NASA CYBERSECURITY: AN EXAMINATION OF THE AGENCY'S INFORMATION SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

WEDNESDAY, FEBRUARY 29, 2012

Serial No. 112–64

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PRINTING OFFICE

72–919PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. RALPH M. HALL, Texas, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
PAUL C. BROUN, Georgia
SANDY ADAMS, Florida
BENJAMIN QUAYLE, Arizona
CHARLES J. "CHUCK" FLEISCHMANN, Tennessee
E. SCOTT RIGELL, Virginia
STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
ANDY HARRIS, Maryland
RANDY HULTGREN, Illinois
CHIP CRAVAACK, Minnesota
LARRY BUCSHON, Indiana
DAN BENISHEK, Michigan
VACANCY

EDDIE BERNICE JOHNSON, Texas
JERRY F. COSTELLO, Illinois
LYNN C. WOOLSEY, California
ZOE LOFGREN, California
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
MARCIA L. FUDGE, Ohio
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
JERRY McNERNEY, California
JOHN P. SARBANES, Maryland
TERRI A. SEWELL, Alabama
FREDERICA S. WILSON, Florida
HANSEN CLARKE, Michigan
VACANCY

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HON. PAUL C. BROUN, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
SANDY ADAMS, Florida
RANDY HULTGREN, Illinois
LARRY BUCSHON, Indiana
DAN BENISHEK, Michigan
VACANCY
RALPH M. HALL, Texas

PAUL D. TONKO, New York
ZOE LOFGREN, California
BRAD MILLER, North Carolina
JERRY McNERNEY, California
EDDIE BERNICE JOHNSON, Texas

CONTENTS

Wednesday, February 29, 2012

NASA CYBERSECURITY: AN EXAMINATION OF THE AGENCY'S INFORMATION SECURITY

WEDNESDAY, FEBRUARY 29, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, DC.

The Subcommittee met, pursuant to call, at 2:33 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Paul Broun [Chairman of the Subcommittee] presiding.

RALPH M. HALL, TEXAS
CHAIRMAN

EDDIE BERNICE JOHNSON, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

Subcommittee on Investigations & Oversight Hearing

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

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

Witnesses

Ms. Linda Y. Cureton, Chief Information Officer, National Aeronautics and Space Administration (NASA).

The Honorable Paul K. Martin, Inspector General, National Aeronautics and Space Administration (NASA).

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.

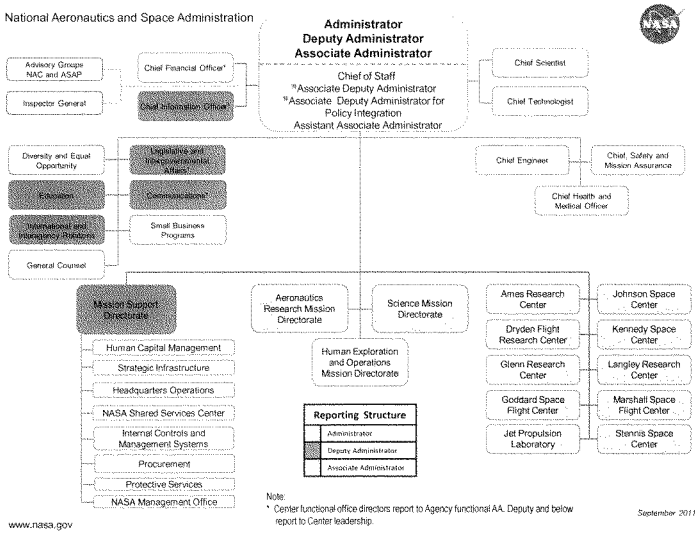
NASA OIG Information Technology Directorate
Open Recommendations for Audit Reports Issued (2006-2011)

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
Advisory Groups
NAC and ASAP
Inspector General
Chief Financial Officer*
Chief Information Officer*
Chief of Staff
*Associate Deputy Administrator
*Associate Deputy Administrator for Policy Integration
Assistant Associate Administrator
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

Chairman BROUN. Subcommittee on Investigations and Oversight will come to order.

Good afternoon, everyone. I appreciate everybody's patience. We just had votes on the Floor, so I appreciate you all's patience to the beginning of this hearing.

I want to welcome you all to the hearing entitled, "NASA Cybersecurity: An Examination of the Agency's Information Security." You will find in front of you packets containing our witness panel's testimony, their biographies, and truth in testimony disclosures. I want to welcome our witnesses here today.

I am going to begin by recognizing myself for five minutes for an opening statement.

The topic of cybersecurity is certainly hot these days. As Washington debates the government's appropriate role in private sector cybersecurity activities, we should remember that the government is already responsible for securing its own networks and information, a task that is executed with mixed successes.

While the defense and intelligence communities take great steps to protect data and operations from theft and corruption, oftentimes civil agencies are not as vigilant. In many instances this is for good reason. Transparency, coordination, and collaboration are core values of an effective government, particularly as it involves scientific agencies.

Openness, however, does not come without risk. Many of the technologies developed and utilized by NASA are just as useful for military purposes as they are for civilian space applications. While our Nation's defense and intelligence communities guard their front door and prevent network intrusions, they could steal or corrupt sensitive information. NASA could essentially become an unlocked back door without persistent vigilance.

Information security concerns at NASA are not limited to nonproliferation. There is a serious economic competitiveness aspect as well. The loss or theft of NASA technologies could compromise U.S. innovation and curtail significant future commercial activities that bolster our economy. In order to ensure that NASA does not become the weak underbelly that allows enemies and competitors to access sensitive technologies, we have to make sure that NASA has the necessary authorities to protect that information.

The NASA Office of the Inspector General has monitored the agency's cybersecurity for over a decade, issuing dozens of reports and recommendations. To NASA's credit, they have taken action to address these recommendations in a timely fashion by clarifying the role of the Headquarters Chief Information Officer, realigning the agency's other CIOs under that office, setting up the security operations center or SOC, and improving integration and visibility. Despite this progress, the threat to NASA's information security is persistent and ever changing. Unless NASA is able to continuously innovate and adapt, their data, systems, and operations will continue to be endangered.

These are not simply bureaucratic matters that have no real world impact or theoretical possibilities with little chance of occurring. As the Inspector General points out in his testimony, NASA has experienced 5,408 computer security incidents in 2010 and 2011. That is a bunch. These intrusions resulted in the installation

of malicious software or unauthorized access which caused significant disruptions to mission operations, the theft of export-controlled data, and technologies, and cost the agency more than $7 million.

Just last year the theft of an encrypted NASA laptop resulted in the loss of algorithms used to command and control the International Space Station. Similarly, the U.S. China Economic and Security Review Commission recently noted in its annual report to Congress that the Terra and Landsat-7 satellites have, "have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems."

The fact that NASA is a high-profile target should come as no surprise. What is astonishing, however, is the fact that they are such a big target. NASA manages approximately 3,400 individual websites. For context, there are approximately 4,000 websites throughout the rest of the government. Simply surveying this attack profile is a challenge, but defending it presents even more difficulties.

Adding to this complexity are differing security profiles for NASA's Centers, Mission Directorates, and institutional capabilities. Despite the challenge, it is still imperative that NASA conduct a thorough agency-wide risk assessment and develop a corresponding mitigation strategy in a timely fashion as recommended by the NASA IG last March.

I look forward to our witnesses' testimony and hope that we can all work together to ensure that our Nation's space agency can securely support and appropriately protect cutting edge research, collaborative science, and mission operations.

[The prepared statement of Dr. Broun follows:]

PREPARED STATEMENT OF SUBCOMMITTEE CHAIRMAN PAUL BROUN

The topic of cybersecurity is certainly hot these days. As Washington debates the government's appropriate role in private-sector cybersecurity activities, we should remember that the government is already responsible for securing its own networks and information—a task that it has executed with mixed success.

While the defense and intelligence communities take great steps to protect data and operations from theft and corruption, often times civil agencies are not as vigilant. In many instances, this is for good reason. Transparency, coordination, and collaboration are core values of an effective government, particularly as it involves scientific agencies.

Openness, however, does not come without risk. Many of the technologies developed and utilized by NASA are just as useful for military purposes as they are for civil space applications. While our nation's defense and intelligence communities guard the "front door" and prevent network intrusions that could steal or corrupt sensitive information, NASA could essentially become an unlocked "back door" without persistent vigilance.

