U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Investigations & Oversight

HEARING CHARTER

NASA Cybersecurity: An Examination of the Agency's Information Security

Wednesday, February 29, 2012
2:00 p.m. – 4:00 p.m.
2318 Rayburn House Office Building

Purpose

The Subcommittee on Investigations and Oversight meets on February 29, 2012 to examine the state of information security at the National Aeronautics and Space Administration (NASA). The hearing will also examine recent NASA Office of the Inspector General (IG) reports concerning information security, the steps NASA is taking to address the recommendations contained in those reports, and discuss future challenges to the Agency's information security posture.

Background

NASA relies on information technology (IT) systems and networks to control spacecraft like the International Space Station, conduct science missions using orbiting satellites like the Hubble Space Telescope, as well as for common institutional needs like email and data sharing. The threat of cyber attack to agency satellite operations, mission support, and technology research is increasing in sophistication and frequency.

NASA supports IT networks at 16 different centers and facilities, employing 58,000 desktop computers, 44 data centers, and 23,582 servers.[1] These, as well as NASA's headquarters information activities, are managed by NASA's Chief Information Officer (CIO). Additionally, NASA manages approximately 3,300 websites, which represent roughly half of all civil government websites, and over 130,000 unique internet protocol (IP) addresses.[2] The sheer scope of the domains linked to the Agency's various networks provides numerous opportunities or "gates" and points of entry for unauthorized access to sensitive information and technology.

For a number of reasons, NASA is a high-priority target for criminals and state-level actors attempting to steal, compromise, or corrupt technical data. Because of NASA's stature as an Agency on the vanguard of technological progress, the tampering or corruption of scientific data from unauthorized intruders is a serious concern. In 2009 and 2010, NASA reported 5,621 computer security incidents that resulted in the installation of malicious software on Agency

[1] "NASA Cyber Security," Briefing from the NASA Office of the Chief Information Officer to the House Science, Space, and Technology Committee Staff, February 2012.
[2] *Ibid.*

systems or unauthorized access to its computers.[3] Even more concerning is the fact that NASA technology is inherently dual-use in nature, meaning many of the civilian-use applications could also be used for military purposes. If compromised, NASA technology could present significant nonproliferation concerns.

NASA's satellite Tracking, Telemetry, and Command (TT&C) operations are also not immune to malicious and unauthorized intrusions. In fact, NASA's Earth observation satellites have been targeted in the past. The recent US-China Economic and Security Commission report to Congress in 2011 stated:

> "The National Aeronautics and Space Administration confirmed two suspicious events related to the Terra EOS satellite in 2008 and the U.S. Geological Survey confirmed two anomalous events related to the Landsat-7 satellite in 2007 and 2008."[4]

Additionally, NASA's unique supercomputing capabilities also make it an attractive target. In 2009, a Swedish national was indicted for system intrusions at the Ames Research Center and the NASA Advanced Supercomputing Division that resulted in $1 million in supercomputing "downtime."[5] Although the hacker, a minor at the time, was never extradited, he was found guilty in Sweden for a variety of similar offenses.[6]

Office of the Chief Information Officer Structure

The NASA Headquarters (HQ) CIO is ultimately the official responsible for managing the agency's IT systems and developing future IT architectures that incorporate new technology. As previously mentioned, NASA maintains separate CIOs at each of the NASA Centers and Mission Directorates. NASA recently reorganized, making individual Centers' CIOs accountable to the CIO at Headquarters.

The Office of the CIO is organized into four divisions that manage different aspects of the agency's IT infrastructure, needs, technology infusion and security.

1. The Capital Planning & Governance Division is the central policy and business management division responsible for the development and compliance of uniform IT management standards and guidelines.
2. The Technology and Innovation Division identifies emerging IT technologies and conducts advanced planning for technology infusion that can best support NASA's missions.

