDW, with patch status reported manually in ITSEC EDW by the second Monday of each month. This requirement applies only to devices that cannot execute the Agency patch management/reporting software agent.

The policy also requires that Center Information Technology Security Managers oversee patch management and reporting activities to ensure that all requirements are met. Accordingly, a recommendation to address this finding was not necessary.

⁷ NITR 2810-24, "NASA IT Device Vulnerability Management," January 28, 2010.

Scope and Methodology

We performed our audit from January 2009 through June 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our work 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.

We assessed whether NASA had effective processes in place for configuration management, vulnerability management, and patch management that met the continuous security control monitoring requirement defined in National Institute of Standards and Technology Special Publication 800-37 at four Centers: Goddard Space Flight Center, Johnson Space Center, Kennedy Space Center, and Langley Research Center.

We developed questionnaires addressing each of those processes. During site visits, we used these questionnaires to interview NASA and contractor staff responsible for each area. We also evaluated processes and tools they used to maintain operating system configurations, to detect and remediate technical vulnerabilities, and to apply software patches. Finally, we conducted configuration tests on Center computer servers to assess compliance with Agency configuration management procedures.

We reviewed the following Federal and Agency criteria, policies, and procedures:

- National Institute for Standards and Technology Special Publication 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems,” May 2004;
- National Institute for Standards and Technology Special Publication 800-40, Version 2.0, “Creating a Patch and Vulnerability Management Program,” November 2005;
- NASA Procedural Requirements 2810.1A, “Security of Information Technology,” May 16, 2006;
- NASA Standard Operating Procedure, ITS-SOP-0012, “Patch Selection and Reporting Procedures,” July 2007;
- NASA Interim Technology Requirement 2810-12, “Continuous Monitoring,” May 18, 2008;

- NASA OCIO Memorandum, “Center for Internet Security (CIS) Consensus Benchmarks,” September 2, 2004;
- NASA OCIO Memorandum, “FY 2007 and FY 2008 Patch Management and Security Configuration Metrics,” April 4, 2007;
- NASA OCIO Memorandum, “Supplemental FY08 Guidance for Agency Security Configurations Standards and FDCC [Federal Desktop Core Configurations] Reporting,” February 20, 2008; and
- NASA OCIO Memorandum, “FY 2009 Scanning and Vulnerability Elimination or Mitigation,” February 6, 2009.

Computer-Processed Data. We relied on data produced from a commercial software program to perform configuration tests on NASA computer servers. Specifically, we used the CIS Configuration Assessment Tool to assess computer server operating system compliance with the applicable CIS benchmarks. We did not validate the data produced by the tool because this tool is widely accepted as a reliable source for providing information on operating system configuration settings.

Review of Internal Controls. We reviewed internal controls for NASA’s IT security program related to authority, responsibility, and organizational structure. We also reviewed IT security procedures governing configuration management, vulnerability detection and mitigation, and software patch management. The control weaknesses we identified are discussed in the Results section of this report. Our recommendations, if implemented, will correct the identified control weaknesses.

Prior Coverage. During the last 5 years, the NASA OIG and the Government Accountability Office (GAO) have issued two reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at <http://oig.nasa.gov/audits/reports/FY10> (NASA OIG) and <http://www.gao.gov> (GAO).

NASA Office of Inspector General

“NASA’s Implementation of Patch Management Software Is Incomplete” (IG-06-007, March 17, 2006)

Government Accountability Office

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

MANAGEMENT COMMENTS

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



AUG 2 - 2010

Reply to Attn. of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits
FROM: Chief Information Officer
SUBJECT: Draft Audit Report, "Information Technology Security: Improvements Needed in NASA's Continuous Monitoring Processes" (Assignment No. A-09-004-02)

The Office of the Chief Information Officer (OCIO) appreciates the Office of Inspector General's (OIG) review of NASA's processes for continuously monitoring critical information technology (IT) security controls. These security controls help protect NASA's information and information systems. Below are the responses from the OCIO, provided in the order of the recommendations and findings made by the OIG.

At the OIG's request, the OCIO has evaluated the report to identify any information that it believes should not be publicly released. The OCIO has determined that this report does not contain any specific sensitive but unclassified information.

Recommendation 1. In order to strengthen the Agency's IT security program, we reiterate our 2006 recommendation that NASA establish inventories of the computers connected to its networks. Moreover, we urge NASA to expedite implementation of this recommendation. In addition, we recommend that the NASA CIO require Centers to monitor computer server operating system configuration for compliance with CIS benchmarks and related OCIO-mandated performance targets.