Information security concerns at NASA are not limited to non-proliferation. There is a serious economic competitiveness aspect as well. The loss or theft of NASA technologies could compromise U.S. innovation and curtail significant future commercial activities that bolster our economy. In order to ensure that NASA does not become the weak underbelly that allows enemies and competitors to access sensitive technologies, we have to make sure that NASA has the necessary authorities to protect that information.

The NASA Office of the Inspector General has monitored the Agency's cyber security for over a decade, issuing dozens of reports and recommendations. To NASA's credit, they have taken action to address those recommendations in a timely fashion by clarifying the role of the Headquarters Chief Information Officer, realigning the Agency's other CIOs under that office, setting up the Security Operations Center (SOC), and improving integration and visibility. Despite this progress, the threat to

NASA's information security is persistent, and ever changing. Unless NASA is able to continuously innovate and adapt, their data, systems, and operations will continue to be endangered.

These are not simply bureaucratic matters that have no real-world impact, or theoretical possibilities with little chance of occurring. As the Inspector General points out in his testimony, NASA experienced 5,408 computer security incidents in 2010 and 2011. These intrusions resulted in the installation of malicious software or unauthorized access which caused significant disruptions to mission operations, the theft of export-controlled data and technologies, and cost the Agency more than $7 million.

Just last year, the theft of an unencrypted NASA laptop resulted in the loss of algorithms used to command and control the International Space Station. Similarly, the U.S. China Economic and Security Review Commission recently noted in its annual report to Congress that the Terra and Landsat-7 satellites "have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems."

The fact that NASA is a high profile target should come as no surprise. What is astonishing, however, is the fact that they are such a big target. NASA manages approximately 3,400 individual websites. For context, there are approximately 4000 websites throughout the rest of the government. Simply surveying this attack profile is a challenge, but defending it presents even more difficulties.

Adding to this complexity are differing security profiles for NASA's Centers, Mission Directorates and institutional capabilities. Despite the challenge, it is still imperative that NASA conduct a thorough Agency-wide risk assessment and develop a corresponding mitigation strategy in a timely fashion as recommended by the NASA IG last March.

I look forward to our witnesses' testimony, and hope that we can all work together to ensure that our nation's space agency can securely support and appropriately protect cutting edge research, collaborative science, and mission operations.

Chairman BROUN. Now I recognize Ranking Member Tonko from New York for his opening statement for five minutes.

Mr. TONKO. Thank you, Mr. Chair, and thank you to our two witnesses, to our Chief Information Officer Cureton, and to our Inspector General Martin. Thank you for joining us.

I want to thank you, Mr. Chair, for calling this hearing, and again, extend a welcome to our two distinguished witnesses this afternoon. Inspector General Martin has been getting high marks for the work of his office, and Ms. Cureton should be congratulated for being willing to take on a tough job that the country needs to see done well.

Twice in 2008, on-earth observation satellite, and earth observation satellite managed by NASA's Goddard Spaceflight Center experienced several minutes of interference that prevented NASA from communicating with the spacecraft. The events were indicative of an international cyber attack, and the techniques were used, and I quote, "consistent with the authoritative Chinese military writings," according to a report by the U.S. China Economic and Security Review Commission.

The report did not attribute the specific instances against the NASA satellites to China, but the implications were clear. NASA's spacecraft may be vulnerable to acts of cyber attack.

In both instances involving NASA's Terra Earth Observation Satellite, the report concluded, and I quote, "The responsible party achieved all steps required to command the satellite but did not issue commands."

Cyber attacks against NASA are nothing new. Over the past decade both American citizens and foreign nationals have penetrated the agency's cyber defenses, installed malicious software, and stolen scientific security and other data. These threats have come

from foreign nationals in China, Great Britain, Italy, Nigeria, Portugal, Romania, Russia, Turkey, and Estonia. Just last month the Romanian national who had allegedly hacked into a NASA computer server and posted sensitive satellite data he acquired online was arrested by Romanian officials. Last November the NASA Office of Inspector General, along with the FBI, announced charges against six Estonian nationals and one Russian national. They infected NASA and other computers with malware that alerted the settings of more than four million infected computers, sending internet searches on them to specific websites, generating more than $14 million in fraudulent advertising fees for the cyber criminals.

The number of potential threats is expanding rapidly. A recent Cisco System study found that there were an estimated 12.5 billion electronic devices capable of connecting to the internet in 2010. This number will increase to approximately 25 billion in 2015, and an astounding 50 billion by 2020. Given this continued expansion of the computer communications networks, organizations such as NASA will face a digital battlefield of constantly-evolving points of attack and new efforts to exploit weaknesses.

The challenge in successfully addressing cybersecurity issues is particularly difficult at NASA. NASA owns a little less than a half of the United States Government's non-defense websites. There are approximately 3,400 NASA-controlled websites, and nearly 1,600 of these are linked to the outside world. There are an estimated 176,000 individual IP addresses assigned to NASA's IT systems and IT networks.

NASA also possesses more than 120,000 computer or related devices located at its centers and facilities that are connected to the agency's IT networks. This huge system of nodes and networks presents enormous IT security challenges and potential IT vulnerabilities to the agency.

Over the past two years NASA reported more than 5,400 computer security intrusions that resulted in the installation of malicious software or unauthorized access to NASA's computer systems. These cyber threats pose unique safety and security concerns to NASA. NASA's IT systems control spacecraft, including the Hubble Space Telescope and International Space Station. They collect and process scientific data and contain records on a wide array of technologically sophisticated intellectual property. These are all attractive targets for cyber attack.

Yet NASA cannot just take those systems off the internet to make them secure because they connect its thousands of scientists, engineers, and other employees around the country to each other, and they connect NASA's human and information resources to the rest of the world.

Unfortunately, NASA has a poor history of addressing cybersecurity threats. Insufficient efforts have been made in the past to take appropriate actions to confront and correct internal agency deficiencies. For example, the IG has reinvestigated cyber-related issues it had identified in prior reports only to find the original weaknesses still uncorrected.

These failures over time have exacerbated the agency's vulnerabilities. They certainly complicate efforts by the new leader-

ship at NASA to address cybersecurity quickly and effectively. NASA's IG has found that the agency does not have an IT security configuration baseline across the agency. In other words, it is unclear what NASA's IT security is supposed to look like because there is no diagram of what it does look like.

In addition, the IG has found that the agency's vulnerability management practices have drastically underestimated the cybersecurity threats and vulnerabilities NASA faces, and the agency lacks a complete, up-to-date inventory of all of its IT components.

Clearly it is easier to protect your home from a potential intruder if you know how many doors you have and where they are located. NASA does not appear to possess an accurate blueprint of its own house's IT infrastructure. Without that NASA cannot ensure that every potential gateway into the agency is monitored and effectively protected.

My comments are not specifically directed at NASA's Office of the Chief Information Officer or Ms. Cureton, NASA's Chief Information Officer, who is testifying before us today. In fact, I hope my statement makes clear that I believe the problems with cybersecurity at NASA are many years in the making, and Ms. Cureton has had limited time to set things right.

I am also aware that the CIO at NASA has limited authority to impose cybersecurity solutions across the entire NASA enterprise of contractors, centers, and mission directorates. There seems to be a gap between the scope of your responsibility and the scope of your authority.

NASA's IT vulnerabilities must be identified and closed. Speed is critical in this context. If there are institutional or financial stumbling blocks that stand in the way of completing these critical tasks, then I hope our witnesses will provide constructive suggestions to address them. The committee is prepared to work with NASA to help close these gaps. I believe this is an important subject, and I look forward to hearing from our witnesses.

Thank you, Mr. Chair.

[The prepared statement of Mr. Tonko follows:]

PREPARED STATEMENT OF SUBCOMMITTEE RANKING MEMBER PAUAL D. TONKO

Thank you for calling this hearing Mr. Chairman, and I want to extend a welcome to our two distinguished witnesses this morning. Inspector General Martin has been getting high marks for the work of his office and Ms. Cureton should be congratulated for being willing to take on a tough job that the country needs to see done well.

Twice in 2008 an earth observation satellite managed by NASA's Goddard Space Flight Center experienced several minutes of interference that prevented NASA from communicating with the spacecraft. The events were indicative of an intentional cyber attack and the techniques used were quote, "consistent with authoritative Chinese military writings," according to a report by the U.S.- China Economic and Security Review Commission. The report did not attribute the specific instances against the NASA satellites to China but the implications were clear: NASA's spacecraft may be vulnerable to acts of cyber attack. In both instances involving NASA's Terra Earth Observation Satellite (EOS), the report concluded—quote: "The responsible party achieved all steps required to command the satellite but did not issue commands."