---

[3] "2011 Report on NASA's Top Management and Performance Challenges," NASA OIG, November 15, 2011, available at: http://oig.nasa.gov/NASA2011ManagementChallenges.pdf

[4] "2011 Report to Congress of the U.S.-China Economic and Security Review Commission," November 16, 2011, available at: http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf

[5] Indictment, United States v. Pettersson, No. 09-0471 (N.D. Cal. May 5, 2009), available at http://www.wired.com/images_blogs/threatlevel/2009/05/petterssonindictment.pdf

[6] Letter from Hon. Paul Martin, Inspector General, NASA, to Rep. Paul Broun, Chairman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives, January 25, 2012, available at: http://oig.nasa.gov/audits/reports/FY12/Export_Control_Letter%281-25-12%29.pdf

3. The Enterprise Service & Integration Division implements the NASA Enterprise Architecture and its elements such as networks, data centers, desktop computers and email.
4. The NASA IT Security (ITS) Division manages Agency-wide security projects to correct known vulnerabilities, reduce barriers to cross-Center collaboration, and provide cost-effective IT security services. The ITS Division ensures that information technology security across NASA meets confidentiality, integrity, and availability objectives for data and information. ITS develops and maintains an information security program that ensures consistent security policy, indentifies and implements risk-based security controls, and tracks security metrics to gauge compliance and effectiveness. The division is responsible for performing audits and reviews to assess compliance with security and privacy policies and procedures such as NPD 2810.1, NASA Information Security Policy, and NPR 2810.1 Security of Information Technology.[7]

Security Operation Center

The Security Operations Center (SOC) detects and monitors security incidents on the institutional IT systems and networks along with the Computer Forensics and Incident Analysis (CFIA) team and the Cyber Threat Analysis Program (CTAP). The SOC also performs testing to determine IT security weaknesses within the agency's networks. Because the SOC has limited insight into Mission Directorate intrusions, the CIO creates Tiger Teams to focus on specific problems and incidents within the Mission Directorates. The Tiger Teams coordinate with the SOC, as well as the NASA IG, when responding to IT security incidences.

Programs

The I3P (Information Technology Infrastructure Integration Program) is designed to help the CIO better manage the IT needs of the Agency by transferring NASA's IT infrastructure services from a Center-based model to an enterprise-based management and provisioning model. The program is executed by the following contracts.

Contract	Description	Contractor
ACES (Agency Consolidated End-user Services)	Provides a "consolidated solution for delivering end-user services across the Agency to achieve increased efficiencies and reduced costs though standardization and commonality while providing means to build specialized solutions when mission needs require them. Services provided include computing and mobile bundled seats, Enterprise-wide email, directory and printing services, and peripherals."[8]	Hewlett-Packard
EAST (Enterprise Applications Service Technologies)	Provides "all services in support of the NASA Enterprise Applications Competency Center."[9]	SAIC
NICS (NASA Integrated Communications Services)	Provides "managerial and technical expertise to support NASA's Office of the Chief Information Officer for corporate and mission communications needs, including local area network management at all NASA centers. Functions include corporate and mission enterprise	SAIC

[7] "Information Technology Infrastructure Integration Program Acquisitions," NASA, available at: http://i3p.nasa.gov/
[8] *Ibid.*
[9] *Ibid.*

	services; center and associated component facility services; infrastructure projects; and contract management services."[10]	
WESTPRIME (Web Enterprises Services and Technology)	Provides NASA "with an agency-wide capability to create maintain and manage web sites and associated ancillary services."[11]	RFI posted February 6, 2012.
NEDC (NASA Enterprise Data Center)	"[I]ntended to consolidate and transform data centers' services, both at the NASA installation level and Agency-wide, to reduce duplicative cost, implement consistent operation procedures and processes, and provide NASA's end users seamless and consistent data center services to support mission success."[12]	Program cancelled in early 2011.

NASA Office of the Inspector General

The NASA IG conducts independent oversight, audits, reviews and investigations of NASA programs and operations. The CIO and the IG work closely on IT security, as both offices exchange timely information and data when assessing Agency vulnerabilities and investigating agency intrusions.

The NASA IG has conducted a number of audits since 2007 (see Appendix 1 for open recommendations) concerning NASA's IT security and released three reports in 2011 with specific recommendations for improving the security posture of the Agency. These reports include:

- *Inadequate Security Practices Expose Key NASA Network to Cyber Attack* (Report No. IG-11-017, March 28, 2011)
    - The NASA IG recommended that NASA, "(1) immediately identify Internet-accessible computers on its mission networks and take prompt action to mitigate identified risks; (2) continuously monitor Agency mission networks for Internet-accessible computers and take prompt action to mitigate identified risks; and (3) conduct an Agency-wide IT security risk assessment."

- *Federal Information Security Management Act: Fiscal Year 2011 Evaluation,* Annual Report (IG-12-002, October 17, 2011)
    - The NASA IG "found that the Agency's programs for risk management, configuration monitoring management, and Plan of Action and Milestones (POA&M) need significant improvements as they do not include all required attributes identified by the Department of Homeland Security."

