

SEPTEMBER 16, 2010

AUDIT REPORT

OFFICE OF AUDITS

REVIEW OF NASA'S MANAGEMENT AND OVERSIGHT
OF ITS INFORMATION TECHNOLOGY
SECURITY PROGRAM

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

FISMA	Federal Information Security Management Act
IT	Information Technology
IV&V	Independent Verification and Validation
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RMS	Risk Management System
SP	Special Publication

OVERVIEW

REVIEW OF NASA'S MANAGEMENT AND OVERSIGHT OF ITS INFORMATION TECHNOLOGY SECURITY PROGRAM

The Issue

As part of our annual audit of NASA's compliance with the Federal Information Security Management Act (FISMA) for fiscal year (FY) 2009, the Office of Inspector General (OIG) reviewed a representative sample of 29 moderate- and high-impact¹ Agency and external (contractor) information technology (IT) systems from the NASA Centers, Headquarters, and the NASA Shared Services Center. Following the issuance of our FISMA summary report,² we issued a series of reports containing detailed findings and recommendations related to specific deficiencies identified in our audit.³ This report, the third in the series, focuses on whether NASA's IT security program met annual IT security controls and contingency plan testing requirements, ensured that external IT systems were certified and accredited, and implemented an effective Agency-wide process for managing IT corrective actions to mitigate known IT security weaknesses. Details of the audit's scope and methodology are in Appendix A.

Results

We found that NASA's IT security program had not fully implemented key FISMA requirements needed to adequately secure Agency information systems and data. For example, we found that only 24 percent (7 of 29) of the systems we reviewed met FISMA requirements for annual security controls testing and only 52 percent (15 of 29) met FISMA requirements for annual contingency plan testing. In addition, only 40 percent

¹ NPR 2810.1A, "Security of Information Technology," Chapter 7, defines moderate impact as "loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on NASA operations, organizational assets, or individuals." High impact is defined as "loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on NASA operations, organizational assets, or individuals."

² NASA OIG. "Federal Information Security Management Act: Fiscal Year 2009 Report from the Office of Inspector General" (IG-10-001, November 10, 2009).

³ NASA OIG. "Review of the Information Technology Security of the Internet Protocol Operational Network (IONet)" (IG-10-013, May 13, 2010); and NASA OIG. "Audit of NASA's Efforts to Continuously Monitor Critical Information Technology Security Controls" (IG-10-019, September 14, 2010).

(2 of 5) of the external systems we reviewed were certified and accredited. These deficiencies occurred because NASA did not have an independent verification and validation function for its IT security program.

We also found that NASA's Office of Chief Information Officer (OCIO) had not effectively managed corrective action plans used to prioritize the mitigation of IT security weaknesses. This occurred because OCIO did not have a formal policy for managing the plans and did not follow recognized best practices when it purchased an information system that it hoped would facilitate Agency-wide management of IT corrective action plans. However, after spending more than \$3 million on the system since October 2005, implementation of the software failed. The Agency is currently expending funds to acquire a replacement system.

Specifically, we found that the information system was significantly underutilized and therefore was not an effective tool for managing corrective action plans across NASA. For example, the system contained corrective actions plans for only 2 percent (7 of 289) of the 29 systems we sampled. In our judgment, the system was underutilized because OCIO did not fully document detailed system requirements prior to selecting the system and did not have users validate requirements via acceptance testing prior to implementing it. Because the information system contained minimal data and the manual process the Agency relied on was not consistently followed, OCIO's management of corrective actions plans was ineffective and did not ensure that significant IT security weaknesses were corrected in a timely manner.

Until NASA takes steps to fully meet FISMA requirements and to improve its system acquisition practices, NASA's IT security program will not be fully effective in protecting critical Agency information systems. Moreover, until such improvements are made OCIO will not be in a position to effectively allocate resources to correct IT security weaknesses.

Management Action

To strengthen NASA's IT security program and to ensure that OCIO can effectively manage and correct IT security weaknesses, we recommended that the NASA Chief Information Officer:

1. establish an independent verification and validation function to ensure that all FISMA and Agency IT security requirements are met;
2. develop a written policy for managing IT security corrective action plans; and
3. adopt industry system acquisition best practices, including documenting detailed requirements prior to system selection and conducting user acceptance testing before system implementation.

