HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
February 29, 2012

Statement of
Linda Y. Cureton
NASA Chief Information Officer
before the
Committee on Science, Space and Technology
Subcommittee on Investigations and Oversight
U.S. House of Representatives

Chairman Broun and Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss the state of Information Technology (IT) security at NASA. The agency shares your concern that we must aggressively protect our IT resources and data.

The NASA 2011 Strategic Plan contains an objective to *"Provide information technology that advances NASA space and research program results and promotes open dissemination through efficient, innovative, reliable, and responsive services that are appropriately secure and valued by stakeholders and the public."* Further, NASA's Information Resources Management (IRM) Strategic Plan identifies IT goals and their underlying strategic objectives to be accomplished over the next three to five years in support of advancing NASA's mission and vision. These goals define a common future ideal for our IT workforce to collaboratively accomplish the IT strategy within the constraints of the forecasted IT budget environment, providing affordable information technology and enhanced IT security. One goal calls for the enhancement and strengthening of IT security and cybersecurity to ensure the integrity, availability, and confidentiality of NASA's critical data and IT assets. Other related goals include transforming the IT infrastructure and application services to better meet evolving stakeholder needs and support mission success, while attracting and retaining a high performing IT workforce.

The NASA IT Security vision calls for integrated, secure, and efficient information technology and solutions that support NASA and provides timely, reliable, and cost effective Agency security that safeguards and protects information and information systems. Over the next three to five years the objectives of the vision include the ability to improve NASA's capability to predict, prevent, and effectively contain potential IT security incidents. This vision is driven by the requirement to identify and protect mission information targeted by adversaries such as nation-states, cyber criminals, and hackers; to integrate IT security solutions across NASA; to establish a risk-based approach to managing IT security; and to transform our security program to better predict rather than react to cyber threats. Additional IT trends impacting the protection of NASA's IT infrastructure include cloud computing, social networking and Web 2.0+, the speed of technology changes, and mobile computing.

Like most Federal agencies, NASA has seen the full spectrum of cyber attacks, ranging from minor attacks, where countermeasures are sufficient and appropriate, to sophisticated attacks where in some cases countermeasures are reactive and need improvement. NASA has a high public and Internet profile, its information can be highly attractive to attackers, and whenever IT security compromises occur they tend to generate media attention when the information is public in nature.

How to prepare an agency such as NASA to defend against these rapidly changing threats is best summarized in the National Institute of Science and Technology (NIST) Special Publication 800-39 (March 2011), *Managing Information Security Risk*, in the Prologue section which quotes from the *National Strategy for Cybersecurity Operations,* written by the Chairman of the Joint Chiefs of Staff at the Department of Defense. *"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"* . The fact is that environmental threats and vulnerabilities have the potential to change faster than NASA's security posture. Many of these threats are well-resourced, exhibit varying levels of sophistication, and are highly motivated.

Since NASA's infrastructure is worldwide, the agency is striving to achieve a risk-based balance between security, system operability, and user requirements. While demanding a culture of security awareness, NASA will continue to improve the defense of our IT security posture and build security into the System Development Life Cycle (SDLC) of our IT solutions and everyday work habits. In addition, IT trends indicate a requirement for an integrated and adaptive Agency security posture to support increased interoperability, mobility of the workforce, and new IT security technologies and services to address and mitigate immerging threats and vulnerabilities. This will allow NASA to evolve and strengthen our IT security capabilities.

Aligned with Federal Information Security Management requirements, NASA's Information Technology Security Division's (ITSD) 2012-2014 Information Security Strategic Plan outlines how the Division will continue to support the Agency's mission and objectives, articulating the goals for the next two years. This plan outlines the vision, mission, principles, goals, objectives, supporting goals and 5-year timeline at the Agency, Mission, and Centers levels. The plan emphasizes both an evolutionary and revolutionary transition, moving from detective and preventive measures to a predictive environment embracing innovation, intelligence-driven cybersecurity, and new processes to enhance the security posture of NASA. The plan stresses the need for an Agency governance, risk, and compliance framework that supports the success or our missions with focused actions to reduce attacks on our IT assets.

The Information Security Strategic Plan focuses on enhancing and strengthening information security and privacy services between all NASA stakeholders, internal and external. The plan leverages cross-NASA skills through the Information Technology Security Advisory Board (ITSAB), which serves as the main governing body for information security at NASA. The ITSAB consists of Chief Information Security Officers (CISOs) and senior cybersecurity professionals from NASA Centers and Missions.