Cyber attacks against NASA are nothing new. Over the past decade both American citizens and foreign nationals have penetrated the agency's cyber defenses, installed malicious software and stolen scientific, security and other data. These threats have come from foreign nationals in China, Great Britain, Italy, Nigeria,

Portugal, Romania, Russia, Turkey and Estonia. Just last month a Romanian national who had allegedly hacked into a NASA computer server and posted sensitive satellite data he acquired on-line was arrested by Romanian officials. Last November, the NASA Office of Inspector General, along with the FBI announced charges against six Estonian nationals and one Russian national for infecting NASA and other computers with malware that secretly altered the settings of more than four million infected computers sending Internet searches on those computers to specific websites generating more than $14 million in fraudulent advertising fees for the cyber criminals.

The number of potential threats is expanding rapidly. A recent Cisco Systems study found that there were an estimated 12.5 billion electronic devices capable of connecting to the Internet in 2010. This number will increase to approximately 25 billion in 2015 and an astounding 50 billion by 2020. Given this continued expansion of computer communications networks, organizations such as NASA will face a digital battlefield of constantly evolving points of attack and new efforts to exploit weaknesses.

The challenge in successfully addressing cyber-security issues is particularly difficult at NASA. NASA owns a little less than half of the U.S. government's non-Defense web-sites. There are approximately 3,400 NASA controlled web-sites and nearly 1,600 of these are linked to the outside world. There are an estimated 176,000 individual IP addresses assigned to NASA's IT systems and networks. NASA also possesses more than 120,000 computer or related devices located at its centers and facilities that are connected to the Agency's IT networks. This huge system of nodes and networks presents enormous IT security challenges and potential IT vulnerabilities to the Agency. Over the past two years NASA reported more than 5,400 computer security intrusions that resulted in the installation of malicious software or unauthorized access to NASA's computer systems.

These cyber threats pose unique safety and security concerns to NASA. NASA's IT systems control spacecraft, including the Hubble Space Telescope and International Space Station, collect and process scientific data, contain records on a wide-array of technologically sophisticated intellectual property. These are all attractive targets for cyber-attack. Yet NASA cannot just take their systems off the internet to make them secure because they connect its thousands of scientists, engineers and other employees around the country to each other and connect NASA's human and information resources to the rest of the world.

Unfortunately NASA has a poor history of addressing cybersecurity threats. Insufficient efforts have been made in the past to take appropriate actions to confront and correct internal agency deficiencies. For example, the IG has re-investigated cyber-related issues it had identified in prior reports only to find the original weaknesses still uncorrected. These failures over time have exacerbated the agency's vulnerabilities. They certainly complicate efforts by the new leadership at NASA to address cybersecurity quickly and effectively.

NASA's IG has found that the Agency does not have an IT security configuration baseline across the agency. In other words, it is unclear what NASA's IT security is supposed to look like because there is no diagram of what it does look like. In addition, the IG has found that the Agency's vulnerability management practices have drastically underestimated the cyber-security threats and vulnerabilities NASA faces. And the Agency lacks a complete up-to-date inventory of all of its IT components.

Clearly it is easier to protect your home from a potential intruder if you know how many doors you have and where they are located. NASA does not appear to possess an accurate blueprint of its own house's IT infrastructure. Without that NASA cannot ensure that every potential gateway into the Agency is monitored and effectively protected.

My comments are not specifically directed at NASA's Office of the Chief Information Officer or Ms. Cureton, NASA's Chief Information Officer (CIO) who is testifying before us today. In fact, I hope my statement makes clear that I believe the problems with cybersecurity at NASA are many years in the making, and Ms. Cureton has had limited time to set things right. I am also aware that the CIO at NASA has limited authority to impose cybersecurity solutions across the entire NASA enterprise of contractors, Centers, and Mission Directorates. There seems to be a gap between the scope of your responsibility and the scope of your authority.

NASA's IT vulnerabilities must be identified and closed. Speed is critical in this context. If there are institutional or financial stumbling blocks that stand in the way of completing these critical tasks then I hope our witnesses will provide constructive suggestions to address them. The Committee is prepared to work with NASA to help close these gaps.

I believe this is an important subject and I look forward to hearing from our witnesses. Thank you Mr. Chairman.

Chairman BROUN. Thank you, Mr. Tonko. If there are Members who wish to submit additional opening statements, their statements will be added to the record at this point.

Now at this time I would like to introduce our panel of witnesses. Ms. Linda Cureton, the Chief Information Officer at NASA, and the Honorable Paul K. Martin, the Inspector General of NASA.

As our witnesses should know, spoken testimony is limited to five minutes each, after which the Members of the Committee will have five minutes each to ask questions. Your written testimony will be included in the record of the hearing.

Now, it is the practice of this subcommittee to receive testimony under oath. Do either of you have any objections to taking the oath? Both indicated by saying "no" and shaking their head side to side reflecting no. Let the record reflect such.

If all of you would please stand and raise your right hand. Do you solemnly swear or affirm to tell the whole truth and nothing but the truth, so help you God? Thank you. You may be seated. Let the record reflect that the witnesses participating have taken the oath.

Now I recognize our first witness, Ms. Cureton. You have five minutes.

TESTIMONY OF LINDA Y. CURETON, CHIEF INFORMATION OFFICER, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Ms. CURETON. Chairman Broun and Members of the Subcommittee, thank you for the opportunity to appear before you to discuss the state of information technology security at NASA.

Today NASA professionally plans, builds, and practices IT security to ensure integrity, availability, and confidentiality of NASA's critical data and IT assets. The challenge is to get ahead and stay ahead of cyber attackers who tend to be well-resourced, exhibit varying levels of sophistication, and are highly motivated. The pace of technological changes such as cloud computing, social networking, and mobile computing modify the landscape and compound the cybersecurity challenges.

NASA's Information Resources Management Strategic Plan outlines strategic goals and objectives to provide cost-effective agency security that safeguards and protects information and information systems. We are determined to improve NASA's capability to predict, prevent, and effectively contain potential IT security incidents. Our motivation is driven by the need to protect mission information targeted by nation states, cyber criminals, and hackers, predict rather than react to cyber threats, and create an adaptive agency security posture that supports increased interoperability, mobility, and innovation.

NASA's Security Operation Center recorded and categorized 1,867 cybersecurity incidents in fiscal year 2011. Analysis of those cyber incidents led to additional patching, vulnerability management, communication, and user training and awareness.

Building a truly successful security program requires independent evaluation and honest appraisal. The NASA Office of In-

spector General IT Audit Staff continuously and aggressively review NASA's IT security program. Over the past several years the OIG has conducted audits of NASA's IT systems, applications, and IT practices. They identified vulnerabilities, threats, and risks to NASA's IT infrastructure. In their last semi-annual report to Congress the OIG noted 37 open IT security audit recommendations, calling 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.

Sixteen of the OIG recommendations have been closed, and a corrective action plan has been implemented to mitigate the remaining open recommendations. NASA has accomplished the following under the plan: Inventory IT devices and security configurations agency wide, scanned for vulnerabilities on internet-connected devices, remediated discovered deficiencies, conducted third-party external assessments of NASA networks to determine website vulnerabilities, introduced new technologies to capture and contain cyber attacks, analyzed approximately 130,000 connected devices to assess vulnerabilities and security patch status. Entered a two-year agreement with the Department of Energy for penetration testing of mission networks, conducted strengths, weaknesses, opportunities, and threat assessments to improve strategic alignment of enterprise IT security services, standardized IT security incident response procedures, and consolidated contracts to provide streamlined IT service management and delivery through the IT Infrastructure Integration Program, I3P.

Finally, NASA remains committed to continued improvement of the IT security posture as the NASA IT Security Program is transforming and maturing.

Thank you.

[The prepared statement of Ms. Cureton follows:]

PREPARED STATEMENT OF MS. LINDA Y. CURETON,
CHIEF INFORMATION OFFICER, NASA

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.

Chairman BROUN. Thank you, Ms. Cureton.

I now recognize our next witness, Mr. Martin, for five minutes.