In response to our August 17, 2010, draft of this report, the Chief Information Officer concurred with our recommendations and stated that NASA will:

1. update policy to require independent assessments of IT system security controls to strengthen the verification and validation function by September 30, 2011;
2. develop a policy for managing IT security corrective action plans by May 16, 2011; and
3. develop a policy requiring detailed system requirements be documented prior to system selection by May 16, 2011, and better enforce existing policy requiring user acceptance testing prior to system implementation.

Management's comments are provided in Appendix B.

In general, we consider the Chief Information Officer's proposed actions to be responsive to our recommendations. However, we were concerned that her response to Recommendation 1 appears to shift responsibility for verification and validation of the Agency's IT security practices from her office to third parties such as NASA OIG and the Government Accountability Office. While these entities perform an important oversight role, the primary responsibility for establishing effective verification and validation practices for the Agency's IT security program must reside with OCIO. Nevertheless, we will consider the recommendations resolved and will close each upon verification that management has completed the corrective actions.

CONTENTS

INTRODUCTION

Background _____	1
Objectives _____	3

RESULTS

NASA Did Not Fully Satisfy FISMA Requirements _____	4
Agency-wide Management of IT Corrective Actions Plans Needs Improvement _____	8

APPENDIX A

Scope and Methodology _____	11
Review of Internal Controls _____	12
Prior Coverage _____	13

APPENDIX B

Management Comments _____	14
---------------------------	----

APPENDIX C

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

INTRODUCTION

Background

The Federal Information Security Management Act (FISMA) sets forth specific information security requirements Federal agencies must adhere to, including requirements relating to system security controls assessments, system contingency plans tests, and system certification and accreditation.

FISMA also assigns specific IT responsibilities to senior agency officials and agency inspectors general. For example, NASA's Chief Information Officer is responsible for developing and overseeing Agency-wide, risk-based, cost-effective policies and procedures for addressing information security. NASA's Deputy Chief Information Officer for Information Technology (IT) Security is responsible for implementing an Agency-wide security program that is consistent with FISMA and Agency policies and procedures. NASA's Office of Inspector General (OIG) is responsible for performing an annual independent evaluation of the information security practices of the Agency in accordance with reporting instructions issued by the Office of Management and Budget (OMB).

Our independent evaluation for fiscal year (FY) 2009 focused on the following 10 review areas required by OMB:

- System Inventory
- Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing
- Agency Oversight of Contractor Systems and Quality of Agency System Inventory
- Agency Plan of Action and Milestones (POA&M) Process
- The Certification and Accreditation Process
- Agency Privacy Program and Privacy Impact Assessment (PIA) Process
- Configuration Management
- Incident Reporting
- Security Awareness Training
- Peer-to-Peer File Sharing

In our FY 2009 FISMA report,⁴ we identified deficiencies in NASA's IT security program related to security controls testing, contingency plan testing, and certification and accreditation of contractor-owned (external) systems. We also found deficiencies in the Agency's process for managing corrective actions intended to remedy known IT security deficiencies.

Security controls are the management, operational, and technical safeguards that help ensure the confidentiality, integrity, and availability of an IT system and its data. If NASA's security controls do not function as intended, the Agency could experience a system breach resulting in the loss of sensitive information or an adverse effect on Agency operations. For example, in January 2009 a system breach caused by an improperly implemented security control resulted in the theft of a large quantity (22 gigabytes) of sensitive data related to Space Exploration programs. Security controls testing evaluates the effectiveness of an agency's controls by determining whether they are implemented correctly, operating as intended, and producing the desired result of protecting the system and its data.

Computer systems are vulnerable to a variety of disruptions such as power outages, hardware failures, or equipment destruction resulting from fire or other catastrophic events. System contingency plans define the resources needed and processes to be followed in order to effectively and efficiently recover a system following a disruption.⁵ If a system disruption occurs and the contingency plan is not effective, NASA could be unable to perform critical business operations. Contingency plan testing helps mitigate the risk to NASA operations by providing assurance that systems will be recoverable and normal operations can be restored following a disruption.

System certification and accreditation (C&A) is a formal risk evaluation and acceptance process that FISMA requires be performed before a system is authorized to store and process agency data.⁶ Because external (contractor) systems store and process NASA data, they are required to comply with the C&A process. NASA's responsibility in the external system C&A process is to ensure that system owners (contractors) have certified

⁴ NASA OIG. "Federal Information Security Management Act: Fiscal Year 2009 Report from the Office of Inspector General" (IG-10-001, November 10, 2009).

