

DECEMBER 5, 2011

---

AUDIT REPORT

---

---

OFFICE OF AUDITS

NASA FACES SIGNIFICANT CHALLENGES IN  
TRANSITIONING TO A CONTINUOUS MONITORING  
APPROACH FOR ITS  
INFORMATION TECHNOLOGY SYSTEMS

---

---

OFFICE OF INSPECTOR GENERAL

---

---



National Aeronautics and  
Space Administration

REPORT No. IG-12-006 (ASSIGNMENT No. A-11-003-00)

Final report released by:



Paul K. Martin  
Inspector General

## Acronyms

---

ASCS	Agency Security Configuration Standards
AVAR	Agency Vulnerability Assessment and Remediation
C&A	Certification and Accreditation
CAT	Configuration Assessment Tool
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IT	Information Technology
ITSEC-EDW	Information Technology Security – Enterprise Data Warehouse
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
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

---

---

## OVERVIEW

---

# NASA FACES SIGNIFICANT CHALLENGES IN TRANSITIONING TO A CONTINUOUS MONITORING APPROACH FOR ITS INFORMATION TECHNOLOGY SYSTEMS

## The Issue

---

Cyber-based threats to NASA's information technology (IT) systems come from a variety of sources, including foreign nations, criminals, terrorists, and disgruntled employees. Combating these threats requires a dynamic security process that effectively and timely identifies and mitigates vulnerabilities in NASA's IT system components.

The Federal Information Security Management Act of 2002 (FISMA) requires NASA and other Federal agencies to annually report the security posture of their information systems.<sup>1</sup> Prior to May 2010, NASA assessed the security posture of its systems using a "snapshot" certification and accreditation (C&A) process in which the Agency assessed security on a periodic schedule and at a fixed point in time. Under this approach, NASA required system owners to reauthorize their systems on a 3-year cycle and placed little emphasis on the use of automation to continuously monitor critical IT controls.

In April 2010, the Office of Management and Budget (OMB) issued new guidance on FISMA reporting requirements that emphasized continuous monitoring to provide ongoing, near real-time risk management and operational security for IT systems. In May 2010, NASA's Office of the Chief Information Officer (OCIO) suspended the C&A process it had been using for reviewing operational IT systems in favor of what it called "a more streamlined system security authorization process with a focus on continuous monitoring, automated tools, and significant paperwork reduction."<sup>2</sup> In a May 2010 interview with *Federal Computer Week*, NASA's Deputy Chief Information Officer (CIO) for Information Technology Security said that C&A "will still be done, but the way we do it is going to change significantly and the frequency of it will change. Instead of every 3 years . . . you're always going to be looking at those controls and adjusting them for changes."<sup>3</sup>

---

<sup>1</sup> See Appendix B for the glossary of terms used in this report.

<sup>2</sup> NASA OCIO memorandum, "Suspension of Certification and Accreditation Activity," May 18, 2010 (see Appendix C).

<sup>3</sup> Ben Bain, "A NASA deputy CIO explains NASA's new policy for certifying its systems as secure," *Federal Computer News*, May 24, 2010.

As part of the transition to a continuous monitoring program, NASA has undertaken the following initiatives:

- Developed the IT Security – Enterprise Data Warehouse (ITSEC-EDW), an inventory of NASA IT components and related security information.
- Formed the Agency Vulnerability Assessment and Remediation (AVAR) team, which is responsible for the Agency’s vulnerability management project and for Foundstone Enterprise, the Agency’s automated network vulnerability scanning tool, as well as for communication between Foundstone Enterprise and ITSEC-EDW.<sup>4</sup>
- Instituted the Agency Security Configuration Standards (ASCS) project to provide assessments, recommendations, processes, and procedures to assist NASA in meeting system security configuration requirements.

This audit reviewed NASA practices to determine whether the Agency was establishing a solid foundation to implement a continuous monitoring program. Specifically, we focused on NASA’s progress in three key elements: record of IT components, configuration management, and vulnerability monitoring.

## Results

---

Although NASA has made progress in transitioning to a continuous monitoring program, the Agency needs to take significant steps to ensure the successful implementation of its program. Specifically, NASA needs to (1) create and maintain a complete, up-to-date record of IT components connected to Agency networks; (2) define the security configuration baselines that are required for its system components and develop an effective means of assessing compliance with those baselines; and (3) use best practices for vulnerability management on all its IT systems. Failure to make improvements in each of these areas will limit NASA’s ability to accurately assess the security of its IT systems.

**Agency Continuous Monitoring and Reporting System Data Are Incomplete.** We found that to ensure successful implementation of continuous monitoring, NASA needs to significantly improve its procedures for recording IT components in ITSEC-EDW, the database it uses to track and report its security posture. NASA’s goal is to monitor 100 percent of its systems and connected components. The first step toward that goal is compiling a complete and up-to-date inventory that provides IT security personnel with a real-time awareness of all components connected to their systems that need protection.

---

<sup>4</sup> Foundstone Enterprise is the commercial off-the-shelf enterprise software solution used when scanning NASA’s networks and systems for vulnerabilities. (McAfee, the manufacturer of Foundstone Enterprise, recently changed the name of the product to Vulnerability Manager.)

NASA established ITSEC-EDW in response to a recommendation we made in a September 2010 audit.<sup>5</sup> As mentioned above, ITSEC-EDW is intended to serve as an automated data warehouse providing an inventory of NASA IT components and related security information. However, we found that the majority of components we reviewed were not included in ITSEC-EDW and that the information concerning the remaining components in the sample was incomplete. Specifically, we judgmentally selected a sample of 289 components connected to NASA systems and found that 175 of these components (61 percent) were not included in the database and that patch agent or vulnerability data was missing for 93 others (32 percent). Moreover, ITSEC-EDW included both patch agent and vulnerability data for only 21 of the 289 component (7 percent) we tested. Failure to maintain a complete and up-to-date inventory of components in ITSEC-EDW will significantly diminish the effectiveness of NASA's continuous monitoring program.

**Security Configuration Baselines Are Not Available and Continuously Monitored on Many IT Components.** NASA's IT components require secure configurations to protect them from internal and external threats. A security configuration baseline is a collection of security settings for components such as file servers, web servers, application servers, and clients that provides a compliance benchmark for how an organization's computer systems are to be configured. Where there are no generally accepted baseline settings for a particular system, Agencies must either adopt other measures, such as Center for Internet Security (CIS) benchmarks, or develop their own security configuration baselines.

For its Windows desktop operating systems, Microsoft Windows XP and Vista, NASA uses Federal Desktop Core Configuration (FDCC) baseline settings. NASA has automated means for tracking compliance with FDCC settings and reports compliance with these settings to OMB. For components such as Unix/Linux and Windows server components that have no FDCC baselines, NASA has adopted CIS benchmarks. NASA does not have automated means for tracking compliance with CIS benchmarks. Our review focused on NASA systems that use CIS benchmarks.

We found that the implementation of CIS benchmarks varies widely from one system to the next across the Agency and that no processes are in place to measure and monitor benchmark compliance. Without an effective monitoring and measurement capability, system owners and NASA management have limited means for determining whether systems are compliant or are meeting the IT security goals of the Agency.

**Inconsistent Vulnerability Monitoring Is Not Effective in Identifying All Known, High-Impact Vulnerabilities.** Vulnerability scanning is an important aspect of continuous monitoring that can help identify all known, high-impact vulnerabilities within a system's components. Vulnerability scans can be performed as credentialed or non-credentialed. A credentialed scan uses administrator rights on the target host, while

---

<sup>5</sup> NASA OIG, "Audit of NASA's Efforts to Continuously Monitor Critical Information Technology Security Controls" (IG-10-019, September 14, 2010).

a non-credentialed scan does not. Administrator rights are permissions granted to users allowing them to view installed software and to make changes to computer system configurations.<sup>6</sup>

Our review of 13 NASA systems revealed inconsistent vulnerability monitoring practices. We identified unmonitored systems with multiple high-impact vulnerabilities, monitored systems that still contained multiple high-impact vulnerabilities, and monitored systems with very few high-impact vulnerabilities.