The key IT Security metrics to measure performance against the plan will come from areas that are apparent within NASA, such as the Security Operations Center (SOC) incident metrics where they recorded and categorized 1,867 cybersecurity incidents in FY 2011, providing incident type and frequency metrics. Analysis of cyber incidents has led to several active mitigation activities including scanning, patching, vulnerability management, communication, and user training and awareness.
In addition, over the past several years the NASA Office of Inspector General (OIG) has conducted nearly 30 audits of NASA's IT systems, applications and IT practices that have identified various vulnerabilities,

threats, and risks to NASA's IT infrastructure. In its recent Semi-Annual Report to Congress, the OIG reported 37 open audit recommendations concerning NASA IT systems. The OCIO has closed 16 of these recommendations and has developed a corrective action plan to mitigate the remaining open recommendations and findings.

The recommendations from the NASA OIG audits called for NASA to:

- Identify Internet accessible computers on mission networks.
- Conduct security assessments of mission networks.
- Mitigate risks on mission networks.
- Implement continuous monitoring across the IT infrastructure.
- Improve vulnerability scanning.
- Reduce network vulnerabilities.
- Improve asset management.
- Improve configuration management.
- Update policies and procedures.

Over the past year NASA took aggressive actions to mitigate OIG and other findings. IT Stakeholders took the following actions to address the findings under the current financial conditions:

Asset Management

- Scanned the enterprise for vulnerabilities on Internet-connected devices and remediating discovered deficiencies.
- Conducted third-party external assessments of networks to determine website vulnerabilities.
- Implemented a Web Application Security Program.

Vulnerability Management

- Correlated data for analysis of approximately 130,000 connected devices to assess vulnerabilities and security patch status.
- Identified and monitored mandatory critical security controls to continuously assess real-time vulnerabilities.
- Entered a two-year Memorandum of Agreement with the Department of Energy to continue penetration test services of mission networks to identify network vulnerabilities.
- Required credentialed scans to increase the detection of vulnerabilities on Internet-facing devices.

Incident Response

- Completed a NASA-wide incident response handbook to standardize incident response procedures.
- Updated an Incident Management System reporting tool to provide a greater ability to analyze and respond to incidents.
- Instituted new technologies to better capture and contain advanced attacks against the Agency.
- Subscribed to the Department of Homeland Security Shared Services for near real-time threat data to improve the Agency's response to emerging threats and vulnerabilities.

Continuous Monitoring

- Implemented a near real-time risk management program.
- Revised NASA IT security policies to improve continuous monitoring and real-time risk management approaches.
- Conducted an Agency-wide inventory of IT devices and security configurations to assess the security posture of Internet-connected devices.
- Implemented governance and risk management strategies to improve IT Security oversight and compliance.
- Conducted internal program assessments using the Strengths, Weaknesses, Opportunities, and Threats (SWOT) planning tool to determine areas of improved strategic alignment of enterprise IT security services.
- Implemented the IT Infrastructure Integration Program (I3P) to become more efficient in providing IT service management and delivery.

NASA has also developed a series of IT Security handbooks that allow NASA to swiftly adjust NASA cybersecurity policies to meet the escalating and emerging threat landscape as well as the changing needs of the cybersecurity arena. In recent months, NASA has updated several process documents. One of the most notable was the finalization of the NASA Incident Response Working Group's handbook on Information Security Incident Response and Management. Another handbook was designed to ensure that the NASA incident response is uniformly managed across the Agency. Currently, the NASA OCIO is in the process of revising the NASA Procedural Requirement (NPR) on Privacy. In order to ensure that the Privacy program at NASA is properly protecting privacy information, the NASA OCIO based the structure of the NPR on the Federal CIO Council Privacy Committee document entitled *Best Practices: Elements of a Federal Privacy Program.* In addition, the NASA OCIO is actively preparing NASA for the transition to Controlled Unclassified Information (CUI). An interim directive was revalidated to bridge the gap between an expiring NPR and the new CUI policy. NASA is working to ensure that the agency will be ready to transition to CUI once instructed to do so.

In conclusion, the NASA IT Security program is transforming and maturing. The real-world requirement is to protect NASA's information and information systems at a level commensurate with mission needs and information value. Therefore, NASA is increasing visibility and responsiveness through enhanced information security monitoring of NASA's systems across the Agency. NASA IT security process modifications sometimes mature over time, including the centralized Security Operations Center, in order to achieve and realize economies of scale. Much of the maturing process requires a build, check, modify, and retest approach. A critical element in the success of building a truly successful security program is having an independent entity evaluate and honestly appraise the program. The NASA Inspector General's IT audit staff has continuously and aggressively reviewed NASA's IT Security program with an unwavering appraisal of our progress.

Thank you for the Committee's interest in this key security issue and we pledge that NASA, in cooperation with our Inspector General and others, will continue to be vigilant in protecting our IT networks and data.