⁵ Contingency Plan: Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. Contingency plans assist managers to ensure that data owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted. (NPR 2810.1A, Glossary [page 119 of 149])

⁶ Certification: The comprehensive assessment of the technical and non-technical security features and other safeguards of an IT [information technology] system and establishes the extent to which a particular design and implementation meets documented security requirements. (NPR 2810.1A, Section 14.2). Accreditation: The formal declaration by a senior Agency official that an IT system is compliant with established security requirements and is approved to operate using a prescribed set of safeguards. This decision should be based on the residual risks identified during the risk mitigation process. By accrediting an information system, the authorizing official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. (NPR 2810.1A, Section 14.4)

and accredited systems. External systems that have not been properly certified and accredited could expose NASA data and the related programs to an unacceptable level of risk.

When IT security deficiencies are identified, Agency employees create corrective action plans documenting the planned remediation process. These plans assist NASA in identifying, assessing, prioritizing, and monitoring the progress of efforts to correct IT security weaknesses found in Agency systems and programs. The plans are also used to close security performance gaps, assist OIG staff in their evaluations of Agency security performance, and assist OMB with oversight responsibilities.

Objectives

We evaluated whether the Agency's IT security and privacy management programs met performance standards set forth in OMB's FY 2009 FISMA and Privacy Act reporting instructions.⁷ We found deficiencies in NASA's IT security program in the following three areas:

- annual assessment of system security controls and testing of contingency plans;
- certification and accreditation of external IT systems; and
- management of corrective actions plans for IT security weaknesses.

We also reviewed internal controls as appropriate. Details of the audit's scope and methodology are in Appendix A.

⁷ OMB. "FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" (M-09-29, August 20, 2009).

NASA DID NOT FULLY SATISFY FISMA REQUIREMENTS

NASA did not fully satisfy FISMA requirements related to security control assessments, contingency plan testing and certification, and accreditation of external systems. Specifically, we reviewed 29 moderate- and high-impact Agency and external systems from all NASA Centers, Headquarters, and the NASA Shared Services Center and found that only

- 24 percent (7 of 29) of NASA’s systems met annual security controls assessment requirements,
- 52 percent (15 of 29) of NASA’s systems met annual contingency plan testing requirements, and
- 40 percent (2 of 5) of external contractor systems were certified and accredited.

NASA did not identify these deficiencies because the OCIO had not implemented an independent verification and validation function to ensure the effectiveness of the Agency’s IT security program. As a result, NASA could not ensure that: (1) its security controls adequately safeguard Agency systems and data; (2) systems could be effectively recovered and normal operations restored following a disruption; and (3) risks had been adequately mitigated in external systems that store and process Agency data.

NASA’s IT Security Program Did Not Meet Key FISMA Performance Standards

We reviewed 29 moderate- and high- impact systems (24 internal and 5 external) for compliance with OMB and National Institute of Standards and Technology (NIST) requirements for the following performance measures:

- a current C&A package;
- security controls that had been assessed within the past year; and
- a contingency plan that had been tested within the past year.

Security Control Assessments Lacked Sufficient Supporting Evidence and Were Not Tailored to System Impact Level. NIST guidance provides detailed instructions for conducting effective security control assessments.⁸ These instructions state that control

⁸ National Institute for Standards and Technology. “Guide for Assessing the Security Controls in Federal Information Systems” (Special Publication 800-53A, December 2007).

assessments involve: (1) examining documents and observing activities; (2) interviewing personnel; and (3) testing controls and recording the results. Examining documents and conducting interviews helps security control assessors understand the information system. While testing controls measures the effectiveness of security controls. For example, if a control fails during testing the Agency has identified a security weakness (i.e., an ineffective control) and is on notice that changes to the design or implementation of the control is required. NIST guidance also requires that security control assessments be tailored to the system's impact level. Specifically, moderate- and high-impact systems require more controls testing than low-impact systems.

We found that only 24 percent (7 of 29) of the system security control assessments we reviewed contained information sufficient for us to conclude that security controls in these moderate- and high-impact systems had been assessed within the past year in accordance with FISMA. The security control assessments we reviewed typically consisted of lists of security controls and a statement indicating that the control had been "tested" or "implemented." However, other required information, such as the method used to perform the control assessment and the results of the tests, was often not provided. Without such information, the system owner and authorizing official cannot make informed decisions about whether security risks have been sufficiently mitigated. Moderate- and high-impact systems operating with ineffective security controls are susceptible to compromise, which could have serious effects on Agency operations, assets, or personnel.