We requested the Agency's recent vulnerability scan results for the monitored systems and were provided with non-credentialed scans. We then requested that NASA IT security personnel perform credentialed scans of these same systems, which we observed. These credentialed scans consistently revealed a much larger number of high-impact vulnerabilities than had been identified by the non-credentialed scans. For example, although the credentialed scans were performed on only a small sample of system components, they identified a staggering 2,644 high-impact vulnerabilities compared with 59 high-impact vulnerabilities identified by the non-credentialed scans. These results illustrate that NASA's current vulnerability monitoring practices capture only a small fraction of the known, high-impact vulnerabilities in NASA's systems. Further, using only non-credentialed vulnerability scanning practices increases the risk of loss of confidentiality, integrity, and availability of NASA systems, data, and intellectual property.

In sum, NASA's move away from a "snapshot" approach for certifying the security of its IT systems to a continuous monitoring approach holds the promise of improving NASA's IT security posture. However, while NASA has made some progress in implementing this new approach, the Agency needs to improve its policies and procedures in several key areas to ensure continuous monitoring will provide adequate protection for the Agency's IT systems.

## Management Action

---

To strengthen existing policies, procedures, and continuous monitoring controls, we recommended that the CIO expedite development of content and metrics for applying secure baseline configuration settings to applicable NASA IT components. In addition, we believe the CIO should institute credentialed vulnerability scanning Agency-wide as part of its continuous monitoring program.

We also recommended that Associate Administrators for Mission Directorates and Center Chief Information Security Officers take an active role to ensure that baseline security configurations are applied to their respective systems; appropriate personnel establish

---

<sup>6</sup> A credentialed scan will identify software installed on a component while a non-credentialed scan will not.

accounts within ITSEC-EDW; appropriate system data are included in ITSEC-EDW and validated; and systems are routinely undergoing credentialed vulnerability scanning.

In response to a draft of this report, NASA concurred with our recommendations and proposed corrective actions to address security configuration baselines, credentialed vulnerability scanning, and maintaining an accurate account of security data for all NASA systems components. NASA plans to complete these actions by January 31, 2013. We consider NASA's planned actions to be responsive to our recommendations, and will close the recommendations upon verification that the actions are complete.





---

---

**CONTENTS**

---

INTRODUCTION

Background _____	1
Objectives _____	2

RESULTS

NASA Has Not Transitioned to an Effective Continuous Monitoring Program _____	4
---	---

APPENDIX A

Scope and Methodology _____	15
Review of Internal Controls _____	17
Prior Coverage _____	18

APPENDIX B

Glossary _____	19
----------------	----

APPENDIX C

NASA OCIO Memorandum _____	22
----------------------------	----

APPENDIX D

Management Comments _____	26
---------------------------	----

APPENDIX E

Report Distribution _____	31
---------------------------	----



---

---

## INTRODUCTION

---

### Background

As technology has advanced, NASA has become dependent on computerized information systems to carry out daily operations and to process, maintain, and report essential information. NASA's information technology (IT) networks and systems control spacecraft, collect and process scientific data, and enable NASA personnel to collaborate with colleagues around the world. Users of these systems number in the hundreds of thousands and include NASA personnel, contractors, academia, and the public. Although most NASA IT systems contain data appropriate for wide dissemination, some contain sensitive information that, if stolen or inappropriately released, could result in significant financial loss or adversely affect national security.

The increasing number of cybersecurity threats facing NASA highlights the significance of ensuring that strong IT security practices are in place at the Agency. In calendar years 2009 and 2010, NASA reported 5,621 cybersecurity incidents that could have resulted in the installation of malicious software on its systems and unauthorized access to sensitive information. These threats continue to evolve in both scope and sophistication, presenting an ongoing challenge to NASA management. Consequently, strong IT security practices are essential to minimize the number and severity of vulnerabilities on NASA's systems.

The Federal Information Security Management Act of 2002 (FISMA) requires Federal agencies to annually report the security posture of their information systems. Prior to May 2010, NASA assessed the security posture of its systems using a "snapshot" certification and accreditation (C&A) process that assessed security on a periodic schedule and at a fixed point in time. Under this approach, NASA required system owners to reauthorize their systems on a 3-year cycle.

In May 2010, NASA announced a fundamental shift away from this "snapshot" C&A approach to real-time, device-level continuous monitoring. According to the Agency, this shift would enable near real-time risk management and ongoing security authorizations that reflect the true intent of applicable National Institute of Standards and Technology (NIST) guidance. NASA's new approach emphasizes the importance of continuously monitoring components connected to NASA's systems and focuses on critical controls that protect against the most common IT security incidents NASA has experienced.

The initial phases of any continuous monitoring process rely on three elements that are of primary importance to system monitoring: maintaining complete and accurate IT component inventories; implementing effective security configuration management;

and vulnerability management. As part of its continuous monitoring program, NASA has undertaken the following initiatives:

- Developed the IT Security – Enterprise Data Warehouse (ITSEC-EDW), an inventory of NASA IT components and security configurations. ITSEC-EDW also includes consolidated patch statistics, vulnerability scan results, hardware and software data, and correlation capabilities.
- Formed the Agency Vulnerability Assessment and Remediation (AVAR) team, which is responsible for the Agency’s vulnerability management project and for Foundstone Enterprise, the Agency’s automated network vulnerability scanning tool, as well as for communication between Foundstone Enterprise and ITSEC-EDW.<sup>7</sup>
- Instituted the Agency Security Configuration Standards (ASCS) project that provides assessments, recommendations, processes, and procedures to assist NASA in meeting system security configuration requirements. NASA currently has three sources for its system configuration standards: United States Government Configuration Baseline (USGCB) settings, Federal Desktop Core Configuration (FDCC) settings, and Center for Internet Security (CIS) benchmark settings.

While these initiatives are appropriate steps to achieving a successful real-time continuous monitoring program, we believe that NASA needs to do more to ensure that its continuous monitoring efforts are based on a solid foundation and have the maximum chance of success.

## Objectives

The objective of this audit was to evaluate NASA’s progress in moving from a periodic C&A assessment to continuously monitoring its IT security posture. This report focuses on three areas that we consider key to the successful implementation of the Agency’s overall continuous monitoring program: maintaining accurate IT component inventories; instituting strong security configuration management; and vulnerability management practices.

To assess the Agency’s progress in these three areas, we examined the extent to which NASA’s ITSEC-EDW captures all relevant IT components; whether mandated configuration settings were being appropriately applied to components; and whether vulnerability monitoring practices were effective for identifying and mitigating known, high-impact vulnerabilities. We also reviewed internal controls related to our overall

---

<sup>7</sup> Foundstone Enterprise is the commercial off-the-shelf enterprise software solution used when scanning NASA’s networks and systems for vulnerabilities. (McAfee is the manufacturer of Foundstone Enterprise and has recently changed the name of the product to Vulnerability Manager.)

objective. We performed our work at four Centers. See Appendix A for details of the audit's scope and methodology, our review of internal controls, and a list of prior audit coverage. See Appendix B for a glossary of terms used in this report.

---

---

## **NASA HAS NOT TRANSITIONED TO AN EFFECTIVE CONTINUOUS MONITORING PROGRAM**

---

NASA has not yet successfully transitioned from “snapshot” C&A processes to a fully implemented continuous monitoring program. In order for the Agency to reach this goal, it needs to (1) create and maintain a complete, up-to-date record of IT components connected to its networks; (2) define the security configuration baselines required for its system components and develop an effective means of assessing compliance with those baselines; and (3) establish best practices for vulnerability management on all Agency IT systems.