- *NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems* (Report No. IG-12-006, December 5, 2011)
    - The NASA IG indicated that "NASA needs to (1) create and maintain a complete, up-to-date record of IT components connected to Agency networks; (2) define the

[10] *Ibid.*
[11] *Ibid.*
[12] *Ibid.*

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."

The NASA IG reports also include numerous examples of IT security incidents that help to better illustrate and characterize the seriousness of the incidents:

- "[I]n May 2009 NASA notified the Office of Inspector General (OIG) of a suspicious computer connection from a system that supports Agency space operations and space exploration activities. The subsequent OIG investigation confirmed that cybercriminals had infected a computer system that supports one of NASA's mission networks. Due to the inadequate security configurations on the system, the infection caused the computer system to make over 3,000 unauthorized connections to domestic and international Internet protocol (IP) addresses including addresses in China, the Netherlands, Saudi Arabia, and Estonia."[13]
- "In another cyber attack in January 2009, cybercriminals stole 22 gigabytes of export-restricted data from a Jet Propulsion Laboratory (JPL) computer system. The sophistication of both of these Internet-based intrusions confirms that they were focused and sustained efforts to target assets on NASA's mission computer networks."[14]
- "[T]he Agency is vulnerable to computer incidents that could have a **severe or even catastrophic effect** on Agency assets and operations."[15] [emphasis added]
- "[The NASA IG] found that six computer servers associated with IT assets that control NASA spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable."[16]

Because of these outstanding issues, the 2011 NASA IG report on NASA's Top Management and Performance Challenges stated that information technology security and governance remains one of five top Agency challenges.

Issues

Governance

While the CIO is tasked with delivering secure information technology services for the entire Agency, the office only has budgetary and management control of institutional and center services, not Mission Directorates, programs, projects, or contractors. The budgets, staffing, and requirements for information security within these areas are maintained and controlled by the respective mission directorates and programs.[17] Additionally, the CIO has very little insight into the development of project requirements or the negotiation of contracts, areas where insight is

[13] "Inadequate Security Practices Expose Key NASA Network to Cyber Attack," NASA OIG, (IG-11-017), March 28, 2011, available at: http://oig.nasa.gov/audits/reports/FY11/IG-11-017.pdf
[14] *Ibid*.
[15] See *Supra* note 2
[16] *Ibid*
[17] Note: The NASA CIO does have insight into the development of standards through NASA Policy Directives (NPD); NASA Procedural Requirements (NPR); NASA Interim Directives (NID); NASA Interim Technical Requirements (NITR); the IT Security Handbooks (ITS-HBK); as well as other standards and memoranda associated with IT security.

crucial to ensuring agency-wide information security. In circumstances like this, the CIO is charged and accountable for ensuring information security, but perhaps not empowered to accomplish this directive.

In testimony before the U.S. House Appropriations Subcommittee on Commerce, Justice, Science and Related Agencies on February 10, 2011, NASA Inspector General Paul Martin stated, "until the Mission Directorates fully implement NASA's IT security programs, the Agency will be at risk for security incidents that can have a severe adverse effect on Agency operations and assets."[18]

One of the main challenges with expanding the CIO's authority is that the Mission Directorates and programs are ultimately responsible for mission assurance, and mission-specific information security expertise usually resides within the Mission Directorates and programs. Before handing over or entrusting control of mission-critical elements, Mission Directorates, programs, and projects will need to be assured that information integrity and security will be equal to, if not greater than, that which is already provided.

Collaboration vs. Security

Another challenge with expanding the CIO's authority is the existence of vast cultural differences within NASA. Not only do individual Centers have unique characteristics, procedures, and standards, individual Mission Directorates also have distinct priorities that make a "one size fits all" approach challenging. For example, the Human Exploration and Operations Mission Directorate is primarily concerned with mission assurance, operational security, and nonproliferation which results in information security practices that limit the release of information. The Science Mission Directorate on the other hand, is tasked with sharing information in a collaborative fashion that is typical of the scientific community. While data integrity issues are still a concern, the directorate weighs those concerns with that of collaboration and transparency. Further, the Aeronautics Research Mission Directorate's priorities span both the Science and Human Exploration and Operations Mission Directorate's concerns, but are even more confounded by undefined and often contradictory practices.