We also found that seven of the security control assessments we reviewed had not been tailored to the system's impact level. For example, the assessment report for one high-impact system showed that only 3 of the selected 55 security controls had been assessed through actual control testing as opposed to reviewing documents or conducting interviews. However, NIST guidelines require extensive controls testing for high-impact systems. In our judgment, NASA's testing 3 of 55 controls did not comport with this guidance and was not adequate to determine whether risks to the system had been adequately mitigated.

Contingency Plan Tests Did Not Include Required Test Elements. We found that only 52 percent (15 of 29) of the system contingency plan tests we reviewed contained documentation sufficient for us to conclude that contingency plans for these moderate- and high-impact systems had been tested within the past year in accordance with FISMA. As discussed above, contingency plan testing is essential for identifying deficiencies and evaluating whether systems can be recovered to allow for normal operations following a disruption.

NIST guidance provides that annual contingency plan tests include: (1) system recovery on an alternate platform from backup media; (2) coordination among recovery teams;

(3) internal and external connectivity; (4) system performance using alternate equipment; (5) restoration of normal operations; and (6) notification procedures.⁹

For the systems that lacked sufficient documentation of contingency plan testing, we found that the documentation either did not show evidence that any of the six NIST-required elements were tested or, in the case of high-impact systems, did not demonstrate that systems could be recovered and normal operations restored. Operating moderate- and high-risk systems without effective contingency plans increases the risk that the systems will not be recoverable and that normal operations might not be restored following a disruption. Such an outcome could have a serious adverse effect on Agency assets, operations, and personnel.

External Systems Were Not Certified and Accredited. Although all 24 Agency systems we reviewed were certified and accredited, we found that only 40 percent (2 of 5) of the external (contractor) IT systems we reviewed met C&A requirements. The other three systems were operating without evidence that two key requirements of the C&A process – the annual security controls assessment and contingency plan test – had been met. Because the security categorization of each external system reviewed was either moderate or high, a system breach could have a serious adverse effect on the Agency operations these systems support.

The C&A process is an important risk management practice and an integral part of an agency's information security program. By certifying and accrediting an IT system, management accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the Agency if a breach of security occurs. FISMA requires that external systems be certified and accredited before they are placed into operation and allowed to store and process a Federal agency's data. In addition, NASA's standard operating procedure related to IT Security¹⁰ states that external systems must follow a C&A process that meets all FISMA standards. Although ensuring C&A is done is the responsibility of the external system owner, NASA is responsible for ensuring that external system owners conduct the C&A in accordance with FISMA. However, we found little evidence to show that NASA had performed required contractor oversight or that contractor management had formally authorized the systems for operation. External systems operating without meeting C&A requirements could expose NASA data and related programs to an unacceptable level of risk, the results of which could be the loss of critical data or NASA being unable to perform mission-critical operations.

OCIO Needs an Independent Verification and Validation Function for the Agency's IT Security Program. The deficiencies we identified in the Agency's IT security program resulted from a lack of effective oversight by the OCIO. Because the OCIO had not implemented an independent verification and validation (IV&V) function for the

⁹ NIST. "Contingency Planning Guide for Information Technology Systems" (Special Publication 800-34, June 2002).

¹⁰ NASA. Standard Operating Procedure "External System Identification and IT Security Requirements" (ITS-SOP-0033, July 19, 2007).

Agency's IT security program, it was unaware of the deficiencies we identified and therefore could not ensure that NASA systems and data were adequately secured.

IV&V is a structured, two-step quality control and quality assurance process widely used for improving products and processes in the information technology domain. Verification, the first step, determines whether a product or process meets regulations. Validation, the second step, establishes evidence to provide a high degree of assurance that a product or process meets its intended requirement. In our judgment, establishing an IV&V function could strengthen the Agency's security program by improving internal processes, which could help ensure that Federal and Agency IT security requirements are met. We believe that without this oversight function NASA cannot ensure that: (1) IT security controls adequately safeguard Agency systems and data; (2) systems can be effectively recovered and normal operations restored following a disruption; and (3) risks have been adequately mitigated in external systems that store and process Agency data.