### **Agency Continuous Monitoring and Reporting System Data Are Incomplete**

We found that NASA lacks a complete inventory database of IT components currently in use. Without a complete and up-to-date inventory of IT components, the effectiveness of NASA’s continuous monitoring program will be significantly diminished.

In September 2010, we recommended that NASA’s Chief Information Officer (CIO) require the Centers to implement a process to verify that their vulnerability monitoring includes 100 percent of applicable network devices. NASA agreed and stated it planned to implement a new system, ITSEC-EDW, that would include an Agency-wide database of the IT components connected to NASA’s networks. NASA’s CIO stated that the IT component information in the database would come from network vulnerability scans and NASA’s patch management and reporting system, among other sources.

ITSEC-EDW retrieves data from multiple Agency and Center data sources to provide a continuously updated record of components connected to NASA’s networks. In NASA Information Technology Requirement (NITR) 2810-24, “NASA IT Device Vulnerability Management,” January 28, 2010, NASA mandated that Centers use ITSEC-EDW and required that C&A information on all NASA systems include “an asset inventory listing all IT components associated with the information system.” This guidance, which expired on May 16, 2011, was subsequently included as part of the IT Security Handbook (ITS-HBK) 2810.07-01, “Configuration Management,” May 6, 2011.

The policy makes clear the IT security challenge the Agency faces in making the transition to continuous monitoring:

There are more than 120,000 devices or nodes located at NASA Centers and Facilities, and connected to NASA networks. Each of these nodes can be a potential vector for unauthorized access, virus infection, or some other security incident. The purpose of this policy is to protect each device by defining standard security measures against viruses and other malware, ensuring patches are applied, setting requirements

for vulnerability scans, and establishing an inventory of all devices and their security configurations.

As part of continuously monitoring IT security, NASA officials said they strive to monitor 100 percent of the Agency's systems and connected components. The first step toward that goal is maintaining a comprehensive record of IT components so that Center Chief Information Security Officers (CISOs) have a real-time awareness of all components connected to their systems.<sup>8</sup> According to the project manager for ITSEC-EDW, the Agency has three ways to ensure that applicable system component information is added to and updated in the database. Two of those ways are automated through the use of software applications that transfer information to ITSEC-EDW. The third way is to input information manually when automation is not technically feasible due to operational constraints. While the Agency envisioned ITSEC-EDW as a comprehensive database to track and report NASA's IT security posture, we found a significant portion of the components we sampled were not included in ITSEC-EDW and that important information concerning our sampled components was incomplete.

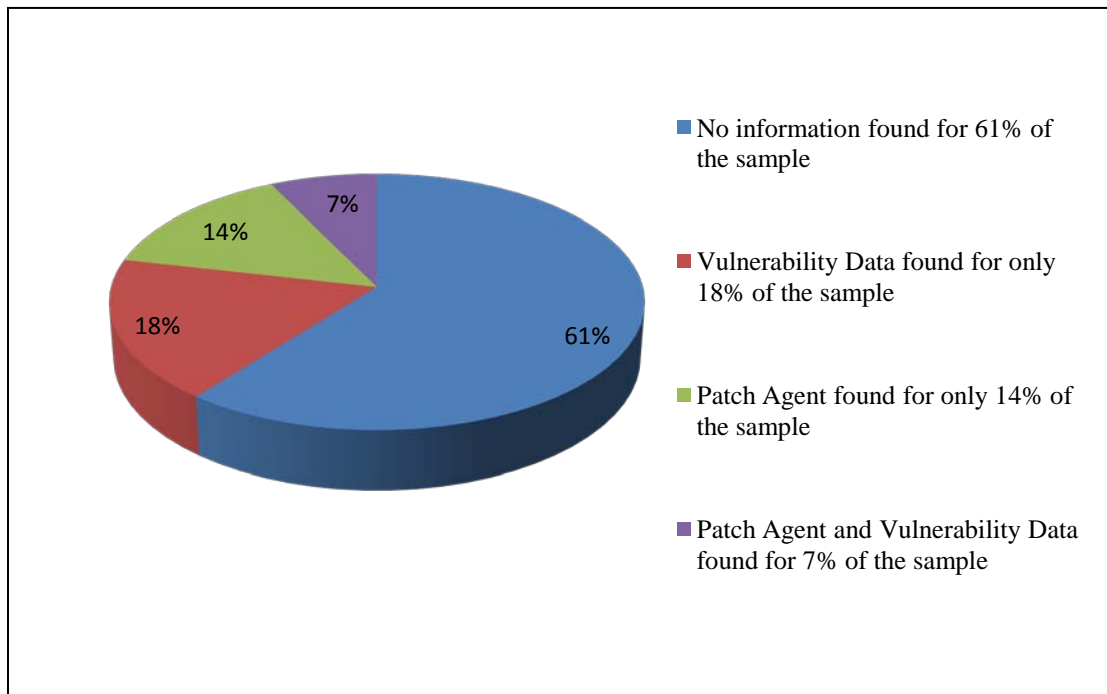
To assess the accuracy of the ITSEC-EDW, we judgmentally selected a sample of 289 connected components from 12 systems across four Centers.<sup>9</sup> We found that 175 of these components (61 percent) were not reflected in the database and that patch agent and vulnerability data for 93 others (32 percent) was incomplete. Moreover, only 21 of the 289 components (7 percent) we sampled included both patch agent and vulnerability data. In summary, we found that ITSEC-EDW was not comprehensively or consistently capturing the IT component information, vulnerability information, or security configuration data needed to ensure the successful implementation of continuous monitoring at NASA. A breakdown of the ITSEC-EDW component queries we conducted is shown in Figure 1.

---

<sup>8</sup> The title for NASA's IT Security Managers changed to Center CISOs in May 2011.

<sup>9</sup> We excluded 1 of the 13 systems originally in our sample because it was not connected to any other Agency network.

**Figure 1. Results of ITSEC-EDW Queries for 289 System Components to Identify Patch Agent and Vulnerability Data**



NITR 2810-24 requires system owners to record all IT components in ITSEC-EDW. However, the overwhelming majority of the components we tested were not included in the database. Until the Agency ensures that it has a more comprehensive inventory of the components connected to its systems, the effectiveness of its continuous monitoring program will be significantly diminished.

### **Security Configuration Baselines Are Not Available and Continuously Monitored on Many IT Components**

Security configuration baselines are essential for protecting systems and data. Of critical importance is establishing security baseline settings for system components and maintaining those security settings throughout the components' life cycles. Security configuration baselines include specific settings needed to ensure a system is protected from malicious attacks. These baselines should be established for both hardware and software connected to a NASA system or network, and any changes to the baseline should be monitored and addressed.

In September 2004, NASA adopted the CIS benchmarks for applying security configuration baselines to many of its operating systems, including Windows, Unix, and various types of Linux. Accordingly, CIS benchmarks are applicable to the desktops, laptops, and servers used by thousands of NASA's employees and contractors.



In February 2008, the Office of Management and Budget (OMB) mandated that Federal agencies apply NIST's FDCC settings to Windows XP and Vista desktop operating systems. These settings provide Federal agencies with commonly accepted baseline security settings for these operating systems. NASA automatically tracks compliance with FDCC settings on its Windows XP and Vista components and reports compliance status to OMB. However, as previously noted, NASA uses CIS benchmarks for applying security configuration baselines to Unix, Linux, and Windows server operating systems. We found that implementation of CIS benchmarks varies widely from system to system. In addition, NASA has no processes in place to measure and monitor CIS benchmark compliance.

