AUGUST 5, 2010

REDACTED FOR PUBLIC RELEASE

OFFICE OF AUDITS

AUDIT OF CYBERSECURITY OVERSIGHT OF [A NASA] SYSTEM

OFFICE OF INSPECTOR GENERAL

National Aeronautics and
Space Administration

REPORT NO. IG-10-018-REDACTED

REDACTED FOR PUBLIC RELEASE

THE FULL VERSION OF THIS REPORT INCLUDED INFORMATION THAT NASA CONSIDERED TO BE SENSITIVE INFORMATION WHICH, IF DISTRIBUTED WIDELY, COULD POSE A SECURITY THREAT TO NASA COMPUTER SYSTEMS. WHERE SUCH INFORMATION HAS BEEN REDACTED IS NOTED IN THE REPORT.

Final report released by:

Paul K. Martin
Inspector General

Acronyms – Redacted

CIO	Chief Information Officer
FIPS	Federal Information Processing Standards
IT	Information Technology
ITS	Information Technology Security
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
SOP	Standard Operating Procedure
SP	Special Publication

OVERVIEW

AUDIT OF CYBERSECURITY OVERSIGHT OF [A NASA] SYSTEM

The Issue

The Center for Strategic and International Studies reported in January 2009 that industrial spies, foreign intelligence agents, Internet criminals, and others have penetrated poorly protected U.S. computer networks and collected immense quantities of valuable information. Because of these and other illegal activities, the President has identified the protection of our digital infrastructure as a national security priority.

[The NASA system that we reviewed for this audit] is a core system used to process, store, and distribute vital Agency intellectual property, such as [. . .], and crucial program and project information. [The reviewed system] is categorized as a "high-impact system" under Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004. As such, a compromise of security controls[1] for a high-impact system could result in severe adverse impact, leading to degradation in or loss of NASA's mission capability, harm to individuals, or life-threatening injuries. In October 20[XX], NASA awarded a 4-year contract to [a contractor] for, among other things, operation of [the reviewed system].

The National Institute of Standards and Technology (NIST) Computer Security Division, under the authority of Title III of the E-Government Act, also known as the Federal Information Security Management Act of 2002, developed security requirements for Federal information and information systems using a standardized, risk-based approach to assist agencies in securing their systems and data.

Our objective in this audit was to determine whether NASA's security controls and practices were implemented to ensure the confidentiality, integrity, and availability of [the reviewed system's] data. Details of the audit's scope and methodology can be found in Appendix A.

[1] Security controls are the management, operational, and technical controls prescribed for information contained in an information system that, when taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and the information.

Results

During the audit, we evaluated security controls for 13 of 17 families[2] listed in NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems," Revision 2, December 2007, that we considered the most critical to mitigate the risk of outside intrusion and internal trespassing of [the reviewed system]. [The reviewed system] contained security controls that met the NIST requirements for an effective information technology (IT) security posture. For example, [the reviewed system] had security controls that included security awareness and training of personnel; contingency planning related to safeguarding data to include file backups and alternative processing sites in case of a disaster; procedures to protect system and information integrity, such as malicious code protection; and comprehensive access controls. However, we found several significant security control weaknesses in [the reviewed system] that could threaten the confidentiality, integrity, and availability of critical information. Those weaknesses include the following:

- **Outdated Security Plan.** NASA has not revised [the reviewed system's] 2008 [. . .] Security Plan to include required NIST SP updates on recommended security controls for Federal information systems. For example, NIST SP 800-53, Revision 2, December 2007, included 6 additional security controls and 37 control enhancements that were not included in prior NIST standards. In addition, the [reviewed system's] Security Plan did not include the appropriate guidance for audit and accountability controls, nor did it reference the most recent guidance on vulnerability scanning. By not keeping security plans current and complete with the appropriate security controls and guidance, NASA officials do not have assurance that essential security control requirements are being addressed appropriately.

- **Limited Vulnerability Scanning Coverage.** [The contractor's] internal IT auditors did not perform credentialed vulnerability scans[3] on [contractor]-managed systems. As a result, as many as 5,130 vulnerability checks of varying impact levels are rendered inoperable, which increases the probability that an attacker could gain access and carry out inappropriate or malicious acts on the Agency's network without being detected.

- **Vulnerability of Local Administrator Accounts.** Three of the five [. . .] servers in our sample (see Appendix A for details about our sample selection) contained built-in administrator accounts that were not renamed as required and their passwords had no expiration. If a built-in administrator account on [a server of

[2] NIST organized security controls into *classes* and *families* for ease of use in the control selection and specification process, as shown in the table on page 4 of this report.

[3] Credentialed vulnerability scans are scans that are performed using administrator-level privileges. Having credentials allows vulnerability checks of all areas of an information system.

the reviewed system] is compromised, a skilled attacker could gain access to any of NASA's systems that are attached to [the reviewed system].

- **Use of Unauthorized Software.** We found software installed on [one of the reviewed system's] server[s] that was not approved for installation, and it contained multiple high-impact vulnerabilities that could allow an intruder to gain undetected access to NASA's network. Having this software installed on [. . .] server[s] potentially compromised NASA's valuable intellectual property.

- **Hardware and Software Inventory Controls Lacking.** Inventories of IT hardware components were not accurate or readily available. We found that active [reviewed system] hardware component listings were not readily available and contained errors and numerous duplicate entries. In addition, as noted earlier, we identified software on [a server of the reviewed system] that was unaccounted for by [contractor] IT security personnel and contained high-impact vulnerabilities. If an organization cannot easily produce an accurate listing of hardware and software components on its system, as well as maintain accurate documentation of those components, the potential for exploitation of vulnerabilities that stem from a lack of security controls is increased.

- **Media Protection Needed.** [The contractor] transferred media tapes to a storage location at [another Federal facility] but did not obtain written confirmation of delivery. Written confirmation of the transfer of the media tapes is essential to ensure continuity of operations; enable the Agency to perform emergency preparedness, response, and recovery; and protect Agency assets.