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

Recommendation 1. To strengthen NASA's IT security program, we recommended that the NASA Chief Information Officer establish an independent verification and validation function to ensure that all FISMA and Agency IT security performance elements are met and information systems are adequately secured.

Management's Response. The CIO concurred with our recommendation and stated that the OCIO will update the Agency approach to IT system security risk management by refining the requirements and capabilities needed for performing independent assessment of IT security controls. NASA will revise its approach to IT system security risk management, including the performance of independent control assessments, by September 30, 2011.

Evaluation of Management's Response. We consider the CIO's proposed actions to be responsive to our recommendation. However, her response appears to shift responsibility for verification and validation of the Agency's IT security practices from the OCIO to third parties such as NASA OIG and the Government Accountability Office. While these entities perform an important oversight role, the primary responsibility for establishing effective verification and validation practices for the Agency's IT security program must reside with the OCIO. Nevertheless, we consider the recommendation resolved and will close it upon verification that the proposed actions have been completed.

AGENCY-WIDE MANAGEMENT OF IT CORRECTIVE ACTION PLANS NEEDS IMPROVEMENT

Corrective action plans are used to prioritize the mitigation of IT security weaknesses. We found that OCIO had not effectively managed corrective action plans for NASA IT systems because it does not have a formal policy for managing the plans and failed to follow recognized best practices when it acquired an information system that was to enable Agency-wide management of these plans. Although OCIO has spent more than \$3 million since 2005 to implement an Agency-wide information system for managing IT security-related information, OCIO continued to administer corrective action plans manually using an unwritten policy that was not consistently followed.

In addition, we found that this information system contained only 2 percent of the corrective action plans related to our sample of 29 systems, indicating substantial underutilization of the system. In our judgment, this underutilization occurred because OCIO did not follow widely recognized best practices when it acquired the system. Specifically, OCIO did not fully document detailed system requirements to support system selection and did not have users validate requirements via acceptance testing. Because the information system contained minimal data and the manual process was not consistently followed OCIO's management of corrective actions plans was ineffective and did not ensure that significant IT security weaknesses were corrected in a timely manner.

Until NASA implements a formal, written policy for managing corrective action plans and follows recognized best practices for acquiring the related IT system, OCIO will not have key IT security information needed to effectively manage NASA's IT security program.

Lack of a Formal Policy Prevented OCIO from Effectively Managing IT Security Corrective Action Plans

Federal criteria and Agency policy require NASA to have processes in place to develop corrective action plans for all known IT security weaknesses and to report progress on remediation efforts known as the Plan of Action and Milestones (POA&M) process. During this review, we identified several deficiencies with NASA's POA&M process. First, the process did not include all known IT security weaknesses. For example, only 2 percent (7 of 289) of corrective actions related to our sample of 29 systems were recorded in the Agency's official repository for IT security-related information. Second, the Agency managed corrective actions using an informal, unwritten policy that was not consistently followed. Based on these deficiencies, OCIO did not have sufficient

information to make informed decisions about prioritizing efforts to correct known IT security weaknesses. As a result, critical Agency IT assets may not be fully or effectively protected.

Deficient Software Acquisition Practices Prevented OCIO from Implementing an Agency-wide IT Security Management System

In October 2005, OCIO selected the Risk Management System (RMS), a commercial, off-the-shelf software system as the Agency-wide solution for managing IT security related information. In 2007, OCIO required that all IT security-related information, including POA&Ms, be recorded in RMS by July 31, 2008. However, almost two years later RMS remains significantly underutilized and OCIO continues to manage POA&Ms using an inadequate manual process. Specifically, each month Center IT personnel provide Headquarters OCIO staff with an Excel spreadsheet of the Center's POA&M data. Headquarters staff manually aggregate this data to create an Agency-wide report. OCIO is not able to use RMS to create an Agency-wide report because users have not input the underlying data into the system. In our judgment, this occurred because OCIO implemented RMS without following recognized software acquisition best practices. Specifically, OCIO selected RMS without adequately developing system requirements and implemented RMS without adequately evaluating whether the product met the business needs of its intended users.

The "Software Acquisition Capability Model," March 2002, developed by the Software Engineering Institute of Carnegie Mellon University, is a recognized authoritative source of best practices for the software acquisition process. The Model notes that the development of a detailed set of requirements as part of the solicitation package significantly contributes to the success of system acquisition efforts. The Model further states that as the system acquisition effort develops, requirements are identified and refined, and by the time the solicitation package is fully developed, it should contain a significant set of technical and non-technical requirements. However, OCIO prepared the solicitation and selected RMS without fully developing detailed system requirements.