To examine NASA's compliance with CIS benchmarks, we used the same sample of 12 systems discussed above. We found that 2 systems had obtained waivers from benchmark requirements because both had operational constraints that prevented CIS benchmark application and 1 system was composed of FDCC-compliant components. We selected a sample of components from the remaining 9 systems and used the CIS Configuration Assessment Tool (CAT) to assess their compliance with the benchmarks. We found compliance scores ranging between 36 and 93 percent, indicating configuration settings were not fully compliant with the benchmark standards. Due to the wide variation in these scores, we evaluated the CAT assessment tool itself and found the following limitations:

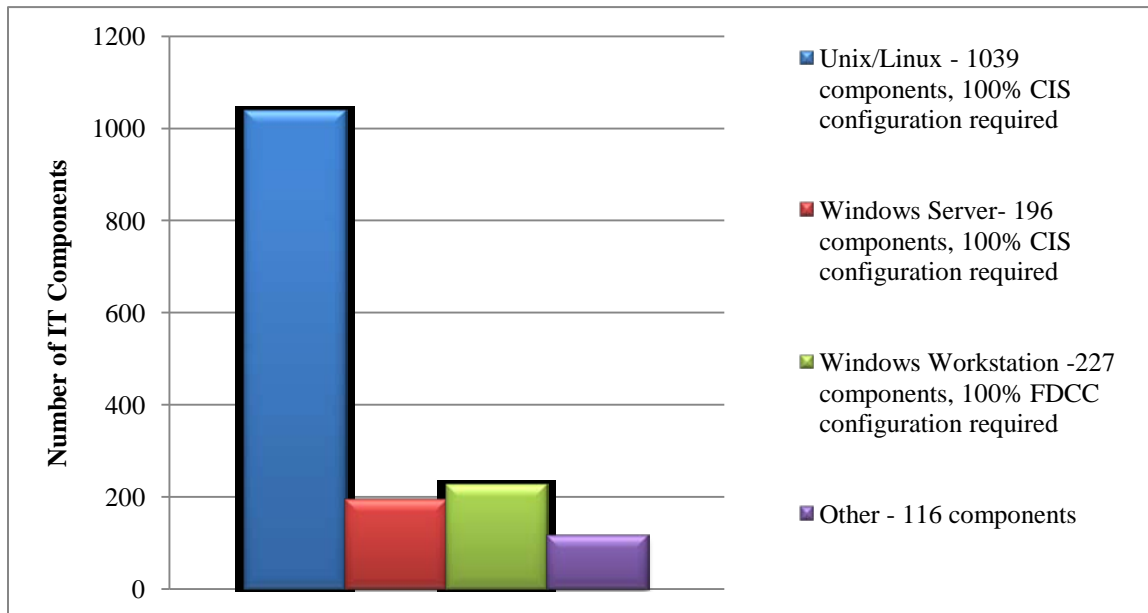
- CIS benchmark metrics were not developed specifically for NASA and many NASA components have more stringent settings or operational constraints. Consequently, NASA deviates from the benchmark in many cases, and some of the settings that CAT reported as failures are actually more secure than the benchmark. In those instances, modifying the settings to conform to CIS benchmarks would actually have a negative effect on the security of NASA's operating environment.
- CAT can only be run against one component at a time. Because NASA has more than 120,000 components that need to be monitored for baseline compliance, CAT may not be a viable tool for continuously monitoring NASA's systems.

Given these limitations and the need to continuously monitor components throughout their life cycles, it is important that NASA clearly define what baseline configuration settings are appropriate to meet the Agency IT security goals. The wide variance in compliance scores occurred because NASA had not established baseline configuration settings, metrics, and a monitoring capability for all of its operating system environments. Therefore, NASA needs to determine what benchmark settings are appropriate for securing the Agency's IT assets.

We also found that even though the CIS benchmark requirement applies to a significant number of components that we reviewed, ITSEC-EDW reports information only on FDCC rather than CIS compliance. Consequently, this can lead to a misconception of NASA's IT security posture when the Agency reports to OMB through ITSEC-EDW.

For example, of the 1,578 IT components connected to NASA’s systems that we reviewed, only 14 percent (227 components) were required to comply with FDCC and would be included in NASA’s IT security reporting to OMB. Therefore, 86 percent of the components in our review would not be included in the Agency’s reporting (1,039 components with a Unix/Linux operating system, 196 components with a Windows server operating system, and 116 components identified as other shown in Figure 2).<sup>10</sup>

**Figure 2. Operating Systems on Components Reviewed**



Improperly configured operating systems and software applications are a frequent avenue for unauthorized access to NASA’s systems. Without the capability to continuously monitor components for compliance with defined baselines, NASA does not have adequate assurance that its systems are protected against malicious attacks. Conversely, with an effective monitoring and measurement capability, system owners, auditors, and NASA management would have the means to determine whether systems are compliant and are meeting the IT security goals of the Agency.

<sup>10</sup> For this portion of our review, we relied on hardware and software documentation provided by the system personnel. The 116 components identified as “Other” in Figure 2 had no known configuration benchmark requirement.

## **Vulnerability Management Is Not Occurring Consistently and Is Not Effective in Identifying All Known, High-Impact Vulnerabilities**

NASA Centers use the McAfee Foundstone Enterprise application to scan their networks for known vulnerabilities. NASA's AVAR project coordinates vulnerability scanning processes, tools, and licensing for all NASA Centers. Mission Directorate and Center program and project managers are responsible for performing vulnerability scans on local NASA systems to identify high-impact vulnerabilities and for managing the local vulnerability scanners. NASA policy states that scans are to be conducted monthly for all known, high-impact vulnerabilities and that any vulnerabilities identified are to be addressed in a plan of action and milestones. As categorized by the United States Computer Emergency Readiness Team (US-CERT), high-impact vulnerabilities are vulnerabilities such as unpatched software that could pose the most risk to the system and could be the most damaging if exploited.

Vulnerability scans can be performed as credentialed or non-credentialed. A credentialed scan uses administrator rights on the target host, while a non-credentialed scan does not. Administrator rights are permissions granted to users allowing them to view installed software and to make changes to computer system configurations. Both scanning techniques will produce a report on vulnerabilities with impact ratings of High, Medium, Low, and Informational, but a credentialed scan performs a much more thorough check of the system and produces more accurate results. For example, a credentialed scan will identify vulnerable software installed on a component, while a non-credentialed scan will not.

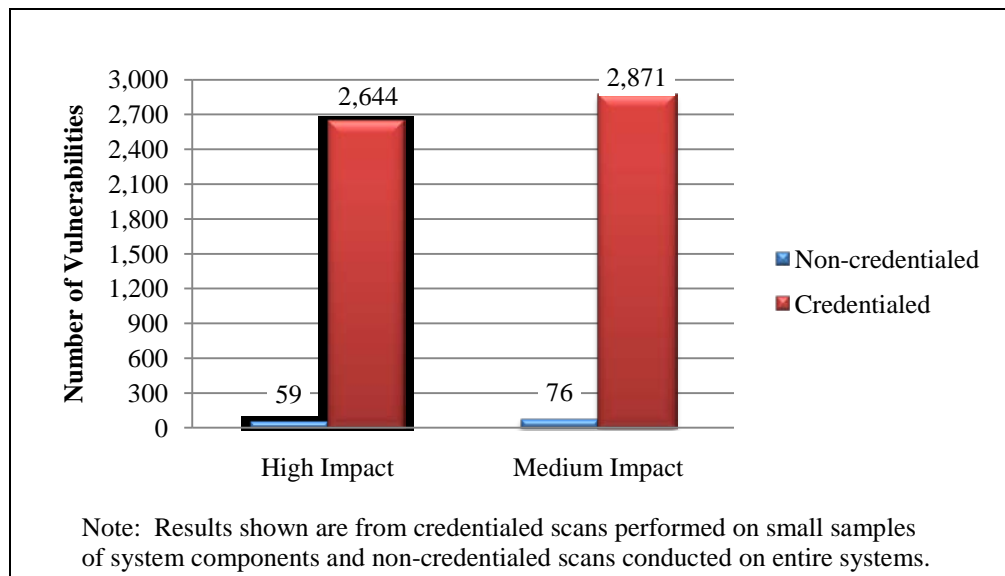
Of the 13 systems we selected for review, 7 were located at one Center. Our review of these systems revealed that 2 of the systems had not been undergoing continuous monitoring for high-impact vulnerabilities. Moreover, when we performed credentialed scans on the Center's systems rather than relying on the non-credentialed scans Center personnel had been performing, we identified a large number of high-impact vulnerabilities. This finding questions the efficacy of NASA's processes for identifying systems that should be subject to vulnerability management and the effectiveness of its vulnerability scanning.