Without comprehensive implementation of security controls, NASA cannot ensure the confidentiality, integrity, and availability of [the reviewed system's] data. The weaknesses we identified occurred because NASA did not perform adequate contract oversight to ensure that [the contractor] complied with NIST security control requirements. As a result, NASA has limited assurance that all required controls are functioning to protect [the reviewed system's] data. Furthermore, given the deficiencies noted, NASA cannot ensure that [the reviewed system] is not vulnerable to attack or compromise with the potential to severely disrupt NASA's mission capability. In addition to [the reviewed system], [the contractor] manages [numerous] other systems for NASA, and we believe that [the contractor] is using similar security practices for all [those] systems. Therefore, although we did not specifically examine the other [contractor]-managed systems for the deficiencies that we identified for [the reviewed system], our audit findings raise serious concerns about the security of NASA data contained in those other [. . .] systems.

Management Action

To improve security control practices for [the reviewed system] and the other [. . .] systems managed by [the contractor], we recommended that NASA officials take

steps to review security plans annually for completeness and eliminate internal control weaknesses related to vulnerability scans, local administrator accounts, installation of unauthorized software, and hardware and software inventories on [the reviewed system's] servers. In addition, we recommended that a review of the other [. . .] systems managed by [the contractor] be completed to identify and correct similar security control weaknesses that may exist in those systems.

We also recommended that the NASA Chief Information Officer, [the reviewed system's] Information System Owner [and various other NASA officials] coordinate their efforts to provide [the contractor] with guidance to meet [the contract] requirements and Federal, NASA, and [contractor] policies and procedures.

During the course of this audit, [the contractor] improved its security controls for media protection by updating its policy to require written confirmation of delivery of media tapes. Accordingly, we are making no additional recommendations for this issue.

In response to our May 26, 2010, draft of this report, NASA management generally concurred with all six recommendations and stated that it will take steps to mitigate and improve [the reviewed system's] security control practices related to vulnerability scans, local administrator accounts, installation of unauthorized software, and hardware and software inventories on [the reviewed system's] servers. In addition, the Office of the Chief Information Officer said it will review the other [. . .] systems managed by [the contractor] to identify and correct similar security control weaknesses that may exist in those systems.

We consider management's proposed actions to be responsive to our recommendations. However, management's responses did not include a timeline for completion of the proposed actions. Therefore, we request that NASA provide a timeline for completing the actions in response to the final report. We will close the recommendations after verifying that the actions have been taken.

CONTENTS

INTRODUCTION

Background

The Center for Strategic and International Studies, one of the world's preeminent public policy institutions on foreign policy and national security issues, reported in January 2009 that industrial spies, foreign intelligence agents, Internet criminals, and others have penetrated poorly protected U.S. computer networks and collected immense quantities of valuable information. Because of these and other illegal activities, the President has identified the protection of our digital infrastructure as a national security priority.

[The NASA system that we reviewed] is a core system used to process, store, and distribute vital Agency intellectual property, such as [. . .], and crucial program and project information. [The reviewed system] is categorized as a "high-impact system" under Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004. A compromise of security controls for a high-impact system could result in severe adverse impact, leading to degradation in or loss of NASA's mission capability, harm to individuals, or life-threatening injuries.

[Subheading Redacted]. [The reviewed system] is a major NASA information system that requires heightened security oversight because of the risk and magnitude of harm that could result from the loss, misuse, unauthorized access to, or modification of the information in the system. Examples of data stored, processed, analyzed, and reported within [the reviewed system] include

- essential [. . .] engineering data,
- NASA program and project life-cycle information,
- [flight project] information,
- [sensitive legal information], and
- NASA lessons learned, historical data, and other relevant information.

[The reviewed system] is a commercial off-the-shelf 3-tier client/server architecture[4] supported by various servers within the information technology (IT) infrastructure of [the contractor]. NASA uses [the reviewed system] to process, store, and distribute important NASA intellectual property, such as [. . .], to NASA's information system users.

[4] A 3-tier architecture contains an intermediary level, meaning the architecture is generally split among (1) a client that requests the resources equipped with a user interface (usually a Web browser) for presentation purposes; (2) the application server, which provides requested resources contained on another server; and (3) the data server, which provides the application server with the data requested.

[The reviewed system] provides a hardware and software infrastructure that enables the integration of multiple operational databases into a single database view designed specifically for reporting and analytical processing. [The reviewed system] consists of 19 applications and [numerous] servers located in [. . .]. [The contractor's] contractual requirements and responsibilities are identified in the [applicable contract].

The contract requires [the contractor] to follow the requirements in NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology," May 16, 2006, which applies to all NASA contracts. NPR 2810.1A states that NASA IT security policies, requirements, and procedures must be established to implement National Institute of Standards and Technology (NIST) standards on IT security to support NASA's missions. The [reviewed system's] Security Plan also references [the contractor's] policies and procedures. The NIST Computer Security Division, under the authority of Title III of the E-Government Act, also known as the Federal Information Security Management Act of 2002, developed security requirements for Federal information and information systems using a standardized, risk-based approach to assist agencies in securing their systems and data.

[Paragraph Redacted]

Guidance. [The reviewed system's] content is subject to the policies outlined in the Arms Export Control Act, as implemented by the International Traffic in Arms Regulations. [Therefore], the International Traffic in Arms Regulations apply to the contents of this system. Therefore, security controls must ensure that information contained in [the reviewed system] is not compromised.

NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems," Revision 2, December 2007, provides a catalog of controls based on a system's impact levels – categorized as low, moderate, and high – to ensure the confidentiality, integrity, and availability of the system. NIST SP 800-53, Revision 2, also provides guidelines for selecting and specifying security control baselines for information systems supporting the executive agencies of the Federal Government. The guidelines apply to all components of an information system that process, store, or transmit Federal information and seek to

- facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security control baselines for information systems and organizations;

- provide a recommendation for minimum security controls for information systems categorized in accordance with FIPS Publication 199;

- provide a stable yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies;

- create a foundation for the development of assessment methods and procedures for determining security control effectiveness; and

- improve communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

To assist organizations in making the appropriate selection of security controls for their information systems, NIST SP 800-53 introduced the concept of baseline controls. Baseline controls identify the starting point for the security control selection process – that is, the minimum set of security controls for an information system. Because the baseline is intended to be a broadly applicable starting point, the baseline can be tailored to achieve adequate risk mitigation. The tailored security control baseline is supplemented by an organizational assessment of risk, and the resulting controls are documented in the security plan for the information system.

NIST has organized security controls into classes and families for ease of use in the control selection and specification process. The following table summarizes the 3 classes and 18 families in the security control catalog and the associated family identifiers.