TESTIMONY OF THE HONORABLE PAUL K. MARTIN, INSPECTOR GENERAL, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Mr. MARTIN. Thank you, Mr. Chairman. Chairman Broun, Ranking Member Tonko, and Congressman, excuse me, Congresswoman Adams, thank you for the opportunity to testify at today's hearing about NASA's efforts to protect its information technology resources.

As it has been pointed out, NASA's IT assets include more than 550 information systems that control spacecraft, collect and process scientific data, and enable NASA personnel to collaborate with contractors, academics, and members of the public around the world. NASA is a regular target of cyber attacks, both because of the large size of its networks and because those networks contain highly-sought after information.

Moreover, some NASA systems house sensitive information, which, if lost or stolen, could result in significant financial loss, adversely affect national security, or significantly impair our Nation's technological advantage.

At the same time NASA's statutory mission to share its scientific information presents heightened IT security challenges because the agency's connectivity with outside organizations provide cyber criminals with a larger target compared to many other government agencies.

In 2010 and 2011, NASA reported 5,408 computer security incidents that resulted in the installation of malicious software on or unauthorized access to its systems. These incidents ranged from individuals testing their hacking skills to well-organized criminal enterprises seeking to exploit NASA's systems for profit to intrusions that may have been sponsored by foreign intelligence services. Taken together these intrusions have affected thousands of NASA computers, caused significant disruptions to mission operations, and resulted in the theft of export controlled and otherwise sensitive data.

The OIG devotes substantial resources to examining NASA's efforts to protect its IT systems. Over the past five years we have issued 21 audit reports containing 69 IT-related recommendations. To date all but 18 have been closed.

In addition, the OIG has conducted more than 16 investigations of breaches of NASA's networks, several of which have resulted in the arrest of individuals as has been pointed out in the U.S., China, Great Britain, Italy, Nigeria, Romania, Turkey, and Estonia.

My written statement discusses in detail five issues that we believe constitute NASA's most pressing challenges in the admittedly-difficult task of protecting the agency's IT information from loss or theft. Briefly, these challenges are, number one, lack of full awareness of agency-wide IT security posture. NASA's IT assets generally fall into two categories; institutional systems and networks that support administrative functions such as budgeting and human resources and mission systems that support the agency's

aeronautics, science, and space programs. While the CIO has the ability to implement security programs for NASA's institutional systems, she cannot fully account for or ensure that the agency's mission assets comply with appropriate IT security policies.

Number two, shortcomings in implementing continuous monitoring. NASA has not fully transitioned from its historic snapshot approach for certifying the security of its IT systems to an approach that relies on a more comprehensive program of ongoing monitoring.

Number three, the slow pace of inscription. NASA has been very slow to implement full-disk encryption on its notebook computers and other mobile devices, exposing sensitive information to unauthorized disclosure when these devices are lost or stolen. OMB has reported a government-wide encryption rate for these devices of 54 percent. In contrast, at the beginning of this month only one percent of NASA's portable devices have been encrypted.

Number four, the ability to combat sophisticated cyber attacks. Increasingly, NASA has become a target of a sophisticated form of cyber attack known as an advanced persistent threat or APT. In fiscal year 2011, alone NASA reported it was the victim of 47 such attacks with 13 successfully compromising agency systems.

And number five, transition to cloud computing. While cloud computing promises significant cost savings, NASA must carefully weigh potential risks such as loss or compromise of its data posted on the cloud.

This concludes my remarks. I would be pleased to answer any questions.

[The prepared statement of Mr. Martin follows:]

PREPARED STATEMENT OF THE HONORABLE PAUL K. MARTIN,
INSPECTOR GENERAL, NASA

Testimony before the Subcommittee on Investigations and Oversight,
House Committee on Science, Space, and Technology

U.S. House of Representatives

For Release on Delivery
expected at
2:00 p.m. EST
Wednesday
February 29, 2012

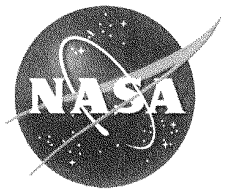
NASA Cybersecurity: An Examination of the Agency's Information Security

Statement of

Paul K. Martin

Inspector General

National Aeronautics and Space Administration



Chairman Broun, Ranking Member Tonko, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing. The Office of Inspector General (OIG) is committed to providing independent and aggressive oversight of the National Aeronautics and Space Administration (NASA), and we welcome this opportunity to discuss the status of the Agency's efforts to protect its information technology (IT) resources.

My testimony today highlights five issues that we believe, based on our extensive audit and investigative work, constitute NASA's most serious challenges in the admittedly difficult task of protecting the Agency's information and systems from inadvertent loss or malicious theft. These challenges are:

- Lack of full awareness of Agency-wide IT security posture;
- Shortcomings in implementing a continuous monitoring approach to IT security;
- Slow pace of encryption for NASA laptop computers and other mobile devices;
- Ability to combat sophisticated cyber attacks; and
- Transition to cloud computing.

By way of background, NASA's portfolio of IT assets includes more than 550 information systems that control spacecraft, collect and process scientific data, and enable NASA personnel to collaborate with colleagues around the world. Hundreds of thousands of individuals, including NASA personnel, contractors, academics, and members of the public use these IT systems daily and NASA depends on these systems to carry out its essential operations.

NASA spends more than $1.5 billion annually on its IT-related activities, including approximately $58 million for IT security. However, because IT networks for many NASA programs and projects are often bundled with funding for the underlying mission, these figures may not represent the full cost of NASA's IT investments.

Some NASA systems house sensitive information which, if lost or stolen, could result in significant financial loss, adversely affect national security, or significantly impair our Nation's competitive technological advantage. Even more troubling, skilled and committed cyber attackers could choose to cause significant disruption to NASA operations, as IT networks are central to all aspects of NASA's operations. NASA is a regular target of cyber attacks both because of the large size of its networks and because those networks contain information highly sought after by criminals attempting to steal technical data or compromise NASA networks to further other criminal activities. Moreover, NASA's statutory mission to share scientific information presents unique IT security challenges. The Agency's connectivity with outside organizations – most notably non-governmental entities such as educational institutions and research facilities – presents cybercriminals with a larger target than that of many other Government agencies.

In 2010 and 2011, NASA reported 5,408 computer security incidents that resulted in the installation of malicious software on or unauthorized access to its systems. These incidents spanned a wide continuum from individuals testing their skill to break into NASA systems, to well-organized criminal enterprises hacking for profit, to intrusions that may have been sponsored by foreign intelligence services seeking to further their countries' objectives. Some of

these intrusions have affected thousands of NASA computers, caused significant disruption to mission operations, and resulted in the theft of export-controlled and otherwise sensitive data, with an estimated cost to NASA of more than $7 million. To put these findings in context, however, NASA OIG is the only Office of Inspector General that regularly conducts international network intrusion cases, and this fact could skew perceptions with regard to NASA's relative rate of significant intrusion events compared to other agencies.

Because of NASA's status as a "target rich" environment for cyber attacks, the OIG devotes substantial resources to overseeing NASA's efforts to protect its IT systems. Over the past 5 years, we have issued 21 audit reports containing 69 IT-related recommendations. In addition, OIG investigators have conducted more than 16 separate investigations of breaches of NASA networks during the past few years, several of which have resulted in the arrests and convictions of foreign nationals in China, Great Britain, Italy, Nigeria, Portugal, Romania, Turkey, and Estonia.

Through our audits and investigations, we have identified systemic internal control weaknesses in NASA's IT security control monitoring and cybersecurity oversight. The second part of my testimony will focus on the most significant findings from our oversight work that present the greatest challenges to NASA in protecting its IT assets.

Chief Information Officer Lacks Visibility of and Oversight Authority for Key NASA IT Assets

NASA needs to improve Agency-wide oversight of the full range of its IT assets. Federal law and NASA policy designate the Headquarters-based Chief Information Officer (CIO) as the official responsible for developing IT security policies and procedures and implementing an Agency-wide IT security program. However, we have found that the CIO has limited ability to direct NASA's Mission Directorates to fully implement CIO-recommended or mandated IT security programs.