While some systems we reviewed showed a stronger security posture than others, we did not find consistent practices in place across Centers. For example, one Center used credentialed scanning as part of the vulnerability monitoring process for one of its systems, and we found very few high-impact vulnerabilities for that system. Local personnel stated that transitioning from non-credentialed to credentialed scanning achieved notable results over a short period of time and that reportable security incidents had been significantly reduced.

We directed NASA personnel to perform credentialed scans on a small sample of system components and observed these scans. We compared the results of those scans with past,

non-credentialed scans performed by the Agency. As shown in Figure 3, although the credentialed scans were performed on only a small sample of system components, they identified 2,644 high-impact vulnerabilities compared with the 59 high-impact vulnerabilities identified by the non-credentialed scans.

**Figure 3. Vulnerabilities Found by Credentialed Versus Non-Credentialed Scans**



While we did not assess whether the identified vulnerabilities were exploitable, these results indicate that NASA's current vulnerability monitoring practices capture only a small fraction of the known, potentially high-impact vulnerabilities that reside in the Agency's systems.

NASA officials said using credential versus non-credentialed scans in a widely distributed environment is difficult due to the large numbers of credentials that must be managed. However, these unmitigated vulnerabilities increase the risk for loss of NASA's systems, data, and intellectual property. By decreasing the number of high-impact vulnerabilities and misconfigured components, NASA can reduce the avenues for cyber attacks, the number of actual attacks, and the resources needed to respond to those attacks. Therefore, in order for NASA to ensure that its continuous monitoring program is effective, the Agency needs to ensure that credentialed scanning is consistently used on all systems.

## Conclusion

We found that NASA faces significant challenges in transitioning to a continuous monitoring process for its IT systems and related components. Until NASA (1) develops

and maintains a complete record of IT components; (2) ensures that security configuration baselines are available, applied, and monitored for all applicable components; and (3) develops consistent credentialed vulnerability scanning processes for use Agency-wide, NASA cannot effectively transition from a system of isolated reviews to an enterprise-wide continuous monitoring program.

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

To strengthen existing policies, procedures, and continuous monitoring controls, we made the following recommendations.

### **Recommendation 1.** The Chief Information Officer should

- a. expedite development of content, metrics, and a monitoring capability for applying secure baseline configuration settings to applicable NASA IT components using NASA's most common attack vectors as a guide for prioritization, beginning with Windows server operating systems and their respective functionality (e.g., web server and file server).
- b. institute credentialed vulnerability scanning Agency-wide as part of its continuous monitoring program. Specifically,
  - (1) develop and disseminate to all affected personnel detailed operating procedures for credentialed vulnerability scanning;
  - (2) develop schedules for performing credentialed vulnerability scans; and
  - (3) require credentialed scans Agency-wide as part of its continuous monitoring program.
- c. verify that the security baselines are applied and that credentialed scans are being performed as directed.

**Management's Response.** NASA concurred with our recommendation, noting that applying and measuring security configuration baselines can improve the Agency's overall IT security posture. NASA tasked its Agency Security Configuration (ASCS) program to develop and manage security configuration baselines and measurement content for all applicable NASA IT components. In addition, NASA officials said they are developing a Windows Server 2008 security configuration baseline and plan to begin measuring compliance with this baseline on March 31, 2012. NASA also agrees that credentialed vulnerability scanning allows for improved awareness of system vulnerabilities. Accordingly, NASA said it plans to update its guidance to include a requirement for performing credentialed vulnerability scanning that will include detailed operating procedures. Finally, NASA plans to propose establishment of a compliance

verification capability within the NASA OCIO. NASA expects to complete all of these corrective actions by November 30, 2012.

**Evaluation of Management's Response.** NASA's planned corrective actions are responsive to our recommendations. We will close the recommendations upon verifying that NASA has completed these actions.

**Recommendation 2.** Associate Administrators for Mission Directorates and Center Chief Information Security Officers should ensure that

- a. OCIO-developed baseline security configurations are applied to their systems; until these baselines settings are made available, ensure the appropriate CIS benchmarks are applied to their system components and deviations from the benchmarks are documented.
- b. all system owners establish accounts within ITSEC-EDW and follow procedures set forth in NASA policies as they relate to ITSEC-EDW, vulnerability monitoring, and configuration security baselines.
- c. appropriate system data are included in ITSEC-EDW and validated on a semiannual schedule.
- d. systems undergo credentialed vulnerability scanning and data are integrated into ITSEC-EDW.

**Management's Response.** NASA concurred with our recommendation, stating that it is taking steps to ensure appropriate security baselines and benchmarks are applied to applicable Mission and Center IT components and that any deviations from the standards are documented. Additionally, NASA is deploying an enterprise-wide patch management and reporting tool for use by Mission Directorates and Centers. In cases where this tool will not be used, systems personnel will maintain documented justification in the form of an approved IT security waiver. In addition, Center CISOs and Mission Directorate Associate Administrators agree that by March 31, 2012, responsible parties will have accounts in and familiarize themselves with the functionality of ITSEC-EDW, and by June 30, 2012, will include the appropriate system information in ITSEC-EDW and coordinate with OCIO on developing a process for validating that data semiannually. NASA also stated that Centers and Mission Directorates have already begun utilizing credentialed scans and that OCIO plans to implement credentialed scanning on all systems that are capable of supporting unique scanning techniques by March 31, 2012. Finally, NASA plans to have vulnerability data from all Center and Mission Directorate systems that are scanned using McAfee Vulnerability Manager integrated into ITSEC-EDW by January 31, 2013. Vulnerability data from NASA systems being scanned with other tools will be integrated into ITSEC-EDW as soon as possible.

**Evaluation of Management's Response.** NASA's planned corrective actions are responsive to our recommendations. We will close the recommendations upon verifying that NASA has completed these actions.