Security Control Classes, Identifiers, and Families		
Class	**Identifier**	**Family**
Management	CA	Certification, Accreditation, and Security Assessments
	PL	Planning
	PM	Program Management[a]
	RA	Risk Assessment
	SA	System and Services Acquisition
Operational	AT	Awareness and Training
	CM	Configuration Management
	CP	Contingency Planning
	IR	Incident Response
	MA	Maintenance
	MP	Media Protection
	PE	Physical and Environmental Protection
	PS	Personnel Security
	SI	System and Information Integrity
Technical	AC	Access Control
	AU	Audit and Accountability
	IA	Identification and Authentication
	SC	System and Communications Protection

[a] NIST SP 800-53, Revision 3, August 2009, added Program Management controls to complement the security controls for an information system by focusing on the organization-wide information security requirements that are independent of any specific information system and are essential for managing information security programs.

Objective

Our objective was to evaluate whether NASA's security practices and controls for [the reviewed system] were adequate to ensure the confidentiality, integrity, and availability of [the reviewed system's] data. We focused on selected controls that we considered necessary to mitigate the risk of outside intrusion and internal trespassing of [the reviewed system]. We also evaluated internal controls as they related to the objective. See Appendix A for details of the audit's scope and methodology, our review of internal controls as they related to the objective, and a list of prior audit coverage.

[THE REVIEWED SYSTEM'S] SECURITY CONTROL PRACTICES NEED IMPROVEMENT

During the audit, we evaluated security controls for 13 of 17 NIST SP 800-53 families that we considered the most critical to mitigate the risk of outside intrusion and internal trespassing of [the reviewed system]. We identified that [the reviewed system], which is categorized as a "high-impact system" under FIPS Publication 199, contained security controls that met NIST baseline requirements for an effective IT security posture for a system of its impact level. Such security controls included security awareness and training of personnel; contingency planning related to safeguarding data to include file backups and alternative processing sites in case of a disaster; procedures to protect system and information integrity, such as malicious code protection; and comprehensive access controls. However, we found several significant security control weaknesses in [the] NASA [system] that could threaten the confidentiality, integrity, and availability of critical information. NASA needs to fully implement the required baseline security controls for [the reviewed system] to protect the confidentiality, integrity, and availability of [the reviewed system's] data.

NASA and [the Contractor] Made Effective Use of Selected Security Controls

During our audit of [the reviewed system], we identified several effective security control practices in use by NASA and [the contractor] for security awareness and training, contingency planning, system and information integrity, and access control.

Security Awareness and Training. NASA and [the contractor] have established IT security awareness and training policy and procedures. NPR 2810.1A requires NASA to follow

- NIST SP 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," April 1998, which outlines a conceptual framework for providing IT security training; and

- NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," October 2003, which provides guidelines for building and maintaining a comprehensive security awareness and training program.

The NIST guidance states that Federal agencies and organizations should protect the confidentiality, integrity, and availability of information by ensuring that all those involved in using and managing IT

- understand their roles and responsibilities related to the organizational mission;
- understand the organization's IT security policy, procedures, and practices; and
- have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

We determined that [the contractor] had developed a process using its Computer User Registration Form (Registration) system to authorize access to [the reviewed system]. The Registration system requires data owner and supervisory approvals before allowing access to [the reviewed system]. Personnel with access to [the reviewed system] are required to complete annual IT security awareness training and the Registration system requires verification of that training. [The contractor] documented and tracked training through its internal computer-based training system for contractor personnel having access to [the reviewed system]. For NASA personnel with access to [the reviewed system], NASA tracked IT security awareness and training through its training system.

Contingency Planning. [The contractor] implemented procedures that would enable recovery of IT services following an emergency or system disruption. NPR 2810.1A requires NASA to follow the contingency planning guidance in NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002. NIST SP 800-34 defines contingency planning as interim measures to recover IT services following an emergency or system disruption. We found that [the contractor] performed a backup of electronic data weekly and then sent those backup media files to alternate storage locations. In addition, [the contractor] identified [appropriate] IT facilities at [. . .] as alternative processing sites in case of a disaster.

System and Information Integrity. [The contractor] implemented policies and procedures that protect information systems and related data from design flaws and data modification. Our review of selected servers [on the reviewed system] revealed that antivirus software was current and contained the most recent virus definitions. In addition, [the contractor]'s patch management procedures were operating as intended to ensure that operating system vulnerabilities of the [reviewed system's] servers were identified and addressed in a timely manner.

Access Control. Our review of [the reviewed system] user listings found that [the contractor] had strict account management practices in place. [The contractor] used its server operating system access enforcement controls to ensure only authorized users had access to [the reviewed system's] data. [The contractor]'s policy, [. . .], Revision 10, "Information Technology Resource Access," March 1, 2008, established and implemented controls for physical and logical (electronic) access to IT resources

managed by [the contractor], which includes [the reviewed system]. [The contractor] used the Registration system process identified in this policy for access enforcement and account management control procedures. Administrators used operating system and application controls to support [the contractor]'s Registration system process, which requires data owner approvals, including level of access, before allowing individuals access to [the reviewed system].

Improvements Needed to Fully Implement Security Controls for NASA's [Reviewed System]

[The reviewed system's] security control practices need improvement to ensure the confidentiality, integrity, and availability of critical information. We found that the latest approved [. . .] Security Plan [for the reviewed system] was not updated to appropriately address baseline security controls, vulnerability scanning procedures were not comprehensive, local administrator accounts were not configured properly, unauthorized software was found installed on [one of the reviewed system's] server[s], hardware and software inventories were not accurate and complete, and written confirmation was not obtained when media tapes were delivered to the storage facility. These security control issues occurred because

- NASA and [contractor] personnel did not always follow all Federal guidelines, contractual requirements, policies, and procedures;
- NASA officials did not provide continual oversight of contractual requirements;
- NASA officials did not update policies and procedures to incorporate the most current IT security practices nor did they disseminate policies and procedures to responsible personnel; and
- NASA officials did not proactively employ the most current practices to mitigate risks to critical information.

The issues we identified reduced the effectiveness of NASA's IT security program and increased the possibility that vulnerabilities will go undetected, remain uncorrected, and be exploited through malicious attacks. The potential for compromise of [the reviewed system], as well as other systems managed by [the contractor], could lead to degradation in or loss of NASA's mission capability or harm to individuals.