NASA's IT assets generally fall into two categories: (1) the "institutional" systems and networks the Agency uses to support such administrative functions as budgeting and human resources and (2) the "mission" systems and networks that support the Agency's aeronautics, science, and space programs such as the Mission Operations Directorate at Johnson Space Center, the Huntsville Operations Center at Marshall Space Flight Center, and the Deep Space Network at the Jet Propulsion Laboratory (JPL). The CIO has a complete inventory of and the authority to implement the Agency's IT security program for NASA's institutional IT assets. However, she cannot fully account for or ensure that NASA's mission IT assets comply with applicable IT security policies and procedures.

IT assets on NASA's mission computer networks are funded by the related Mission Directorate, which is responsible for IT security, including the authority for risk determination and risk acceptance. Moreover, IT staff responsible for implementing security controls on mission IT assets report to the Mission Directorate and not the NASA CIO. Thus, the CIO does not have the authority to ensure that NASA's IT security policies are followed across the Agency.

Through our work, we have found that the Mission Directorates often lack effective IT security, and as a result, IT assets operated by these Directorates do not consistently implement key IT security controls. For example, a May 2010 OIG audit found that only 24 percent of applicable computers on a mission network were monitored for critical software patches and only 62 percent were monitored for technical vulnerabilities. Our detailed control test of this network identified several high-risk technical vulnerabilities on a system that provides mission support to manned and unmanned spacecraft.

Achieving the Agency's IT security goals will require sustained improvements in NASA's overarching IT management practices, particularly as they apply to the CIO's oversight of NASA's mission IT assets. Effective IT governance is the key to accommodating the myriad interests of internal and external stakeholders and making decisions that balance compliance, cost, risks, and mission success. As one step in this process, in October 2011 NASA adopted an IT governance model to streamline decision making for and prioritization of strategic IT investments across the Agency. However, our review of this model revealed limited involvement by senior Mission Directorate officials in these decisions. Moreover, the model does not incorporate IT security policy as a key element when evaluating significant IT investments. Until NASA incorporates IT security policy into its Agency-wide IT governance model and fully implements related IT security programs, it will continue to be at risk for security incidents that can have a severe adverse effect on Agency operations and assets.

Finally, a December 2010 audit highlighted another example of the CIO's lack of Agency-wide control of IT security processes. Specifically, we examined NASA's internal controls for sanitization and disposal of excess Shuttle IT equipment at four NASA Centers. We found significant weaknesses that resulted in computers and hard drives being sold or prepared for sale even though they still contained sensitive NASA data. For example, one Center released 10 computers to the public that had failed sanitization testing and therefore may have contained sensitive NASA data. OIG auditors confiscated four additional computers that had failed sanitization testing but were nevertheless being prepared for sale. Significantly, one of these computers contained data subject to export control restrictions. We also found a lack of accountability for IT equipment, which included the discovery of excessed hard drives in an unsecured dumpster accessible to the public at one Center.

Shortcomings in Implementing Continuous Monitoring of IT Security

The Federal Information Security Management Act or FISMA requires agencies to develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of agency information assets. In order to satisfy annual reporting requirements, agencies expend large amounts of money and resources to document compliance with the many FISMA reporting areas. However, an agency's FISMA grade has been found to be unrelated to whether its IT assets are adequately protected from attack. Thus, FISMA has, to a large extent, devolved into an expensive paperwork exercise that fails to accurately measure an organization's IT security posture.

More recent FISMA guidance has shifted the focus of Agency oversight from periodic assessments and compliance reporting to using tools and techniques to conduct ongoing monitoring of IT security controls. Specifically, the goal of this "continuous monitoring"

initiative is to determine whether a system's key IT security controls continue to be effective over time in light of system changes. A well-designed and well-managed continuous monitoring program can transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential information about a system's security status on a real-time basis. This, in turn, enables officials to take timely risk mitigation actions and make risk-based decisions regarding the operation of their IT systems.

Our oversight work has identified several issues relating to NASA's transition from its previous "snapshot" approach for certifying the security of its IT systems to a continuous monitoring program.

We found that although NASA has made progress in transitioning to continuous monitoring, the Agency needs to take significant steps to ensure its successful implementation. 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. Only by making improvements in each of these areas can NASA ensure that its continuous monitoring will provide adequate protection for the Agency's IT systems.

NASA Lags Far Behind Other Federal Agencies in Protecting Data on Agency Laptops

Encrypting sensitive data on notebooks and other mobile computing devices is a widely recognized best practice and an action required by the Office of Management and Budget (OMB). However, NASA has been slow to implement full-disk encryption on the notebook computers and other mobile computing devices it provides to its employees, potentially exposing sensitive information to unauthorized disclosure when such devices are lost or stolen. In fact, in its fiscal year (FY) 2010 report to Congress on FISMA implementation, the OMB reported a Government-wide encryption rate for these devices of 54 percent. However, as of February 1, 2012, only 1 percent of NASA portable devices/laptops have been encrypted.

Between April 2009 and April 2011, NASA reported the loss or theft of 48 Agency mobile computing devices, some of which resulted in the unauthorized release of sensitive data including export-controlled, Personally Identifiable Information (PII), and third-party intellectual property. For example, the March 2011 theft of an unencrypted NASA notebook computer resulted in the loss of the algorithms used to command and control the International Space Station. Other lost or stolen notebooks contained Social Security numbers and sensitive data on NASA's Constellation and Orion programs. Moreover, NASA cannot consistently measure the amount of sensitive data exposed when employee notebooks are lost or stolen because the Agency relies on employees to self-report regarding the lost data rather than determining what was stored on the devices by reviewing backup files.

Until NASA fully implements an Agency-wide data encryption solution, sensitive data on its mobile computing and portable data storage devices will remain at high risk for loss or theft.

NASA's Readiness to Combat Sophisticated Cyber Attacks

Increasingly, NASA has become a target of a sophisticated form of cyber attack known as advanced persistent threats (APTs). APTs refer to those groups that are particularly well resourced and committed to steal or modify information from computer systems and networks without detection. The individuals or nations behind these attacks are typically well organized and well funded and often target high-profile organizations like NASA. Moreover, even after NASA fixes the vulnerability that permitted the attack to succeed, the attacker may covertly maintain a foothold inside NASA's system for future exploits.

In FY 2011, NASA reported it was the victim of 47 APT attacks, 13 of which successfully compromised Agency computers. In one of the successful attacks, intruders stole user credentials for more than 150 NASA employees – credentials that could have been used to gain unauthorized access to NASA systems. Our ongoing investigation of another such attack at JPL involving Chinese-based Internet protocol (IP) addresses has confirmed that the intruders gained full access to key JPL systems and sensitive user accounts. With full system access the intruders could: (1) modify, copy, or delete sensitive files; (2) add, modify, or delete user accounts for mission-critical JPL systems; (3) upload hacking tools to steal user credentials and compromise other NASA systems; and (4) modify system logs to conceal their actions. In other words, the attackers had full functional control over these networks.

Our computer crimes investigations indicate that the sophistication of cyber attacks against NASA is increasing. For example, in November 2011 the Federal Bureau of Investigation and NASA OIG worked with partners throughout the world to dismantle a cybercriminal network operated under the cover of an Estonian company called Rove Digital. Seven individuals were charged with engaging in a financial fraud scheme that spanned over 100 countries and infected 4 million computers. At least 500,000 of the victim computers were in the United States, including more than 130 NASA computers. Fortunately, we found no evidence of operational harm to NASA or compromise of sensitive data caused by these intrusions. Nevertheless, the scope and success of the intrusions demonstrate the increasingly complex nature of the IT security challenges facing NASA and other Government agencies.

In an effort to improve the Agency's capability to detect and respond to cyber threats, in November 2008 NASA consolidated its Center-based computer security incident detection and response programs into a single, Agency-wide computer security incident handling capability called the Security Operations Center (SOC). Located at Ames Research Center, the SOC is NASA's central coordination point for incident detection, response, and reporting. The SOC provides NASA with: (1) continuous Agency-wide incident monitoring and detection; (2) communication with Centers in the form of weekly conference calls and security bulletins to share incident and threat information with Agency incident responders; (3) a centralized information system called the Incident Management System for storing, managing, and reporting incidents internally and to parties such as the NASA OIG and the U.S. Computer Emergency Readiness Team; and (4) a hotline for reporting potential IT security incidents. We currently are conducting an audit examining the effectiveness of the SOC and NASA's computer security incident detection and handling program.