## Scope and Methodology

We performed this audit from January through October 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We assessed NASA's progress in shifting toward a continuous monitoring approach to IT security by focusing on processes in place at four NASA Centers for three key elements: record of IT components, configuration management, and vulnerability monitoring. NIST Special Publication (SP) 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, defines requirements for control monitoring. In addition to NIST SP 800-53 and the OCIO's May 18, 2010, memorandum (Appendix C), we reviewed the following Federal and Agency criteria, policies, and procedures:

- NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010
- NIST SP 800-40, Version 2.0, "Creating a Patch and Vulnerability Management Program," November 2005
- NIST SP 800-128 (Initial Public Draft), "Guide for Security Configuration Management of Information Systems," March 2010
- NIST SP 800-137 (Initial Public Draft), "Information Security Continuous Monitoring for Federal Information Systems and Organizations," December 2010
- Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
- NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology (Revalidated with Change 1, May 19, 2011)"
- NITR 2810-12, "Continuous Monitoring," May 18, 2008 (expired May 18, 2011)

- NITR 2810-24, “NASA IT Device Vulnerability Management,” January 28, 2010 (expired May 16, 2011)
- IT Security Handbook (ITS-HBK) 2810.02-04, “Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments,” November 10, 2010
- ITS-HBK 2810.07-01, “Configuration Management,” May 2011
- NASA OCIO Memorandum, “Center for Internet Security (CIS) Consensus Benchmarks,” September 2, 2004
- NASA OCIO Memorandum, “Implementation of Center for Internet Security (CIS) Benchmarks,” June 29, 2005
- NASA OCIO Memorandum, “FY [Fiscal Year] 2007 and FY 2008 Patch Management and Security Configuration Metrics,” April 4, 2007
- NASA OCIO Memorandum, “Agency Security Configuration Standards: Federal Desktop Core Configurations,” November 15, 2007
- NASA OCIO Memorandum, “Supplemental FY08 Guidance for Agency Security Configurations Standards and FDCC Reporting,” February 20, 2008
- NASA OCIO Memorandum, “FY 2009 Scanning and Vulnerability Elimination or Mitigation,” February 6, 2009
- NASA OCIO Memorandum, “Fiscal Year 2011 (FY11) Continuous Monitoring and Reauthorization Activities,” January 11, 2011
- Johnson Space Center Chief Information Officer Memorandum, “[Johnson Space Center’s] FY11 Strategy for Vulnerability Scanning and Risk Mitigation,” January 21, 2011

We reviewed NASA policies and procedures to determine the roles, responsibilities, and procedures for including system components in ITSEC-EDW, applying configuration settings to system components, and vulnerability monitoring of NASA systems.

We interviewed system owners, system administrators, organization computer security Officials, and the Center IT Security Managers (now called CISOs) at the Centers we visited, as well as OCIO personnel, including AVAR project personnel, the Emerging Technology and Desktop Standards project manager, and the ASCS technical lead. We interviewed key personnel at the project and system level to determine their awareness of NASA guidance and the procedures that they follow for ensuring their components are included in ITSEC-EDW. To evaluate the comprehensiveness and accuracy of ITSEC-EDW, we compared the results of queries to that database with the results of our

review. We also discussed ITSEC-EDW functionality with the Agency Security Update Service project manager.

We evaluated processes and tools used at the Centers to monitor and report IT components, to maintain system and component configurations, and to detect and remediate vulnerabilities.

We judgmentally selected 13 systems to review from an Agency-wide, non-national security system inventory list maintained by the OCIO. As of November 2010, the inventory list identified 550 internal systems and 43 external (contractor) systems. We did not verify the accuracy of this list. We limited our selection to high- and moderate-impact systems at the four Centers visited. Of the 13 systems originally selected, we excluded 1 from our review because it was not connected to any other Agency network.

For each system that we reviewed, we assessed whether component samples reflected appropriate baseline security configurations, reviewed configuration documentation, and observed credentialed scans for vulnerabilities. We also judgmentally selected a sample of components connected to each system to query for information in ITSEC-EDW. We compared the results of the queries to data collected in configuration assessments and vulnerability scans.

**Computer-Processed Data.** We relied on data produced by a commercial software program to perform configuration tests on NASA's computer servers. Specifically, we used the CIS CAT to assess computer server operating system compliance with the applicable CIS benchmarks. We did not validate the data produced by the CIS CAT because this tool is widely accepted as a reliable source for providing information on operating system configuration settings. However, due to the wide variance in compliance scores, we evaluated the tool and found limitations, as discussed in the report.

We directed and observed the use of McAfee Foundstone Enterprise, a commercial vulnerability scanner, to test system components for technical vulnerabilities. We did not validate the data produced by Foundstone Enterprise because it is widely accepted as a reliable source for providing information related to the presence of technical vulnerabilities in information systems.

## Review of Internal Controls

We identified and evaluated the effectiveness of internal controls in place to manage configurations and continuously monitor systems and components. The control weaknesses we identified are discussed in the Results section of this report. Our recommendations, if implemented, will help to correct the identified control weaknesses.

## Prior Coverage

During the last 5 years, the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) have issued three reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at <http://oig.nasa.gov/audits/reports/FY11> (NASA OIG) and <http://www.gao.gov> (GAO).

### NASA Office of Inspector General

“Federal Information Security Management Act: Fiscal Year 2010 Report from the Office of Inspector General” (IG-11-005, November 10, 2010)

“Audit of NASA’s Efforts to Continuously Monitor Critical Information Technology Security Controls” (IG-10-019, September 14, 2010)

### Government Accountability Office

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

---

---

## GLOSSARY

---

**Center Chief Information Security Officer (CISO):** CISOs serve as advisors to the Senior Agency Information Security Officer, Center CIO, and senior Center officials on matters pertaining to information security. This role was previously referred to as the Information Technology Security Manager.

**Center for Internet Security (CIS):** The CIS is a not-for-profit organization that serves as a central resource to improve cybersecurity posture. The CIS Security Benchmarks division improves organizations' security posture by helping reduce the risk of inadequate technical security controls.

**Certification and Accreditation (C&A):** Certification is the comprehensive evaluation of security features of a system, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements. Accreditation is the process by which certification is reviewed and a formal declaration made that a system is approved to operate.

**Configuration Baseline Settings:** Security baseline configurations should conform to applicable Federal requirements (e.g., FDCC and USGCB). USGCB security configuration checklists (for Windows XP, Windows Vista, and Internet Explorer 7) support the FDCC policy, and the USGCB checklists address a wide variety of security and non-security settings that are largely based on the recommendations of product vendors but customized to meet Federal requirements. The USGCB checklists are referred to as baselines because they define minimum sets of configurations that must be implemented.

**Continuous Monitoring:** Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The objective is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.

**Credentialed Vulnerability Scans:** A scanning engine uses credentials to login to the system to enumerate services, applications, and patches. The information obtained by using credentials during a vulnerability scan allows administrators to perform a more comprehensive assessment of the security posture of their system, verify the performance of their patching mechanisms, check service configurations, and discover erroneously or maliciously installed services.

**Federal Desktop Core Configuration (FDCC):** FDCC is a security configuration mandated by OMB. FDCC currently exists for Microsoft Windows XP and Vista operating system software.

**Foundstone Enterprise:** See McAfee Vulnerability Manager.

**Incident:** Any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality.

**Information Technology (IT):** The term "information technology" means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.

**Information Technology Security – Enterprise Data Warehouse (ITSEC-EDW):** ITSEC-EDW is intended to serve as an automated data warehouse providing an inventory of NASA IT components and related security information. It will include consolidated patch statistics, vulnerability scan results and hardware and software identification data.

**Linux:** Unix-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive Unix systems. Linux has a reputation as a very efficient and fast-performing system.

**Malware:** Also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

**McAfee Vulnerability Manager:** Formerly known as Foundstone Enterprise, the McAfee Vulnerability Manager finds and prioritizes vulnerabilities and policy violations on a network.

**Patch:** An additional piece of code developed to address a problem in an existing piece of software.

**Patch Agent:** A commercially available automated inventory management tool that monitors changes in the computer's configuration and reports to a central database, thereby providing the patch and vulnerability group and management a picture of a system's IT resources.

**Patch Management:** The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.

**Risk Management:** The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the

operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal approval to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, and regulations.

**Security Authorization:** The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

**Security Controls:** The management, operational, and technical controls (e.g., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

**Security Posture:** The overall state of an information system's confidentiality, integrity, and availability in the face of an ever-changing risk landscape.

**Unix:** Unix is a multi-user environment that has been implemented on a variety of platforms. With the exception of Microsoft Windows, all current major operating systems have some kind of Unix at their cores. Unix is not so much a single operating system as it is a standard upon which organizations and companies base their own systems.