Outdated Security Plan. NASA and [contractor] officials had not properly updated the [reviewed system's] Security Plan, Revision D, since September 2008. Federal, NASA, and [contractor] regulations, policies, procedures, and guidance, as well as the contract between NASA and [the contractor], require the creation and maintenance of security plans containing security controls appropriate for the risks assigned to that system and that the security plans be current.

Federal, NASA, and [contractor] regulations, policies, procedures, and guidance essential in the preparation and maintenance of the [reviewed system's] Security Plan at the time of our audit included

- Office of Management and Budget (OMB) Circular No. A-130, Revised, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," November 28, 2000;

- NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," Revision 2, December 2007;

- NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems," Revision 1, February 2006;

- NPR 2810.1A, "Security of Information Technology," May 16, 2006;

- Information Technology Security (ITS)-Standard Operating Procedure (SOP)-0016B, "Subordinate Information Technology Security Plan Template, Requirements, Guidance and Examples," July 11, 2006; and

- [contractor's policy]

A complete listing of Federal, NASA, and [contractor] regulations, policies, procedures, and guidance, as well as a synopsis of those requirements, is provided in Appendix B.

We compared the [reviewed system's] Security Plan, Revision D, with requirements in NIST SP 800-53, Revision 2, which was the applicable guidance when the [reviewed system's] Security Plan was updated. We noted that not all security controls and security control enhancements were included. For example, the [reviewed system's] Security Plan contained 157 baseline security controls of the 163 baseline security controls for a high-impact system that are required by NIST SP 800-53, Revision 2. Examples of security controls not in the [reviewed system's] Security Plan included the following:

- **Security-Related Activity Planning.** The organization is to plan and coordinate activities affecting information systems before conducting such activities to reduce the impact on organizational operations, organizational assets, and individuals. (See Limited Vulnerability Scanning Coverage, on page 10.)

- **Information System Component Inventory.** The organization is to develop, document, and maintain an inventory of hardware and software components that is accurate and available for review and audit by designated organizational officials. (See Hardware and Software Inventory Controls Lacking, on page 12.)

Also, NIST SP 800-53, Revision 2, requires an additional 37 control enhancements that were not included in NIST SP 800-53, February 2005.

The [reviewed system's] Security Plan, Revision D, did not include the appropriate guidance for audit and accountability controls, nor did it reference the most recent guidance on vulnerability scanning. We identified the following issues in the [reviewed system's] Security Plan:

- NASA Information Technology Requirement (NITR) 2810-19, "Audit and Accountability Policy and Procedures," was issued in November 2008 as the replacement for NPR 2810.lA, Chapter 21, "Audit Trails and Accountability." However, NPR 2810.1A was not updated to reference the procedures outlined in NITR 2810-19. In addition, [contractor] IT security personnel were unaware that NITR 2810-19 replaced NPR 2810.1A, Chapter 21.

- The [reviewed system's] Security Plan references ITS-SOP-0038, "Procedure for Auditing and Accountability Controls," for audit and accountability controls. NASA officials stated that ITS-SOP-0038 was replaced by NITR 2810-19. However, ITS-SOP-0038 is not referenced in NITR 2810-19, and NASA officials could not provide us a copy of ITS-SOP-0038.

- NPR 2810.1A and ITS-SOP-0021 both reference and require adherence to NIST SP 800-42, "Guideline on Network Security Testing," October 2003, for vulnerability scanning. However, NIST SP 800-42 was replaced by NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," in September 2008. NIST SP 800-115 provides more current and detailed guidance on vulnerability scanning, security assessments, and network discovery.

If NASA IT security personnel are not aware of the most current security guidance, this can increase the risks to Agency information systems.

We also found that the [reviewed system's] Security Plan had not been periodically assessed or properly updated, contributing to the failure to identify references to expired and nonexistent criteria. For example, the Security Plan referenced five ITS-SOPs that expired between October 2007 and July 2008 and referenced two ITS-SOPs that NASA and [contractor] officials could not locate (see Appendix B, page 22, for a complete list of expired and nonexistent procedures referenced in the Security Plan). According to [the contractor]'s past two annual review letters, 10 [of the contractor's] system administrators reviewed the [system's] Security Plan for accuracy and completeness. However, these reviewers failed to identify the deficiencies noted in this audit report. The [reviewed system's] Security Plan even contradicts NPR 2810.1A by stating that updates are required every 3 years when, in fact, they are required annually.

Our analysis showed that [the contractor] did not update the [reviewed system's] Security Plan to reflect the format mandated by ITS-SOP-0016B to include specific information related to each system. We identified 43 instances in the [reviewed system's] Security Plan, Revision D, where the information was not complete. For example, the [reviewed system's] Security Plan did not include how often the organization should

- review and revise the plan to address system and organization changes or problems identified during plan implementation or security control assessments,

- conduct an assessment of the information system's security controls, or

- scan for vulnerabilities in the information system using appropriate vulnerability scanning tools and techniques.

In addition, because the [reviewed system's] Security Plan was not complete, it was not possible for the contractor who conducted the certification and accreditation analysis for [the reviewed system] to verify whether security controls had been implemented and were operating as intended. This problem was also identified in three other security plans supporting [the reviewed system]. Furthermore, the contractor had reported this problem 13 months before [the reviewed system's] Security Plan, Revision D, was issued. NPR 2810.1A requires information system owners to ensure that system security plans have been reviewed for completeness prior to proceeding with the certification and accreditation process. We found that NASA's review process did not identify that the [reviewed system's] Security Plan and the three supporting security plans were not complete prior to the certification and accreditation process.

These deficiencies occurred because officials in the NASA Office of the Chief Information Officer (OCIO) did not review, update, and disseminate all guidance related to system security plans. The NASA Chief Information Officer (CIO) is responsible for updating NPR 2810.1A and ITS-SOPs and for disseminating the information to the appropriate personnel. Because the updated guidance was not identified and referenced properly in NASA's IT security requirements publication, NASA and [contractor] IT security personnel were unaware of improvements that they could have applied to [the reviewed system].