The Software Acquisition Capability Model also recommends use of a structured process to evaluate whether a potential system satisfies end-user needs. User acceptance testing is a system evaluation process whereby the users determine if the system satisfies identified requirements before the system is formally accepted or implemented. However, OCIO did not follow this best practice and implemented RMS without having its users validate that the product met business requirements. As a result, OCIO spent more than \$3 million since October 2005 on a software implementation that failed.

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

Recommendations. To improve Agency-wide management of IT security corrective action plans and to ensure that funds for the related IT system acquisition efforts are effectively spent, we recommended that the NASA Chief Information Officer:

2. develop a written policy for managing corrective action plans to mitigate IT security weaknesses; and
3. adopt industry system acquisition best practices, including documenting detailed requirements prior to system selection and conducting user acceptance testing, before implementing a new system.

Management's Response. The CIO concurred with our recommendations and will perform the following corrective actions by May 16, 2011:

1. include written policy statements, addressing the management of corrective action plans, in NPR 2810.1B; and
2. require that detailed requirements are documented prior to selection and acquisition of IT systems as part of NPR 2810.1B. Further, OCIO states that they will follow the NPR 7210.7 policy in its system acquisition efforts, which includes the use of industry best practices including end user testing.

Evaluation of Management's Response. We consider the CIO's proposed actions to be responsive to our recommendation. Therefore, the recommendation is resolved and will be closed upon verification that the proposed actions have been completed.

Scope and Methodology

We performed our audit from January through October 2009 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 during this audit provides a reasonable basis for our findings and conclusions based on our objectives.

For this report, we evaluated whether NASA complied with FISMA and Agency privacy management requirements. We followed OMB Memorandum M-08-21, "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," July 14, 2008, until OMB released the FY 2009 reporting instructions, OMB Memorandum M-09-29, "FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," August 20, 2009.

We did not evaluate whether NASA's national security systems met FISMA and Agency privacy management requirements because a separate OIG audit addressed that issue : "Audit of the Reporting of NASA's National Security Systems" (IG-09-024, August 28, 2009).

The systems we reviewed were selected from an Agency-wide, non-national security system inventory list maintained by the Office of the Chief Information Officer (OCIO). As of November 2008, the inventory list, identified 598 internal systems and 30 external (contractor) systems. Before selecting our sample, we removed from the inventory those systems that were either reviewed in the FY 2008 FISMA audit or are low impact based on the system's security classification.

The result was a population of 338 high- and moderate-impact internal systems and a population of 13 moderate- and high- and moderate- impact external systems. Using the EZ-Quant Statistical Sampling Module to generate random numbers, we selected a representative sample of systems from each population.

For our sample of internal systems, we selected two internal systems from each of NASA's 10 Centers, NASA Headquarters, and NSSC, and one external system from each of the 7 NASA entities listed as having an external system. During fieldwork, we discovered that two of the external systems selected were not in use: one was under development and the other had been disposed of. We removed those two systems from our sample.

In total, we reviewed 29 high- or moderate-impact systems (24 internal and 5 external) for compliance with OMB and National Institute of Standards and Technology (NIST) requirements for the following performance measures:

- a current security certification and accreditation package;
- security controls that had been tested within the past year; and
- a contingency plan that had been tested within the past year.

To determine compliance, we reviewed key documents, including system security plans, risk assessments, security assessment results, plans of action and milestones, accreditation decision letters, tests of security controls, contingency plans, and contingency plan tests. We did not evaluate the technical adequacy of these documents other than to determine whether they generally met OMB and NIST guidelines. We reviewed the following Federal and Agency criteria, policies, and procedures:

- “E-Government Act of 2002,” December 17, 2002;
- OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources,” February 8, 1996;
- NIST Special Publication 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems,” July 2008;
- NIST Special Publication 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems,” May 2004;
- NIST Special Publication 800-34, “Contingency Planning Guide for Information Technology Systems,” June 2002; and
- NASA Procedural Requirements (NPR) 2810.1A, “Security of Information Technology,” May 16, 2006.