**Virus:** A program designed with malicious intent that has the ability to spread to multiple computers or programs. Most viruses have a trigger mechanism that defines the conditions under which it will spread and deliver a malicious payload of some type.

**Vulnerability:** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

**Vulnerability Management:** The process of managing the weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Vulnerability Scanning:** An assessment technique used to identify hosts/host attributes and associated vulnerabilities.

---

---

## NASA OCIO MEMORANDUM

---

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



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

MAY 18 2010

TO: Distribution

FROM: Deputy Chief Information Officer for IT Security

SUBJECT: Suspension of Certification and Accreditation Activity

This memorandum is for wide distribution. For maximum effectiveness, it is critical that this guidance be distributed to all Information System Security Officials, Information System Owners, Authorizing Officials, managers and operators across all IT domains to include both corporate and mission IT environments, whenever and wherever feasible.

On April 21, 2010, The Office of Management and Budget (OMB) issued memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The reporting instructions for FY10 significantly change the way federal agencies assess the security posture of their information systems. The memo is clear regarding a shift away from cumbersome and expensive C&A paperwork processes, in favor of a value-driven, risk-based approach to system security.

Per M-10-15, NIST recommendations inherently "allow agencies latitude in their application [of security solutions...]. Consequently, the application of NIST guidelines by agencies can result in different security solutions that are equally acceptable and compliant." As such, the ITSD is creating a more streamlined system security authorization process with a focus on continuous monitoring, automated tools, and significant paperwork reduction. These developing processes will eventually enable near real-time risk management and ongoing security authorizations that reflect the true intent of NIST guidance, and fall in line with the objectives of DHS, DOJ, the Whitehouse, recently proposed amendments to federal security legislation, and new OMB mandated tools.

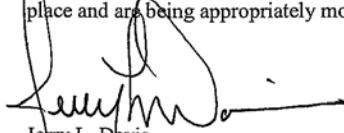
To guide NASA through this strategic transitional period, the IT Security Division (ITSD) within the NASA Office of the Chief Information Officer (OCIO) is issuing the following:

- The OCIO will not require Information System Owners (ISO) to recertify their systems in FY 2010 to satisfy OMB requirements.
- In lieu of C&A activities in FY 2010, AOs must extend current Authorizations to Operate (ATO) for a period not to exceed one year from the date of their system's current ATO expiration, using form NF1740 (see attached sample with appropriate extension conditions).



- Updated ATO expiration dates should be reported to OCIO via normal ITS monthly reporting activities.
- At the discretion of the Authorizing Official (AO), for systems under their cognizant authority, an ATO may still be obtained through existing NASA C&A processes; however, these processes have proven largely ineffective and do not ensure a system's security, or a true understanding of the system's risk posture.
- All new systems (internal and external) will adhere to the current NASA C&A processes to obtain an initial ATO until a more effective security authorization process is established. However, as always intended, the focus of new ATOs should be a near real-time understanding of risk posture, and not the production of paperwork.

Nothing in this memo relieves system owners and operators from exercising due diligence and care in ensuring that information systems under their authority have adequate security controls in place and are being appropriately monitored.



Jerry L. Davis

Enclosure

Distribution:

ITSM

ARC/Mr. Ernest Lopez  
DFRC/Mr. Anthony Thomas  
GRC/Mr. Les Farkas  
GSFC/Mr. Joshua Krage  
HQ/Mr. Greg Kerr  
JPL/Mr. Jay Brar  
JSC/Mr. Ted Dyson  
KSC/Mr. Henry Yu  
LaRC/Mr. Kendall Freeman  
MSFC/Mr. David Black  
NSSC/Mr. Dave Epperson  
SSC/Mr. Monti Muhsin

Center CIOs

ARC/J. Williams (Acting)

DFRC/R. Binkley

GRC/S. Pillay

GSFC/A. Gardner

HQ/K. Carter

JPL/J. Rinaldi

JSC/L. Sweet

KSC/M. Bolger

LaRC/C. Mangum

MSFC/J. Pettus

NSSC/B. O'Dell

SSC/D. Cottrell

Mission Directorates

Aeronautics Research/P. Milstead

Exploration Systems/B. Hamilton

Science/J. Bredekamp

Space Operations/S. Goodwin



## IT System Authorization to Operate (ATO)

TO: <SYSTEM OWNER NAME>, Information System Owner

FROM: <AUTHORIZING OFFICIAL NAME>, Authorizing Official

SUBJECT: Security authorization Decision for <NASA SYSTEM NAME>

After reviewing the results of the security assessment of <NASA System Name> and its constituent system-level components, managed by HQ, and the supporting evidence provided in the associated security authorization package, I have determined that the risk to Agency operations, Agency assets, or individuals resulting from the operation of the information system is FULLY ACCEPTABLE.

Accordingly, I am issuing AN ATO WITHOUT ANY SIGNIFICANT RESTRICTIONS OR LIMITATIONS. This security authorization is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security authorization of this information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office once every year (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security authorizations in accordance with Federal or Agency policy.

A copy of this form with all supporting security assessment and authorization documentation must be retained in accordance with the Agency's record retention schedule, as well as posted in the NASA System Security Plan Repository.

Conditions to obtain an ATO are shown below or on a separate document.

**CONDITIONS**  
Per Agency OCIO guidance, this document extends the current authorization to operate (ATO) one year from the date of expiration. It is the expectation of the authorizing official that the system owner will continue to practice due diligence in ensuring the security posture of the information system. This ATO will expire <Insert Current Expiration Date + 1 Year>.

<Authorizing Official Name>	<Authorizing Official Title>	HQ	
AUTHORIZING OFFICIAL NAME	TITLE	ORG CODE	CENTER

SIGNATURE - DATE

NASA FORM 1740 APR 10 PREVIOUS EDITIONS ARE OBSOLETE

---

---

## MANAGEMENT COMMENTS

---

National Aeronautics and  
Space Administration  
**Office of the Administrator**  
Washington, DC 20546-0001



Office of the Chief Information Officer

NOV 29 2011

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Response to OIG Draft Audit Report, "NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems" (Assignment No. A-11-003-00)

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to review your draft audit report entitled "NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems" (Assignment No. A-11-003-00).

In the draft report, the Office of the Inspector General (OIG) outlines several findings and communicates two recommendations. NASA's response to the recommendations, including planned corrective actions, follows:

**Recommendation 1:** The CIO should:

- a. Expedite development of content, metrics, and a monitoring capability for applying secure baseline configuration settings to applicable NASA IT components using NASA's most common attack vectors as a guide for prioritization, beginning with Windows server operating systems and their respective functionality (e.g., web server and file server).
- b. Institute credentialed vulnerability scanning Agency-wide as part of its continuous monitoring program. Specifically:
  - (1) Develop and disseminate to all affected personnel detailed operating procedures for credentialed vulnerability scanning;
  - (2) Develop schedules for performing credentialed vulnerability scans; and
  - (3) Require credentialed scans Agency-wide as part of its continuous monitoring program.

- c. Verify that the security baselines are applied and that credentialed scans are being performed as directed.