In addition, the [responsible Center official] did not ensure that [the contractor] complied with NPR 2810.1A and ITS-SOP-0016B. As a result, the [reviewed system's] Security Plan was not complete, current, correct, or properly updated. Finally, the [. . .] Contracting Officer and the NASA CIO did not provide sufficient oversight to ensure that [the contractor] complied with contractual responsibilities, IT security requirements, and Federal, NASA, and [contractor] policies and procedures. Therefore, NASA officials cannot have assurance that all necessary security controls are in place and operating as required.

[Paragraph Redacted]

Limited Vulnerability Scanning Coverage. [The contractor's] internal IT auditors did not perform credentialed vulnerability scans on NASA's systems. Credentialed vulnerability scans are performed using administrator-level privileges, which allows vulnerability checks of all areas of an information system. In addition, the NASA CIO had not established procedures to eliminate or mitigate the risks associated with not performing credentialed scans. NPR 2810.1A states that hardware and software

configuration management activities should include an effective vulnerability reduction program that periodically scans for critical high-impact vulnerabilities. [One of the contractor's policies] requires [the contractor's] internal IT auditors to ignore credentials when performing vulnerability scans.

During our audit, we identified vulnerable software on one of the five [reviewed system's] servers in our sample (see Appendix A for details of our sample selection). The software had three vulnerabilities listed as high impact and one vulnerability listed as low impact by the U.S. Computer Emergency Readiness Team and NIST's National Vulnerability Database. Both organizations reported that the identified software could allow an attacker to gain full access to the affected system. If [the contractor]'s internal IT auditors performed credentialed scans, the software would have been detected and mitigation strategies would have been deployed. However, the [responsible Center official] stated that they did not perform credentialed scans because of concern about overutilization of server and network resources, which could create a denial of service for [the reviewed system] users. While this may have been true in the past when conducting credentialed vulnerability scans over the network, there are practices, such as customized filtering and host-based scans, that may minimize the disruption to servers and network resources. Credentialed vulnerability scans can be filtered and conducted at the specific server being targeted to minimize disruption to the system. By not performing credentialed scans, as many as 5,130 vulnerability checks of varying impact levels are rendered inoperable and high-impact vulnerabilities will go undetected. Further, [the contractor] manages [numerous] systems for NASA using the same vulnerability management practices.

While we understand that credentialed scans are not a NASA requirement, without supplemental mitigating strategies, such as ensuring accurate inventories and software discovery, un-credentialed scans are simply not sufficient to provide an acceptable level of security, as evidenced by our identification of vulnerable software on [the reviewed system].

By not performing credentialed scans, the probability that high-impact vulnerabilities remain undetected and uncorrected is increased. Risk cannot be effectively measured and mitigated in such an environment, increasing the possibility that vulnerabilities would be exploited by attackers.

Vulnerability of Local Administrator Accounts. [Out] of the five [reviewed system's] servers in our sample[, three] contained built-in administrator accounts that had not been renamed as required and their passwords had no expiration. [One of the contractor's policies] requires system administrators, prior to placing servers on NASA's network, to rename administrator accounts and set the passwords to expire every 60 days. Prior to a server being introduced into NASA's network, an initial scan report is generated to identify any built-in administrator accounts with noncompliant settings. [The contractor] provides this report to [a NASA official] when a server is initially placed in a production environment.

Although additional scans were performed during the life cycle of a server, [the contractor] did not provide the scan, which would identify built-in administrator account settings, to the [responsible Center official]. Therefore, if the built-in administrator account settings are changed to noncompliant after a server has been introduced into NASA's network, there is no process in place to identify those noncompliant settings. This essentially means that built-in administrator accounts could go through an entire life cycle of the server without the proper settings and without a process to mitigate this risk. The chances that an adversary could gain unauthorized access to [the reviewed system] increases if built-in administrator accounts are not configured with the proper settings and the passwords are not set to expire. Moreover, if [a] local administrator account [on a server of the reviewed system] is compromised, a skilled attacker could gain access to any of NASA's systems that are either physically or logically attached to [the reviewed system].

Use of Unauthorized Software. We also found that software had been installed on [the reviewed system's] server without [contractor] IT security officials' approval, and the software contained multiple high-impact vulnerabilities. [A policy of the contractor] dictates that any changes to server configurations must be processed through a system change request. [Contractor] officials determined that a third-party vendor had installed the software without [the contractor]'s approval and without submitting a system change request. [Contractor] IT security officials' attempt to track the software installation revealed no record of the change taking place.

This occurred because [the contractor] did not properly manage NASA's system to ensure that vulnerable software was not being installed and, if installed, was identified and removed. All [of the systems] managed [by the contractor] rely solely on manual intervention to ensure that their systems maintain an approved configuration. As evidenced by our audit findings, vulnerable software can be installed without prior review or approval by [contractor] IT security officials and can go undetected unless officials conduct a careful, manual review of server settings and installed software. However, [the contractor] does not conduct manual reviews of [the reviewed system's] servers. Rather, [the contractor] conducts only monthly un-credentialed scans and periodic IT security audits. The presence of unauthorized software could enable an attacker to execute arbitrary code, obtain sensitive information, bypass security restrictions, or cause a denial-of-service condition.

Hardware and Software Inventory Controls Lacking. NASA did not maintain an accurate inventory of active hardware and software components on [the reviewed system]. Contractual responsibilities require [the contractor] to follow the requirements in NPR 2810.1A, and NPR 2810.1A establishes the implementation of NIST publications on IT security, which includes NIST SP 800-53. NIST SP 800-53 requires organizations to develop, document, and maintain a current, accurate inventory of hardware and software components on their information systems. NIST SP 800-53 notes that the inventory should be available for review and audit.

During our audit, we requested a list of active [reviewed system] hardware components from [the contractor] so that we could select a sample for review to determine the accuracy of the hardware inventory. [Contractor] IT security personnel had a difficult time providing a list of active [reviewed system] hardware components because the list was not readily available to them. Once the list was provided, we determined that only 50 of the 231 components listed were active (12 components were no longer active and 169 were duplicate entries). Although we could not determine whether the list was complete, we were able to locate all of the [reviewed system's] hardware components on the list.