IT Security Challenges in Moving to Cloud Computing

Looking to the future, like other Federal agencies NASA will face challenges as it seeks to leverage the benefits of cloud computing. Cloud computing is an emerging form of delivering computing services by providing users with scalable, on-demand IT capabilities over the Internet. Examples of cloud computing include web-based e-mail applications and common business applications accessed online through a browser instead of provided by an Agency data center. Cloud computing offers the potential for significant cost savings through faster deployment of computing resources, a decreased need to buy hardware or build data centers, and enhanced collaboration capabilities. However, along with these benefits are potential risks such as when the provider of cloud-computing services experiences infrastructure failure or loss of customer data. The need to effectively secure Agency data stored in the cloud has emerged as the major challenge to Federal agencies reaping the substantial benefits cloud computing offers. In addition, as Federal agencies move more toward cloud computing, it is imperative that Inspectors General across the Government retain access to Agency information maintained by cloud-computing providers.

In conclusion, I note that overall the OIG and NASA's Office of the CIO (OCIO) have worked well together to improve NASA's IT security. Of the 69 recommendations for improvement we made in our IT audit reports over the last 5 years, 51 have been closed after full implementation by the Agency. NASA continues to work toward implementation of the remaining 18, most of which stem from our more recent work. In addition, the OCIO has invited OIG staff to speak at various Agency training sessions such as the annual OCIO IT summit and Agency-wide IT security forums.

The final part of my statement summarizes the OIG's major IT audit reports and significant computer intrusion investigations over the last several years.

OIG IT-Related Audit Reports

NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems (December 5, 2011)

The OIG evaluated NASA's efforts to transition to a system that continuously monitors components connected to NASA's IT systems and focuses on critical controls that protect against the most common IT security incidents NASA has experienced. We found that NASA has not yet successfully made this transition and faces significant challenges in doing so. In particular, we found that 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. The Agency concurred with our recommendations to maintain an accurate account of security data for all NASA systems components, expedite development of content and metrics for applying secure baseline configuration settings to IT components, and institute credentialed vulnerability scanning Agency-wide. All report recommendations remain open. Overall, 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, 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.

Federal Information Security Management Act: Fiscal Year 2011 Evaluation (October 17, 2011)

This annual report, submitted as a memorandum from the Inspector General to the NASA Administrator, provides the Office of Management and Budget with our independent assessment of NASA's IT security posture. For FY 2011, we adopted a risk-based approach in which we selected 25 high- and moderate-impact non-national security Agency systems for review. We reported to OMB that NASA had established programs in each of the 11 required areas of FISMA review – risk management, configuration management, incident response and reporting, security training, plan of action and milestones (POA&M), remote access management, identity and access management, continuous monitoring management, contingency planning, contractor systems, and security capital planning. However, we found that the Agency's programs for risk management, configuration monitoring management, and POA&M need significant improvements because they do not include all required attributes identified by the Department of Homeland Security. Although our audit work identified challenges to and weaknesses in NASA's IT security program, we concluded that the Agency is steadily working to improve its overall IT security posture.

Inadequate Security Practices Expose Key NASA Network to Cyber Attack (March 28, 2011)

In this audit we evaluated how well NASA is protecting its Agency-wide mission computer network from Internet-based attacks. We found that six computer servers associated with IT assets that control NASA spacecraft and contain critical data had vulnerabilities that could allow a remote attacker to take control of or render them unavailable. Moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA operations. We also found network servers that were not securely configured and, as a result, exposed encryption keys, encrypted passwords, and user account information to potential attackers. The deficiencies occurred because NASA had not fully assessed and mitigated risks to the Agency-wide mission network and was slow to establish an IT security oversight program to ensure the network was adequately protected. The Agency concurred with our recommendations to (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. All three recommendations remain open.

Review of the Information Technology Security of [a NASA Computer Network] (May 13, 2010)

We examined the processes for continuously monitoring selected IT security controls on a NASA-wide computer network that supports mission-critical spaceflight and science operations. We found that only 24 percent of applicable computers at the Goddard Space Flight Center were

monitored for critical software patches and only 62 percent were monitored for technical vulnerabilities. Monitoring computers for vulnerabilities and timely patching is widely recognized as critical to maintaining the security of IT systems. Moreover, during detailed control testing we identified several high-risk technical vulnerabilities on the system that provides mission support to the Space Shuttle and International Space Station. If exploited, these vulnerabilities could allow a remote intruder to gain control of the system or render it unavailable. The Agency concurred with the report's two recommendations to: (1) designate a NASA Directorate or Center to immediately establish an oversight process to include monitoring of systems for the presence of critical patches and technical vulnerabilities; and (2) review all other Agency mission network IT security programs to determine whether each contains an effective oversight process. Both recommendations remain open.

Significant IT-Related OIG Investigations

- In February 2012, a Romanian national was indicted in the Central District of California for hacking into JPL systems. The U.S. indictment followed convictions in Romania for related criminal activity. This series of intrusions resulted in losses of over $500,000 to the Atmospheric Infrared Sounder (AIRS) Program.

- In January 2012, a 20-year-old Romanian national was arrested by Romanian authorities for unauthorized accesses into numerous systems belonging to NASA, the Pentagon, the Romanian government, and commercial entities. Due to this intrusion, products from a variety of NASA scientific research efforts were inaccessible to the general public for a brief period of time. However, no long-term damage to the underlying programs has been reported.

- In November 2011, JPL IT Security reported suspicious network activity involving Chinese-based IP addresses. Our review disclosed that the intruders had compromised the accounts of the most privileged JPL users, giving the intruders access to most of JPL's networks. The OIG continues to investigate this matter.

- As previously mentioned, the U.S. Attorney's Office for the Southern District of New York announced in November 2011 the indictment of six Estonians and one Russian national who were part of an international fraud scheme that compromised more than 4 million computers worldwide, including 135 NASA systems. To date, authorities have seized more than $15 million in assets from the operation.

- In February 2011, a Texas man pled guilty to wire fraud in Federal court in Minnesota for hacking two NASA systems and a Minnesota-based company's pay and accounting system. Because of the intrusion, more than 3,000 registered users were denied access to oceanographic data supplied by NASA for several days. Direct remediation costs in this case exceeded $66,000.

- In February 2011, a British citizen was sentenced in England to 18 months' imprisonment for his role in the distribution of malware that caused NASA data to be compromised. Approximately 2,000 NASA e-mail users were infected with this malware as part of a worldwide computer fraud scheme.

- As a result of an OIG investigation and lengthy international coordination efforts, a Chinese national was detained in December 2010 by Chinese authorities for violations of Chinese Administrative Law. This case resulted in the first confirmed detention of a Chinese national for hacking activity targeting U.S. Government agencies. Seven NASA systems, many containing export-restricted technical data, were compromised by the Chinese national.

- In March 2009, Italian authorities raided the home of an Italian national suspected of taking part in several unauthorized intrusions into NASA JPL systems. Italian authorities suspect the individual of being a member of a hacker group responsible for an Internet fraud and hacking schemes. The subject is scheduled for trial in March 2012. Two computer systems used to support NASA's Deep Space Network and several Goddard Space Flight Center systems were affected by the intrusions, although NASA officials assured us that no critical space operations were ever at risk.

- Back-to-back OIG investigations of rogue Internet Service Providers (ISPs), specifically "McColo Inc." and "Triple Fiber Networks," resulted in a shutdown of those service providers. These ISPs were identified by NASA OIG and other law enforcement agencies as a major source of child pornography, e-mail spam, stolen credit cards, and malicious software. As an indicator of the scope of the illegal activities hosted by these rogue ISPs, Internet security researchers reported a worldwide reduction in spam of approximately 50 percent shortly after the ISPs were taken offline. Twenty-one NASA systems were compromised as part of the array of criminal activity hosted by the rogue ISPs. The U.S. District Court in the Northern District of California ordered McColo Inc. to pay the Federal Government a $1.08 million civil judgment. The OIG investigation found that 53 NASA systems were affected by the criminal activity sponsored by McColo Inc., but none of the systems were mission critical.

- A Swedish citizen was indicted in 2009 for the theft of Cisco Systems, Inc., proprietary code and numerous intrusions into NASA systems. Swedish and U.S. authorities agreed to an arrangement whereby the subject would be tried in Sweden. The subject was found guilty and a "formal criminal history" was filed by Swedish authorities. The majority of the damages suffered by NASA related to several instances when the Ames Research Center's Super Computing Center was temporarily shutdown to clean up after the intrusions. Losses to NASA were estimated at more than $5 million.