Primary Outstanding NASA IG Recommendations

NASA has agreed with many of the NASA IG findings related to information security, and has endeavored to implement the related recommendations contained in those reports. Despite this, a number of key recommendations remain outstanding, particularly the recommendations to develop an Agency-wide risk assessment and mitigation strategy.[19] The original timeline for completing these reviews was August of 2011, but was eventually extended to February 2012. The estimated close-out of these two recommendations is now later this Spring. Aside from the fundamental tasks of determining an Agency-wide risk assessment, and mitigation strategy, the NASA IG has also recommended that the Agency conduct continuous monitoring.

[18] "Major Challenges Facing NASA in 2011," testimony of Hon. Paul Martin, NASA IG, "Oversight Hearing on the National Science Foundation and the National Aeronautics and Space Administration - Inspector Generals," House Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies, February 10, 2011, available at: http://oig.nasa.gov/NASA2011MajorChallenges.pdf

[19] See *Supra* note 11

Persistent Challenges

These challenges are not new. At a hearing in 2003, the previous NASA IG testified that "The Centers have diverse roles and historical cultures and, over time, have had substantial operational freedom in fulfilling mission objectives. NASA, like every other agency, faces a challenge in convincing its workforce that IT security is a primary rather than secondary responsibility."[20] Much of what the IG testified to almost ten years ago is still applicable today:

> "The environment in which NASA IT systems operate provides a context and setting for understanding NASA's IT security challenges. The elements of this environment include:
>
> - NASA has hundreds of programs requiring unique IT solutions.
> - NASA's information security program is reliant on the judgment of all persons with access to sensitive information.
> - NASA has a responsibility to protect varied types of sensitive and classified information.
> - NASA carries out a civilian mission for which distribution of information about scientific exploration, discovery, and achievement is practiced by the Agency and expected and desired by the public.
> - Contractors receive 90 percent of NASA dollars.
> - NASA is a highly visible Agency with many readily available Web sites, making it a natural target for those seeking to illegally access Government systems.
> - NASA scientists and engineers focus on meeting specific program objectives and may not give sufficient attention to the IT security environment.
> - NASA scientists and engineers often work in "open" educational environments with university scientists where "closed" information systems are an anathema.
> - NASA maintains many institutional and mission-critical information systems for which security is critical in carrying out NASA programs and operation"[21]

Witnesses

The Subcommittee will hear from two witnesses:

- Ms. Linda Y. Cureton, Chief Information Officer, NASA
- The Honorable Paul K. Martin, Inspector General, NASA

[20] Statement of Hon. Robert Cobb, NASA IG, Hearing on "Cyber Security: The Status of Information Security and the Effects of the Federal Information Security Management Act at Federal Agencies, House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, June 24, 2003, available at: http://www.access.gpo.gov/congress/house/pdf/108hrg/91648.pdf

[21] *Ibid*.

Appendix 1.