Because of the difficulties we encountered in obtaining an inventory of [the reviewed system's active] hardware components, in addition to the unauthorized, vulnerable software [. . .] that we identified, we concluded that [the contractor] had not implemented a process to ensure a current, accurate, complete, and readily available inventory and that the [. . .] Contracting Officer and the NASA CIO had not provided sufficient oversight to ensure that [the contractor] complied with its contractual responsibilities and with NIST SP-800-53 requirements. If an organization cannot easily produce an accurate listing of hardware and software components, as well as maintain accurate documentation of those components, the potential for exploitation of vulnerabilities that stem from a lack of security controls is increased.

Media Protection Needed. When [the contractor] transferred media tapes to a storage location at [another Federal facility], it did not obtain a written confirmation to verify their delivery. NASA Policy Directive 1440.6H, "NASA Records Management," March 24, 2008, requires NASA to identify, select, preserve, and protect records, which includes media tapes. [Contractor policy] does not require written receipts when media tapes are transferred. During our audit, we visited the storage location after a delivery was made, and the custodian noted that a media tape was missing from that delivery. The custodian stated that past deliveries also had been missing tapes. Because [the contractor] did not obtain written confirmation of the delivery, there was no assurance that the media tapes had actually been delivered. We believe that written confirmation of delivery of media tapes would provide the necessary security controls for media protection, which are needed to ensure continuity of operations; enable the Agency to perform emergency preparedness, response, and recovery; and protect Agency assets. We discussed the missing media tapes with a [contractor] official who revised [the contractor's policy] to require written confirmation of delivery, and [the contractor] reissued [the policy] on September 17, 2009. Accordingly, we are making no additional recommendation about this issue.

More Oversight Needed to Ensure Security of Systems and Data

The weaknesses we identified occurred because NASA did not have sufficient oversight to ensure that [the contractor] complied with security control requirements for [the reviewed system] and, possibly, the [numerous] other systems that [the contractor]

manages for NASA. We believe that NASA needs to enhance its oversight of [the contractor]'s management of systems containing NASA data, specifically for the weaknesses identified and discussed in this report concerning security plans, vulnerability scanning, administrator accounts, installation of software, and hardware and software inventory controls. In addition, to provide assurance that all controls are functioning to protect NASA's data and systems from attack or compromise, it is vital that NASA officials perform their duties in the following areas:

- The NASA CIO for IT Security has management oversight and responsibility for ensuring the confidentiality, integrity, and availability of IT resources.
- The [. . .] Contracting Officer has contract oversight to ensure [the contractor] complies with the terms of the contract.
- Center Information Technology Security Managers support the Center Chief Information Officers to ensure compliance with NASA policies, requirements, and directives and to maintain and track the status of all security plans, which includes monitoring contractors' security plans to ensure that IT security controls are current and correct.
- Center Organization Computer Security Officials are required to annually review system security plans and identify any changes that would require an update, such as changes in personnel, software and hardware, function, categories of information, information ownership, or risk. Organization Computer Security Officials are also required to verify the viability of the contingency plan and the date of the last test.
- Information system owners ensure that system security plans are developed and reviewed for completeness prior to the certification and accreditation process, conduct an annual test and assessment of the system security controls to assure effectiveness, and review the system security plans for completeness prior to the recertification and reaccreditation process.

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

To improve security control practices for [the reviewed system] and the other [. . .] systems managed by [the contractor], we made the following recommendations.

Recommendation 1. The Information System Owner for each of the [. . .] systems should

a. Update, as required, the system security plan to include the baseline security controls and the security control enhancements identified in the latest revision of NIST SP 800-53 and periodically assess the effectiveness of these controls.

b. Comply with the latest revision of ITS-SOP-0016 to ensure that the security plans are updated with the specific information related to the system.

Recommendation 2. The [responsible Center official] should direct [the contractor] to

a. Perform a comprehensive review at least annually of security plans for the [. . .] systems managed by [the contractor] for completeness and compliance prior to proceeding with any future recertification and reaccreditation.

b. Implement procedures for eliminating or mitigating the risk associated with not performing credentialed scans (if credentialed scans continue to not be required).

c. Establish procedures for monitoring built-in administrator account settings throughout the life cycle for any server placed in the production environment.

d. Implement comprehensive configuration management practices, which would include automated discovery and approved software lists.

e. Implement a process that ensures accurate and readily available inventories of active information system hardware and software components.

Recommendation 3. The NASA Chief Information Officer should

a. Update NPR 2810.1A to incorporate the requirements of NITR 2810-19, which was issued as the replacement for NPR 2810.1A, Chapter 21, to provide guidance on proper audit and accountability controls.

b. Develop and implement procedures for notifying Centers and designated officials when security control guidelines are updated or changed.

c. Require the use of credentialed scans, or implement supplemental controls that will reduce risk associated with not performing credentialed scans.

d. Update or replace ITS-SOP-0021, which expired October 5, 2007, to include more current security and vulnerability scanning guidance, and update NPR 2810.1A to reference the updated guidance.

Recommendation 4. The appropriate Organization Computer Security Official should review each of the other [. . .] systems managed by [the contractor] to determine whether their system has security control weaknesses similar to those identified for [the reviewed system]. If security control weaknesses exist, the Organization Computer Security Official should direct [the contractor] to correct those deficiencies, as outlined in Recommendation 2.

Recommendation 5. The NASA Chief Information Officer and the [. . .] Contracting Officer coordinate their efforts to ensure that the security control weaknesses we identified are corrected and incorporated in the contract.

Recommendation 6. The NASA Chief Information Officer should require all Center Information Technology Security Managers to

a. Track the status of all security plans assigned to their Center for compliance with the most current revisions of guidance from the National Institute of Standards and Technology and the NASA Office of the Chief Information Officer.

b. Ensure that controls are in place and effective for vulnerability scanning and configuration management.

Management's Response. In responding to our draft report, NASA provided separate responses from the OCIO [and other organizations] (see Appendix C [comments redacted]). Because we were unable to obtain a consolidated Agency response despite repeated requests, we reviewed and cross-referenced each response and found that, with the exception discussed below, all [. . .] organizations generally concurred with our recommendations.

The OCIO said that it would take steps to mitigate and improve [the reviewed system's] security control practices related to vulnerability scans, local administrator accounts, and hardware and software inventories on [the reviewed system's] servers and that it will review the other [. . .] systems managed by [the contractor] to identify and correct similar security control weaknesses that may exist in those systems. [. . .] However, [one organization] nonconcurred with our recommendation to implement comprehensive configuration management practices to include automated discovery and approved software lists [. . .]. [The organization] stated that it was in the process of developing a mitigation plan to prevent future occurrences of unauthorized software on the [reviewed system's] servers and that actions would be taken to determine whether this vulnerability exists in the other [contractor]-managed systems.