NASA Management Response: Concur. Since 2006, NASA has developed the IT Security Enterprise Data Warehouse (ITSEC-EDW) as its inventory of computers connected to NASA networks. The ITSEC-EDW became operational on July 1, 2010. Information from network vulnerability scans, NASA's patch management and reporting system, and other data sources is collected and correlated in the ITSEC-EDW to make this tool the most comprehensive inventory of NASA computers. In addition, NASA is developing security configuration baselines for computer server operating systems, which will incorporate best practices from CIS benchmarks and other related guidance. NASA is also implementing tools that can monitor computer servers for compliance with these baseline configurations. The OCIO will require that compliance be monitored at the Agency-level, rather than Center by Center, to ensure consistency and enable reporting across all NASA information systems.

Management Corrective Action Dates: The ITSEC-EDW was established as NASA's inventory of computers connected to its networks and became operational on July 1, 2010. A NASA security configuration baseline for Microsoft Windows Server 2003 will be developed by January 1, 2011. OCIO will issue guidance to require monitoring of compliance with this security configuration by August 1, 2011.

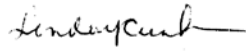
Recommendation 2. To reduce the risk of undetected and uncorrected vulnerabilities, the NASA CIO should require that Centers implement a process to validate that 100 percent of applicable network devices, including computers, routers, and firewalls, undergo regular monitoring for technical vulnerabilities.

NASA Management Response: Partially Concur. NASA Information Technology Requirements (NITR) 2810-24, dated January 28, 2010, requires that "All NASA IT devices and all devices on NASA networks, shall be subjected to routine (at least monthly) network based vulnerability scans ..." Further, this policy requires that Center IT Security Managers (ITSMs) "oversee the vulnerability scanning, reporting, and mitigation activities at their Center to ensure that the requirements are met." While the OCIO strongly agrees that all applicable devices should undergo regular monitoring for technical vulnerabilities, ensuring and validating that 100 percent of devices are in fact monitored is impossible. This is due to constant fluctuations of devices connected to the networks, devices being turned off occasionally, the infeasibility of scanning all networks constantly, and mission requirements that prevent scanning during certain time periods.

Management Corrective Action Dates: NITR-2810-24 was issued on January 28, 2010 and addresses this recommendation to the greatest extent possible. NASA therefore requests that this recommendation be closed as of the issuance of NITR-2810-24.

In its draft report, the OIG reported on a third finding but made no related recommendation. The OIG stated that NASA's process for monitoring Agency IT systems for software patches was not effective. In its report, the OIG cited an initial lack of NASA policy, requiring system owners to implement NASA's software patch monitoring and reporting solution, as the reason that NASA did not have assurance that all applicable Agency computers were monitored to ensure that required software patches had been applied. The OIG further reported that the OCIO issued such a policy in January 2010. Given that the OIG's expressed concerns were addressed by the issued policy and no further evidence was cited to support the OIG's finding, the OCIO respectfully requests that the OIG's final report be revised to remove the finding that "NASA's process for monitoring Agency IT systems for software patches was not effective."

We appreciate the courtesies extended to the OCIO by the OIG in providing the opportunity to comment on the subject draft audit. Please direct any questions to Mr. Jerry L. Davis at (202) 358-1401 or Mr. Dana M. Mellerio at (202) 358-0271.



Linda Y. Cureton

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Chief Information Officer
Ames Research Center Chief Information Officer
Information Technology Security Manager
Dryden Flight Research Center Chief Information Officer
Information Technology Security Manager
Glenn Research Center Chief Information Officer
Information Technology Security Manager
Goddard Space Flight Center Chief Information Officer
Information Technology Security Manager
Jet Propulsion Laboratory Chief Information Officer
Information Technology Security Manager
Johnson Space Center Chief Information Officer,
Information Technology Security Manager
Director of Information Technology and Communication Services, Kennedy Space
Center
Information Technology Security Manager
Langley Research Center Chief Information Officer
Information Technology Security Manager
Director, Office of the Chief Information Officer, Marshall Space Flight Center
Information Technology Security Manager
Chief Information Officer, NASA Shared Services Center
Information Technology Security Manager, NASA Shared Services Center
Stennis Space Center Chief Information Officer
Information Technology Security Manager

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, NASA Financial Management, Office of Financial Management and
Assurance
Director, NASA Issues, 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 Management, Organization, and Procurement

House Committee on Science and Technology

 Subcommittee on Investigations and Oversight

 Subcommittee on Space and Aeronautics

Major Contributors to the Report:

Wen Song, Director, Information Technology Directorate

Jefferson Gilkeson, Project Manager

Richard Curtis, Audit Team Lead

Howard Kwok, Senior Auditor

Eric Jeanmaire, Auditor



OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit <http://oig.nasa.gov/audits/reports/FY10/> 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.