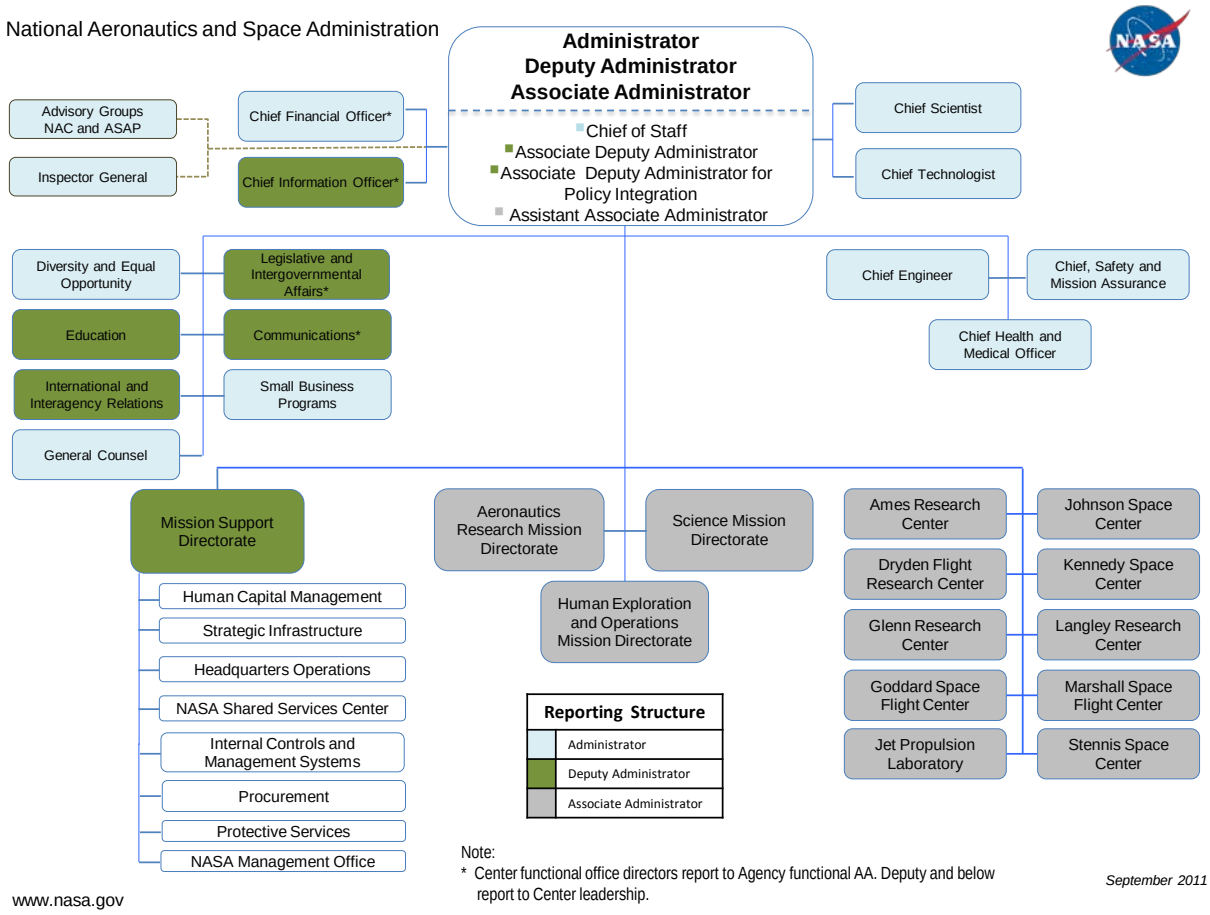
NASA OIG Information Technology Directorate
Open Recommendations for Audit Reports Issued (2006-2011)

Report No.	Final Issued	Report Title	Rec No.	Recommendation	Rec Type	Mgt Estimated Completion
IG07014	6/19/2007	Controls over the Detection, Response, and Reporting of Network Security Incidents Needed Improvement at the Four NASA Centers Reviewed (Sensitive But Unclassified)	1	The ARC CIO should adopt the controls outlined in NIST SP 800-53 by placing incident detection sensors as appropriate in order to monitor all NASA networks under ARC control that contain moderate-impact and high-impact systems.	Policy Change	*12/31/2011*[22]
IG10013	5/13/2010	Review of the Information Technology Security of [a NASA Network] (Sensitive But Unclassified)	1	The NASA Chief Information Officer should designate a NASA Directorate or Center to immediately develop an oversight process for [a NASA Network] that will include recurrent monitoring of [that Network's] systems for the presence of critical software patches and technical vulnerabilities.	System Change (IT)	2/29/2012
IG10013	5/13/2010	Review of the Information Technology Security of [a NASA Network] (Sensitive But Unclassified)	2	The NASA Chief Information Officer should review all other Agency mission network IT security programs to determine whether each contains an effective oversight process.	System Change (IT)	2/29/2012
IG10019	9/14/2010	Information Technology Security: Improvements Needed in NASA's Continuous Monitoring Processes	1	The NASA CIO should require Centers to monitor computer server operating system configuration for compliance with CIS benchmarks and related OCIS-mandated performance targets.	IT Security Only	2/28/2012
IG10019	9/14/2010	Information Technology Security: Improvements Needed in NASA's Continuous Monitoring Processes	2	The NASA CIO should require Centers to implement a process to validate that 100 percent of applicable network devices, including computers, routers, and firewalls, undergo regular monitoring for technical vulnerabilities.	IT Security Only	2/28/2012
IG10024	9/16/2010	Review of NASA's Management and Oversight of Its Information Technology Security Program	1	The NASA Chief Information Officer should establish an independent verification and validation function to ensure that all FISMA and Agency IT security performance elements are met and information systems are adequately secured.	IT Security Only	4/30/2012
IG10024	9/16/2010	Review of NASA's Management and Oversight of Its Information Technology Security Program	2	The NASA Chief Information Officer should develop a written policy for managing corrective action plans to mitigate IT security weaknesses.	IT Security Only	3/31/2012
IG10018	8/5/2010	Audit of Cyber security Oversight of [a NASA System] (Redacted)	6b	The NASA Chief Information Officer should require all Center Information Technology Security Managers to ensure that controls are in place and effective for vulnerability scanning and configuration management.	IT Security Only	*12/15/2011*[23]
IG11017	3/28/2011	Inadequate Security Practices Expose Key NASA Network to Cyber Attack	1	The Chief Information Officer should immediately identify Internet-accessible computers on their mission computer networks and take prompt action to mitigate identified risks.	IT Security Only	2/29/2012
IG11017	3/28/2011	Inadequate Security Practices Expose Key NASA Network to Cyber Attack	2	The Chief Information Officer should add continuous monitoring of their mission computer networks for Internet-accessible computers as a security control and take prompt action to mitigate identified risks.	IT Security Only	2/29/2012