Evaluation of Management's Response. Although the OCIO [and other organizations] generally concurred with our recommendations and described the corrective steps they intend to take in response, they did not provide planned completion dates for these actions. Accordingly, we are requesting that NASA provide this information. With regard to [the] nonconcurrence with our recommendation to implement comprehensive configuration management practices, we do not believe that the [organization's rationale alleviated the need to implement our recommendation]. However, we find that the [organization's] proposed actions to develop a mitigation plan to prevent future occurrences of unauthorized software on the [reviewed system's] servers and validate whether this vulnerability exists for the other [. . .] systems are responsive to our recommendation. Accordingly, we will close the recommendations after verifying that NASA has taken the proposed corrective actions.

APPENDIX A

Scope and Methodology

We performed this audit from February 2009 through May 2010 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We performed the audit to review the security controls included in the [reviewed system's] Security Plan to mitigate the risk of outside intrusion or internal trespassing of [the reviewed system]. Audit work was performed at the [. . .] locations where [the reviewed system's] servers are maintained: [. . .]. NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," Revision 2, December 2007, applicable at the beginning of audit fieldwork, identified the security control baselines for information systems. We reviewed the [reviewed system's] latest [. . .] Security Plan, Revision D, September 26, 2008, to determine whether the security controls identified to mitigate risks for [the reviewed system] were in line with Federal requirements. Other documents used in our audit are described in Appendix B.

Audit Sample. [The reviewed system] comprises [numerous] servers [. . .]. We randomly selected [a small percentage] of these servers for review. The purpose of the sample was to randomly select servers for our audit, but the results from the sample were never intended to be projected to the population.

We reviewed selected controls on the five servers to determine whether the controls were adequately implemented. We selected 13 of 17 families (see the table on page 3; Program Management was not identified by NIST as a security control when we began our audit). We did not review (1) System and Services Acquisition, (2) Incident Response, (3) Maintenance, or (4) Personnel Security.

Computer-Processed Data. We did not use computer-processed data in the performance of this audit. We did however obtain information that was the result of data manually entered into the system via a word processor or spreadsheet. We verified the information provided and used during our audit to source documentation.

Review of Internal Controls

We examined controls for ensuring the confidentiality, integrity, and availability of [the reviewed system's] data. 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 last 5 years, the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) have issued seven reports relevant 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

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

"Final Memorandum on the Audit of the Reporting of NASA's National Security Systems" (IG-09-024, August 28, 2009)

"Federal Information Security Management Act: Fiscal Year 2008 Report from the Office of Inspector General" (IG-08-031, September 30, 2008)

"Controls over the Detection, Response, and Reporting of Network Security Incidents Needed Improvement at the Four NASA Centers Reviewed" (IG-07-014, June 19, 2007)

Government Accountability Office

"Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats" (GAO-10-230T, November 17, 2009)

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

"Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks" (GAO-10-3SU, October 15, 2009)

POLICIES AND PROCEDURES

In the evaluation of NASA's and [the contractor]'s efforts to secure [the reviewed system] and the data within, we reviewed the following Federal, NASA, and [contractor] laws, regulations, policies, procedures, and guidance to determine whether the requirements were being met in the [reviewed system's] operational environment.

Federal Guidelines

OMB Circular No. A-130, Revised, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," November 28, 2000. This Circular requires Federal agencies to implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in major applications. The Circular establishes the minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management controls systems established in accordance with OMB Circular No. A-123, "Management's Responsibility for Internal Control," (revised) December 21, 2004; and incorporates requirements of the Computer Security Act of 1987 (Public Law 100-235) and responsibilities assigned in applicable national security directives. The Circular also requires the review of application controls, stating that an independent review or audit of the security controls for each major application should be performed at least every 3 years; the review or audit should be independent of the manager responsible for the application because of the higher risk involved in major applications; and the review should verify that responsibility for the security of the application has been assigned, that a viable security plan for the application is in place, and that a manager has authorized the processing of the application. A deficiency in any of these controls should be considered a deficiency pursuant to the Federal Managers' Financial Integrity Act and OMB Circular No. A-123.

FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004. This publication specifies the standards for categorizing information and information systems supporting the executive agencies of the Federal Government. Security categorization standards for information and information systems provide a common framework and understanding for expressing security and promotes (1) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities and (2) consistent reporting to OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," September 2008. This publication provides guidelines for organizations on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies. It replaced NIST SP 800-42.

NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3, August 2009. This publication provides guidelines for selecting and specifying security controls for information systems. The guidelines apply to all components of an information system that processes, stores, or transmits Federal information and were developed to help achieve more secure information systems and effective risk management within the Federal Government. This latest revision of NIST SP 800-53 identifies 178 baseline security controls. Revision 2 (December 2007) had identified 163 baseline security controls, as had Revision 1 (December 2006). The original NIST SP 800-53, issued in February 2005, identified 157 baseline security controls.

NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems," July 2008. This publication provides guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the Federal Government. The guidelines apply to the security controls defined in NIST SP 800-53 (as amended) and any additional security controls developed by the organization. The guidelines were developed to help achieve more secure information systems within the Federal Government.

NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," October 2003. This publication provides guidelines for building and maintaining a comprehensive security awareness and training program.

NIST SP 800-42, "Guideline on Network Security Testing," October 2003 (replaced by NIST SP 800-115 in September 2008). NIST SP 800-42 provided guidance on network security testing. The main focus of the publication was the basic information about techniques and tools for individuals to begin a network security testing program, and it identified network testing requirements and how to prioritize testing activities with limited resources. It also described network security testing techniques and tools. NITS SP 800-42 also provided guidance to assist an organization in avoiding duplication of effort by providing a consistent approach to network security testing throughout the organization's networks. Further, it provided a feasible approach for organizations by offering varying levels of network security testing as appropriate to the organization's mission and security objectives.

NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002. This publication provides instructions, recommendations, and considerations for Government IT contingency planning.

NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems," Revision 1, February 2006. This publication provides the bulk of the information for preparing security plans. It stresses the importance of periodically assessing system security plans, to include a review of any change in the system status, functionality, or design to ensure that the plan continued to reflect the correct information about the system. The security plan and its correctness are critical for system certification activity. In addition, the publication states that all security plans should be reviewed and updated, if appropriate, at least annually. The completion of security plans is required by OMB Circular No. A-130, Appendix III.

NIST SP 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," April 1998. This publication outlines the conceptual framework for providing IT security training. This framework includes the IT security training requirements appropriate for today's distributed computing environment and provides flexibility for extension to accommodate future technologies and the related risk management decisions.

NASA Policies and Procedures

NPR 2810.1A, "Security of Information Technology," May 16, 2006. This NPR establishes the procedures and requirements of the NASA IT security program. The NPR provides direction to ensure the safeguards for protecting the confidentiality, integrity, and availability of unclassified IT resources are integrated into and support NASA's missions, functional lines of business, and infrastructure based on risk-managed, cost-effective IT security and information security principles and practices. The NPR requires that system security plans contain security controls appropriate for the risks assigned to that system, that required baseline security controls be periodically assessed to determine their effectiveness, and that security plans be updated annually. Security plans are considered living documents, with sections being added or modified, and should be reviewed annually to identify any changes that would require an update.
NPR 2810.1A also requires the Centers' Information Technology Security Managers to maintain and track the status of all system security plans assigned to their Center for compliance with NIST.

NITR 2810-19, "Audit and Accountability Policy and Procedures," November 12, 2008. NITRs are interim policies and requirements necessary to address new issues and to clarify existing policy and requirements. Once a NITR has been incorporated into the appropriate NPR, it is canceled. This NITR provided NASA information system audit and accountability policy and procedures to meet current NIST requirements.
NITR 2810-19 is a replacement for NPR 2810.1A, Chapter 21, "Audit Trail and Accountability." It has not yet been incorporated into the NPR.

ITS-SOP-0016C, "Information Technology Security Plan Template, Requirements, Guidance and Examples," April 17, 2008. This procedure provides requirements,

guidance, and examples for the completion of IT security plans and implements the baseline security controls in NIST SP 800-53. It also requires that every baseline security control be addressed in the security plan, whether it is applicable or not applicable to (or not accepted by) the system. The template identifies information such as the frequency and criteria for testing security controls to allow an organization to tailor the security controls to support specific mission, business, or operational needs. ITS-SOP-0016C replaced ITS-SOP-0016B, issued July 11, 2006.

ITS-SOP-0021, "Network Security Vulnerability Scanning," effective October 5, 2005, expired October 5, 2007. This procedure provided guidance on network vulnerability scanning. NPR 2810.1A requires that the Center Information Technology Security Manager, along with two other NASA officials, develop and maintain this procedure. This procedure also referenced NIST SP 800-42, which was replaced by NIST SP 800-115 in September 2008. ITS-SOP-0021 is no longer included in the NASA Online Directives Information System although it is still referenced in NPR 2810.1A.

[Contractor] Policies and Procedures

[Paragraphs Redacted]

Updated, Expired, or Nonexistent Guidance

Updated Federal Guidance

NPR 2810.1A and ITS-SOP-0021 both reference and require NIST SP 800-42. NIST SP 800-115 replaced NIST SP 800-42 in September 2008 and provides more detailed guidance on network and software discovery and vulnerability scanning and mitigation.

Expired or Nonexistent NASA Procedures

The following procedures are identified in the [reviewed system's] Security Plan, Revision D, even though expired. Two procedures have been expired for more than 2 years. All of the procedures have been removed from the NASA Online Directives Information System, except ITS-SOP-0033 (even though expired) and ITS-SOP-0006, which was reissued with an effective date of January 11, 2010.[5]

- ITS-SOP-0018, "Contract IT Security Program Plan Procedures," effective October 5, 2005 (expired October 5, 2007)

[5] ITS-SOPs no longer exist and are now referred to as ITS Handbooks. ITS-SOP-0006 was reissued as ITS-HBK-0006.

- ITS-SOP-0021, "Network Security Vulnerability Scanning" effective October 5, 2005 (expired October 5, 2007)

- ITS-SOP-0019B, "Procedure for the FIPS-199 Categorization of Information Systems," effective July 11, 2006 (expired July 11, 2008)

- ITS-SOP-0032, "Master Information Technology Security Plan Template, Requirements, Guidance and Examples," effective July 11, 2006 (expired July 11, 2008)

- ITS-SOP-0013, "Procedures for Routine NASA Network and Context Monitoring," effective July 18, 2006 (expired July 18, 2008)

- ITS-SOP-0006C, "Procedures for Extending an IT System Authorization to Operate," effective March 3, 2007 (expired March 3, 2009)

- ITS-SOP-0014, "Procedures for Approving Changes to NASA's Information Technology Baseline," effective April 18, 2006 (expired April 18, 2009)

- ITS-SOP-0033, "External System Identification and IT Security Requirements," effective July 19, 2007 (expired July 19, 2009)

The [reviewed system's] Security Plan, Revision D, also references two ITS-SOPs that we were unable to locate, and NASA officials could not provide us a copy.

- ITS-SOP-0011, "Procedure for Development and Life-Cycle of NASA Master Security Plans"

- ITS-SOP-0038, "Procedure for Audit and Accountability Controls"

MANAGEMENT COMMENTS

Comments
Redacted

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief Information Officer
[some addressees deleted]
Information Technology Security Manager, Ames Research Center
Information Technology Security Manager, Dryden Flight Research Center
Information Technology Security Manager, Glenn Research Center
Information Technology Security Manager, Goddard Space Flight Center
Information Technology Security Manager, Headquarters
Information Technology Security Manager, Jet Propulsion Laboratory
Information Technology Security Manager, Johnson Space Center
Information Technology Security Manager, Kennedy Space Center
Information Technology Security Manager, Langley Research Center
Information Technology Security Manager, Marshall Space Flight Center
Information Technology Security Manager, NASA Shared Services Center
Information Technology Security Manager, Stennis Space 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

Congressional Committees and Subcommittees, Chairman and Ranking Member (continued)

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
Vincent Small, Project Manager
Bret Skalsky, Team Lead
Bessie Cox, Auditor
Christopher Reeves, IT Specialist

REDACTED FOR PUBLIC RELEASE

AUGUST 5, 2010

REPORT No. IG-10-018-R

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.