Computer-Processed Data

We relied on data from the Risk Management System -- the Agency’s central repository for plans of actions and milestones associated with Agency information systems. We did not validate the reliability of the data in the Risk Management System.

Review of Internal Controls

We reviewed and evaluated internal controls associated with the C&A process. Specifically, we examined Agency oversight of contractors who manage external systems, the POA&M process, security controls testing, and contingency plan testing. We found that oversight for external systems could be improved. In addition, we

identified internal control weaknesses related to the POA&M process, security controls testing, and contingency plan testing.

Prior Coverage

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

Government Accountability Office

“NASA Needs to Remedy Vulnerabilities in Key Networks” (GAO-10-04, October 15, 2009)

National Aeronautics and Space Administration

“Federal Information Security Management Act: Fiscal Year 2008 Report from the Office of Inspector General” (IG-10-001, November 10, 2009)

“Audit of the Reporting of NASA’s National Security Systems” (IG-09-024, August 28, 2009)

MANAGEMENT COMMENTS

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



SEP - 9 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, "Review of NASA's Management and Oversight of Its Information Technology Security Program" (Assignment No. A-09-004-03)

The Office of the Chief Information Officer (OCIO) appreciates the Office of Inspector General's (OIG) review of information technology (IT) security controls and contingency plan testing requirements to ensure that external IT systems were certified and accredited and implemented and whether NASA implemented an effective Agency-wide process for managing IT corrective actions to mitigate known IT security weaknesses. Below are the OCIO responses to the recommendations made by the OIG:

Recommendation 1. To strengthen NASA's IT security program, we recommend the NASA Chief Information Officer establish an independent verification and validation function to ensure that all FISMA and Agency IT security performance elements are met and information systems are adequately secured.

NASA Management Response: Concur. NASA agrees that an independent verification and validation function is important in ensuring that FISMA and Agency IT security requirements are met. Several OCIO activities contribute to performing this function including internal and external penetration testing, continuous monitoring and reporting of selected security controls using Agency-managed automated tools, and oversight of Center and Program IT security activities by IT Security Managers (ITSM) and security control assessors (formerly CAOs). In addition, the OCIO relies on the OIG and the Government Accountability Office (GAO) reviews to round out the independent verification and validation of NASA IT security activities. As part of updating the Agency approach to IT system security risk management, the OCIO is refining the requirements and capabilities needed for performing independent assessments of IT system security controls. This approach will further strengthen the independent verification and validation function.

Management Corrective Action Dates: NASA's approach to IT system security risk management, including performance of independent assessments, will be updated by September 30, 2011.

Recommendation 2. To improve Agency-wide management of IT security corrective action plans and to ensure that funds for the related IT system acquisition efforts are effectively spent, we recommend the NASA Chief Information Officer develop a written policy for managing corrective action plans to mitigate IT security weaknesses.

NASA Management Response: Concur. NASA agrees that a written policy for managing corrective action plans to mitigate IT security weaknesses can improve the Agency-wide management of IT security corrective action plans. Policy statements addressing this area will be included in NPR 2810.1B, which is currently being drafted.

Management Corrective Action Dates: NPR 2810.1B will be finalized by May 16, 2011.

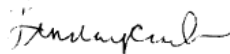
Recommendation 3. To improve Agency-wide management of IT security corrective action plans and to ensure that funds for the related IT system acquisition efforts are effectively spent, we recommend that NASA Chief Information Officer adopt industry system acquisition best practices, including documenting detailed requirements prior to system selection and conducting user acceptance testing, before implementing a new system.

NASA Management Response: Concur. The NASA OCIO follows NPR 7120.7 in its IT system acquisition efforts. This policy includes industry system acquisition best practices such as development, vetting and documentation of detailed requirements, and user acceptance testing. In addition, NPR 2810.1B, which is currently being drafted, will require that detailed requirements be documented prior to selection and acquisition of IT systems.

Management Corrective Action Dates: NPR 2810.1B will be finalized by May 16, 2011.

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.

We appreciate the courtesies extended to the OCIO by the OIG in providing the opportunity to submit a revised response to the subject audit. Please direct any questions to Ms. Marion Meissner at (202) 358-0585 or Mr. Dana M. Mellerio at (202) 358-0271.



Linda Y. Cureton

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief Information Officer
Associate Administrator, Space Operations Mission Directorate
Director, Goddard Space Flight Center
Director, Marshall Space Flight Center

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.