**Management's Response:** NASA concurs with the recommendation.

- a. NASA agrees that developing, applying and measuring security configuration baselines can improve overall system security by ensuring that all information systems are configured with the most secure settings possible. To that end, NASA has tasked the Agency Security Configuration Settings (ASCS) program to develop and manage security configuration baselines and measurement content for all applicable NASA Information Technology (IT) components. NASA has also purchased and deployed the Dell KACE patch and configuration management tool, which can measure compliance with security configuration baselines for many of NASA's operating systems. NASA plans to complete development of a Windows Server 2008 security configuration baseline, and begin regular compliance measurement against this baseline, by March 31, 2012.
- b. Because credentialed vulnerability scanning can detect additional vulnerabilities on NASA's IT assets, NASA has instituted credentialed vulnerability scanning as a vital part of its continuous monitoring program. NASA's IT security handbook on Risk Assessment (ITS-HBK-2810.04-01), dated May 6, 2011, requires vulnerability scanning of all devices on NASA non-guest networks, addressing part 1.b.(3) of the recommendation. This policy requires at least quarterly scanning of all devices, addressing part 1.b.(2) of the recommendation. NASA's IT security handbook regarding continuous monitoring expires in November 2012. When NASA updates this policy, it will ensure that credentialed vulnerability scanning is part of the required approach and that detailed operating procedures for credentialed vulnerability scanning are included.
- c. In order to ensure that security configuration baselines are applied and that credentialed scans are being performed, NASA agrees that oversight and verification are necessary. OCIO will propose the establishment of an IT Security program management office capability within the OCIO's IT Security Division, with verification of security compliance as one of its core functions.

NASA has already completed many of the actions needed to address recommendation 1. The Agency plans to complete the remaining corrective actions by November 30, 2012, contingent upon sufficient funding in Fiscal Year 2012 and the out years.

**Recommendation 2:** Associate Administrators for Mission Directorates and Center Chief Information Security Officers should ensure that:

- a. OCIO-developed baseline security configurations are applied to their systems; until these baselines settings are made available, ensure the appropriate CIS benchmarks are applied to their system components and deviations from the benchmarks are documented.

- b. All system owners establish accounts within ITSEC-EDW and follow procedures set forth in NASA policies as they relate to ITSEC-EDW, vulnerability monitoring, and configuration security baselines.
- c. Appropriate system data are included in ITSEC-EDW and validated on a semiannual schedule.
- d. Systems undergo credentialed vulnerability scanning and data are integrated into ITSEC-EDW.

**Management's Response:** NASA concurs with the recommendation. While NASA strongly agrees with the intent of the OIG's recommendation to strengthen existing policies, procedures and continuous monitoring controls, some aspects of this recommendation are not practicable due to NASA's current resource constraints or other technical considerations. Additional details are provided below.

- a. NASA Mission Directorates and Centers are already working to ensure that NASA security configuration baselines, such as the Federal Desktop Core Configuration (FDCC) and the US Government Configuration Baseline (USGCB), are applied to their applicable systems; that the appropriate Center for Internet Security (CIS) benchmarks are applied as needed; and that deviations from the benchmarks are documented. Mission Directorates and Centers utilize the Agency patch management and reporting tool (Dell KACE), where possible, to verify that security baselines are applied. They will continue to deploy this tool across their applicable information systems, including mission systems, and will obtain waivers when the tool cannot be deployed. The Dell KACE tool will be supplemented by configuration management tools provided by the new Agency Consolidated End-user Services (ACES) provider by June 30, 2012. However, as previously noted by NASA and acknowledged by OIG auditors, CIS benchmarks do not lend themselves to automated deployment or verification on an enterprise-wide or even Center-wide scale. While Mission Directorate AAs and Center CISOs will continue to work with system owners to ensure that the requirements for applying CIS benchmarks are understood and met, true enterprise verification of compliance is not possible with available tools and resources. Therefore, Mission Directorates and Centers will use automated methods to apply security configurations baselines, such as for Windows servers, as they become available.
- b. The Mission Directorate AAs and Center CISOs agree that those responsible for the security posture of NASA's information systems should have accounts in IT Security Enterprise Data Warehouse (ITSEC-EDW) and should use all information available for managing the risks to their systems. While the information system owner (ISO) may not always be the person most directly involved in managing system security, the Mission Directorate AAs and Center CISOs will ensure that, for each NASA information system, at least one person responsible for system security, such as the ISO, information system security official, or system administrator, establishes an

account in ITSEC-EDW and that personnel are familiar with the reports and information available, by March 31, 2012.

- c. The Mission Directorate AAs and Center CISOs strongly support the goal of ensuring that all appropriate system data is included and validated in NASA's security inventory, regardless of how this inventory is implemented. They will continue to take the following actions: working with Center organizations to ensure that the necessary data is provided, deploying the Dell KACE agent on as many devices as possible, working with OCIO to integrate data from additional vulnerability scanning tools into ITSEC-EDW so that information from all scans can be captured, and coordinating with the ACES and NASA Integrated Communications Services (NICS) providers to ensure that data from their automated management tools is integrated into ITSEC-EDW. Comparison with data from ACES and NICS management tools will also aid in the validation of NASA's security inventory data. Semiannual validation of all data in ITSEC-EDW is not practicable as recommended, given that the database currently contains detailed information on approximately 130,000 devices. Nevertheless, the Mission Directorates and Centers will work with OCIO to develop a semiannual process, by June 30, 2012, to validate that data is being accurately submitted into ITSEC-EDW and that devices are associated with the appropriate System Security Plan.
- d. Since NASA instituted the requirement for quarterly credentialed vulnerability scanning in May 2011, Centers and Mission Directorates have already begun utilizing credentialed scanning as part of their continuous monitoring program. Implementation of full credentialed scanning across the Agency is hampered by a lack of automated credential management for all NASA devices; insufficient resources to accomplish the increased management of scanning, to handle a higher number of false positives and to manually manage scanning credentials on some systems; the potential of credentialed scanning to negatively impact critical system performance; and, in some cases, transitions of the contracts providing IT infrastructure or IT security services. Given these limitations, NASA Centers and Mission Directorates plan to institute credentialed vulnerability scanning of all systems that are capable of supporting unique scanning credentials and whose credentials are managed through Active Directory by March 31, 2012. Credentialed scanning of the remaining systems is being accomplished as resources permit, prioritized by the sensitivity and risk level of each system and the feasibility of performing a credentialed vulnerability scan. NASA Centers and Mission Directorates will ensure that data from all credentialed scans performed using the Agency vulnerability scanning tool (McAfee Vulnerability Manager, or Foundstone) is integrated into ITSEC-EDW by January 31, 2012. For any other scanning tools used for credentialed vulnerability scanning, the Centers and Mission Directorates will work with OCIO to ensure that data from these tools is integrated into ITSEC-EDW as soon as possible.

NASA plans to complete all the actions to address recommendation 2 by June 30, 2012.

5

As requested, we have reviewed the report to identify any information that we believe should not be publicly released. After coordinating with your office we believe the OIG has removed any sensitive information from this report.

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

  
Linda Y. Cureton



---

---

## REPORT DISTRIBUTION

---

### **National Aeronautics and Space Administration**

Administrator  
Deputy Administrator  
Chief of Staff  
Chief Information Officer  
Associate Administrator for Aeronautics Research  
Associate Administrator for Exploration Systems  
Associate Administrator for Science  
Associate Administrator for Space Operations  
NASA Advisory Council's Audit, Finance, and Analysis Committee  
Director, Ames Research Center  
Director, Dryden Flight Research Center  
Director, Glenn Research Center  
Director, Goddard  
    Manager, White Sands Test Facility  
Director, Jet Propulsion Laboratory  
Director, Johnson Space Center  
Director, Kennedy Space Center  
Director, Langley Research Center  
Director, Marshall Space Flight Center  
Director, Stennis Space Center  
Executive Director, NASA Shared Services 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 Organization, Efficiency, and Financial Management

House Committee on Science, Space, 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

Chris Reeves, Audit Lead

Bessie Cox, Auditor

Bret Skalsky, Auditor



OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit <http://oig.nasa.gov/audits/reports/FY12/> to obtain additional copies of this report, or contact the Assistant Inspector General for Audits at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Mr. Laurence Hawkins, Audit Operations and Quality Assurance Director, at [Laurence.B.Hawkins@nasa.gov](mailto: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.