[22] NASA Management requested closure on February 2, 2012. We are currently assessing the corrective actions.
[23] NASA Management has not requested closure or an extension.

Report No.	Final Issued	Report Title	Rec No.	Recommendation	Rec Type	Mgt Cmplt. Est.
IG11017	3/28/2011	Inadequate Security Practices Expose Key NASA Network to Cyber Attack	3	The Chief Information Officer should conduct an Agency-wide IT security risk assessment of NASA's mission-related networks and systems in accordance with Federal guidelines and industry best practices.	IT Security Only	2/29/2012
IG12006	12/5/2011	NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems	1a	The Chief Information Officer should 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)	System Change (IT)	11/30/2012
IG12006	12/5/2011	NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems	1b	The Chief Information Officer should 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 programs.	System Change (IT)	11/30/2012
IG12006	12/5/2011	NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems	1c	The Chief Information Officer should verify that the security baselines are applied and that credentialed scans are being performed as directed.	System Change (IT)	11/30/2012
IG12006	12/5/2011	NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems	2a	Associate Administrators for Mission Directorates and Center Chief Information Security Officers should ensure that 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.	System Change (IT)	11/30/2012
IG12006	12/5/2011	NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems	2b	Associate Administrator for Mission Directorates and Center Chief Information Security Officers should ensure that 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	System Change (IT)	11/30/2012
IG12006	12/5/2011	NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems	2c	Associate Administrators for Mission Directorates and Center Chief Information Security Officers should ensure that appropriate system data are included in ITSEC-EDW and validated on a semiannual schedule.	System Change (IT)	11/30/2012
IG12006	12/5/2011	NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems	2d	Associate Administrators for Mission Directorates and Center Chief Information Security Officers should ensure that systems undergo credentialed vulnerability scanning and data are integrated into ITSEC-EDW.	System Change (IT)	11/30/2012

Appendix 2.


National Aeronautics and Space Administration
Administrator
Deputy Administrator
Associate Administrator
Chief of Staff
Associate Deputy Administrator
Associate Deputy Administrator for Policy Integration
Assistant Associate Administrator
Advisory Groups NAC and ASAP
Inspector General
Chief Financial Officer*
Chief Information Officer*
Chief Scientist
Chief Technologist
Diversity and Equal Opportunity
Education
International and Interagency Relations
General Counsel
Legislative and Intergovernmental Affairs*
Communications*
Small Business Programs
Chief Engineer
Chief, Safety and Mission Assurance
Chief Health and Medical Officer
Mission Support Directorate
Human Capital Management
Strategic Infrastructure
Headquarters Operations
NASA Shared Services Center
Internal Controls and Management Systems
Procurement
Protective Services
NASA Management Office
Aeronautics Research Mission Directorate
Science Mission Directorate
Human Exploration and Operations Mission Directorate
Ames Research Center
Dryden Flight Research Center
Glenn Research Center
Goddard Space Flight Center
Jet Propulsion Laboratory
Johnson Space Center
Kennedy Space Center
Langley Research Center
Marshall Space Flight Center
Stennis Space Center
Reporting Structure
Administrator
Deputy Administrator
Associate Administrator
Note:
* Center functional office directors report to Agency functional AA. Deputy and below report to Center leadership.
September 2011
www.nasa.gov