Chairman BROUN. Thank you, Mr. Martin. You were dead on exactly five minutes. I appreciate that, and Ms. Cureton, you were great, too, so I appreciate you all's expediency in getting through this process. I thank you all for your testimony.

Reminding Committee Members that committee rules limit Members' questions to five minutes per round of questions. I am going to defer the normal chair's starting the round of questions. I am going to recognize Ms. Adams because she has a meeting to go to, so Ms. Adams, you are recognized for five minutes.

Mrs. ADAMS. Thank you, Mr. Chairman.

Mr. Martin, you referenced in your testimony a 2010, audit where you discovered only 24 percent of mission network computer were monitored for critical software patches and only 62 percent were monitored for technical vulnerabilities. Additionally, you mentioned that only one percent, again, of NASA's portable devices and laptops are encrypted.

Is this negligence by the CIO's Office, or is there another explanation as to why this is not being done?

Mr. MARTIN. I don't think it is negligence by the Office of the CIO, and you can ask the CIO that question. However, it is disturbing. Certainly the encryption rate of one percent is very disturbing because as we have discussed here NASA's mobile computing devices contain very sensitive information.

Mrs. ADAMS. Right, and your office discovered in December of 2010 that NASA failed to properly sanitize excess Shuttle computers and hard drives and that at least ten had been released to the public with sensitive data on them.

Did you recover any of these improperly-released computers, and what has NASA done to ensure this doesn't happen in the future?

Mr. MARTIN. Again, our auditors during that actually were able, during the conduct of an audit, and again, this was not a criminal investigation but an audit, the auditors caught what was supposed to have been a sanitized hard drive, and we prevented that and gave it back to the agency. This was troubling. There were inconsistent procedures at the four NASA centers that we went to for sanitizing excess Shuttle equipment, and this was very troubling.

Mrs. ADAMS. Ms. Cureton, according to the IG between April, 2009, and April, 2011, NASA reported 48 agency mobile computing devices with sensitive data and even some including export control and a third-party intellectual property on them stolen. How many of these devices were encrypted, and have any of them been recovered?

Ms. CURETON. I am sorry I don't have the specific details about those devices, but one of the things that we have done is work closely with our desktop service provider to make sure that the devices such as the laptops and mobile devices have the appropriate encryption.

I mentioned in my opening statement that we recently awarded our IT Infrastructure Programs, I3P, and the key critical contract and program that needed to do that was awarded in December. We have developed a plan for accelerating our encryption of devices, and we have prioritized encryption of laptop and other mobile devices.

Mrs. ADAMS. How many of the 5,400 attacks against NASA in the last two years have originated from those devices or information that was available on those devices? Do you know?

Ms. CURETON. I don't have the exact number, but generally most of the attacks are sourced through our websites and vulnerabilities through there. With the large number of websites that we do have it creates a large attack surface where attackers can easily get in and exploit things if they are not appropriately protected.

So our biggest risk is the websites, and the mobile devices do not represent a significant amount of risk in terms of what we have seen.

Mrs. ADAMS. Has NASA's relationships with contractors and other third parties been affected by the lack of security by what we are hearing today?

Ms. CURETON. Excuse me? Has it been effective or——

Mrs. ADAMS. Affected.

Ms. CURETON. We work closely with our industry partners. We work through organizations like the American Council of Technology, the Information Advisory Council, and another organization called the Cyberspace Intelligence Association or Cyber Fajitas and Margaritas, and we work through them so we have a safe forum for exchanging information and getting information flowing freely between industry partners about what we can do to jointly protect our common threats.

Mrs. ADAMS. So you are in constant contact and conversation with those contractors and third parties because I would think they would be concerned about their information, intellectual property being stolen.

Ms. CURETON. Yes, and also we are concerned about vulnerabilities that we present to their networks and they present to ours.

Mrs. ADAMS. Thank you. I yield back.

Chairman BROUN. Thank you, Ms. Adams.

Now recognize Mr. Tonko for five minutes.

Mr. TONKO. Thank you, Mr. Chair.

Mr. Martin, you have suggested that NASA may not gain full control of its IT security problems until the CIO's Office has the authority to ensure IT security policies are enforced across the entire agency. Would you please expand on how the CIO's authority is limited and why that raises hurdles to effective cyber security?

Mr. MARTIN. Certainly. I am not sure we used the word authority. I think the CIO under certainly the Clinger-Cohen Act and NASA policies has the authority. She does not have the operational control as I indicated in my opening remarks over the mission networks at NASA, and frankly that is where we are seeing the bulk of the attacks coming from are the mission networks that are in the control of the mission directorates or based at the centers. She doesn't control the funding for those, and Linda can speak to that. She doesn't control the funding, and as we have all seen in Washington, when you don't control the funding, you have a difficult time getting folks' full attention.

Mr. TONKO. Thank you, and Ms. Cureton, to illustrate the limits of your authority, can you share with us just what proportion of NASA's IT budget you directly control?

Ms. CURETON. The fiscal year 2013 requested level is at approximately 1.4 billion. Of that I am allocated a portion of that, and it is 152 million. That allocation is given to me by another directorate, so I am going to get whatever I am allocated from that directorate, and the rest of it is controlled either by CIOs at centers, a relatively small portion of it, and I will say that the center CIOs do report to me, but their budgets report to their center directors. And then the rest of the $1.4 billion budget is controlled by missions and programs.

Mr. TONKO. Interesting. Ms. Cureton, if you were given more authority over the IT budget and over the mission directorates, how would you use that to enhance cybersecurity policies?

Ms. CURETON. I would attempt to consolidate many of our networks. One of the challenges that we do have, especially as it relates to the funding required to implement these safeguards, there are many networks that need to be safeguarded, many doors, many gates to guard. And there needs to be a consolidation of the local area networks that exist at the agency so that safeguarding these networks is a more practical effort.

So I would definitely do that. I would prioritize on addressing the vulnerabilities and risks that exist on our networks and then finally address the proliferation of websites to the extent that it makes it difficult for us to secure our networks. There is a strong need for NASA to have networks and internet technologies to collaborate and share information with our partners, but in looking at some of the innovative abilities, innovative solutions that exist now, there are more modern ways to securely collaborate with partners and still accomplish our mission.

Mr. TONKO. And that ought to be, I would think, a high priority within the operations that you serve.

Ms. CURETON. Correct.

Mr. TONKO. Absent more authority, how can you assure us that you can build a bulletproof cybersecurity program for NASA?

Ms. CURETON. I am committed to work diligently with the goals that I have set before the Administrator. I have a very capable IT security staff, my deputy CIO for IT security. We work closely as we can with missions. We work to build credibility, to communicate, to improve user awareness. We continue to do those things and continue to attempt to make progress in breaking down some of the barriers while closing some of the loopholes that we do have.

Mr. TONKO. Thank you, and Mr. Martin, do you believe cybersecurity can be effectively established at NASA absent consolidation of authority?

Mr. MARTIN. Even with consolidation of authority there needs to be a new mindset and a new way to operate. Again, having control solely over the IT security apparatus for just the institutional side of the house is woefully inadequate to securing NASA's very important information.

Mr. TONKO. Thank you. Thank you very much.

Mr. Chair, I yield back.

Chairman BROUN. Thank you, Mr. Tonko. I yield myself five minutes now.

Last March the NASA IG issued a report that called for NASA to conduct an agency-wide IT risk assessment. In that report the

CIO committed to developing and implementing a strategy for conducting this risk assessment by August 31, 2011.

First, Mr. Martin, what is the status of this effort, and do you know of a firm date where we can expect that.

Mr. MARTIN. I think Ms. Cureton would probably know the exact date.

Chairman BROUN. I am going to ask her that next.

Mr. MARTIN. I believe the date of August, 2011, has slipped, and NASA has asked until I believe November of this year to complete that action.

Chairman BROUN. Okay. Ms. Cureton. What is the status?

Ms. CURETON. Yes. The date has slipped, and we have made a formal request for an extension.

Chairman BROUN. When are we going to have the report, and I mean, the risk assessment done and full accounting for what you are doing to implement that?

Ms. CURETON. June, 2012.

Chairman BROUN. Absolutely, positively June, 2012. We keep slipping past these dates, and this committee would like to know when we can expect that.

Ms. CURETON. I believe that I will make it. I am committed to make that happen. I can't say that there are things that won't happen that cause us to change our priorities, but it is an absolute priority for me, and I am committed to make sure that it happens.

Chairman BROUN. Well, certainly we need to have a way to implement this risk assessment. September of 2010 and December of 2011 the NASA IG issued reports recommending that NASA transition to a continuous monitoring approach for this IT system.

Mr. Martin, what is the status of this effort?

Mr. MARTIN. It is ongoing. I think NASA has made some significant strides. This is a whole new approach to monitoring the security of government systems, and you may be familiar with the FISMA, the Federal Information Security Management Act of a number of years back.

Unfortunately, we have seen in the IG community it devolve into really somewhat of a less effective paper-driven exercise. And so there has been a move that has been promoted by OMB and the Department of Homeland Security to move more toward what is called continuous monitoring a more dynamic security oversight process because the IT systems that you are reviewing are dynamic and ever changing.

So we assess NASA's move from the old static, what we call "snapshot" system, once a year at this moment in time, do you have the policies, do you have the paperwork, as opposed to, "do those policies and paper mean anything, do they work," and moving to a continuous monitoring. NASA has made strides, but as we point out in our audit report, we found a couple significant areas where NASA needs to make significant efforts in order to have an effective continuous monitoring program.

Chairman BROUN. And you have made those recommendations to NASA?

Mr. MARTIN. We absolutely have.

Chairman BROUN. Okay. Ms. Cureton, do you want to answer the question?

Ms. CURETON. We committed to completing the activities, enable that in November, 2012. There are several steps that we need to make, one of them will be to have a more robust asset management program to have situational awareness of the configuration of the networks and the endpoint devices, and we believe that that should be essentially completed in the first quarter fiscal year 2013.

Chairman BROUN. And this is going to be a continuing monitoring process?

Ms. CURETON. Yes.

Chairman BROUN. Okay. In 2011, NASA developed a governance model to streamline IT decision making. What role do the mission directorate senior officials, the subject matter experts that are responsible for mission success, play in the IT security decision making process, Ms. Cureton?

Ms. CURETON. We have governance boards and working groups that have representation from each mission directorate, and we have enterprise architecture boards that have representations from the mission directorates. Our IT management board has representation from a mission directorate in terms of a mission directorate CIO. At the senior levels there is a mission support council that consists of myself, the assistant associate administrator for mission support, the associate administrator, the deputy associate administrator, and the CFO, and then report to the executive council, which consists of the administrator, the deputy administrator, and some of the others that I mentioned earlier.

The representation from the directors and the centers would come from the administrator, the deputy administrator, and also through the associate administrator.

Chairman BROUN. Okay. My time has expired.

I will now yield five minutes to Mr. Tonko.

Mr. TONKO. Thank you, Mr. Chair.

This is a question I will pose to both of our witnesses. What do you see as the biggest IT security threat facing NASA today? Would it be foreign governments, 16-year-old children in the United States, cyber criminals, groups like anonymous—is there any way for either of you to quantify the IT threats that NASA faces and what the actual impact of these threats have been to NASA?

Mr. MARTIN. After you.

Ms. CURETON. Thank you.

Mr. MARTIN. You are welcome.

Ms. CURETON. In saying big, big would be quantified as like the largest number of attacks or perhaps it could be a smaller number of attacks but a bigger impact. So it is hard to really say what is big, but certainly the impact is the advanced persistent threat in terms of what it means to our Nation's security and our Nation's future.

But then big in terms of numbers tends to be more along the criminal side because there is opportunities to get financial information, personal identification from employees that could financially benefit hackers. And probably by numbers some of them appear like that, but by impact it is probably more along the lines of the advanced persistent threat that is probably attributable to nation states or organized crime.

Mr. TONKO. Uh-huh. Mr. Martin.

Mr. MARTIN. Thank you. I don't disagree with that assessment at all, but we have seen the whole gamut. We have seen the Swedish teenager bringing down NASA's super computer at Ames causing upwards of $6 million in damage for remediation. We have seen the criminal, sophisticated criminal enterprises. As we mentioned, we had six arrests in Estonia working with the Estonian National Police. That was primarily a financially-derived initiative, but once you are in the NASA systems, even if your goal is to redirect internet traffic, you know, for what they called internet fraud, click fraud, or more of an advertising scam, you have access into NASA's systems. You can sell that access to other folks who are after NASA-sensitive information.

So it really runs the gamut.

Mr. TONKO. Thank you, and all NASA IT components are supposed to be identified in a database established by the CIO's Office, all the IT security enterprise data warehouse. The IG's audit found, I believe, that out of 289 NASA IT components they reviewed only 175 that were included in that database. The IG found that NASA's failure to maintain a complete, up-to-date inventory of IT components significantly diminishes its ability to develop and maintain a continuous monitoring program.

Where do we take this from there?

Ms. CURETON. So the first step would be to increase the number of assets that we do monitor, and that would be by increasing and improving our asset management program, and once we do that we are able to determine the configuration of those assets and maintain the right inventory of baseline configuration levels.

And then finally, make sure that we are able to monitor each component of the network to look for intrusions and identify them as soon as possible.

Mr. TONKO. Thank you, and many of the issues we are talking about here today have been endemic at NASA for at least the past decade. Can both of you please address that issue and tell us why you believe these IT security issues at NASA continue to occur, why it appears NASA management has had such a difficult time reigning in these issues and managing its IT security structure in a better format.

Ms. CURETON. Me first? Okay. The most difficult part of addressing this is culture. We spend a lot of time focused in the technology part of it, which is really difficult, too, but culture is probably the number one impediment.

IT security is considered a CIO's problem, but IT security is basically a mission problem. The information that the actors are looking for is mission information. They are looking for the information to get some advantage in terms of whatever the motives they have would dictate.

And being more focused on the institutional side doesn't really protect where the biggest risk is, but being able to persuade the mission, the culture of the mission that they should include a culture of looking at IT security issues is a big challenge admittedly.

And so as with working through any culture, it takes a long time to build the credibility to provide the impetus to change, to get crit-

ical mass that says, yes, we are going to do it and go forward, and so that process takes a long time, and it has taken a long time.

Mr. TONKO. Anything?

Mr. MARTIN. I think I would agree with that. I think if the goal is to have IT security at NASA more centralized in the CIO's Office, she would need a much larger stick than she currently has now.

Mr. TONKO. Thank you, and I have exceeded my time, so, Mr. Chair, I yield back.

Chairman BROUN. Thank you, Mr. Tonko. I yield myself five minutes.

The "Wall Street Journal" article on November 17, 2011, titled, "China, U.S. Use Same Tracking Base," states that the Chinese entity, China satellite launch and tracking control general, part of PLA's General Armament Department, leases a ground station in Dongara, Western Australia that is run by a Swedish state-owned company called Swedish Space Corp SSC and a U.S. subsidiary that supports U.S. Air Force space surveillance satellites and NASA.

According to a spokesman for Australia's Department of Innovation, Industry, Science, and Research, "Australia did not consult the U.S. on the establishment of the SSC facilities or its customers."

Ms. Cureton, what insight does NASA have into the information security measures employed at foreign satellite ground stations, and do these foreign sites have a multinational presence present unique—do they present a unique challenge to NASA IT security?

Ms. CURETON. Well, obviously we have to work within the constraints of what state and local authorities are there, but we do protect the nodes of our network that exist at foreign locations. I can't speak specifically to the article that you quote, but I will say that we do take the proper security precautions at foreign locations.

Chairman BROUN. That seems just to be kind of a roundabout way of losing our security. I hope you all look at the presence that these do present, because I think it does present a unique challenge to your all's security.

The U.S. China Economic Security Review Commission issued an annual report last November that indicated that the Terra and Landsat-7 satellites experiences interference apparently consistent with cyber activities against their command and control systems.

Ms. Cureton, who is currently responsible for ensuring data integrity and security for NASA satellite operations? Is it the CIO or mission directorates?

Ms. CURETON. It is the mission directorates.

Chairman BROUN. How do we make sure that they stay secure? Do they stay there, or do we come back to your office or how do—tell us what you would recommend?

Ms. CURETON. I believe that the mission directorates need to own the responsibility of security for their assets. One of the challenges is that I own the responsibility of securing other people's assets, and I own the responsibility of making them a priority according to somebody else's priority. So once the responsibility of securing mission networks and assets in this case properly resides with the

proper management authority, I think we would see better responses.

Chairman BROUN. You would see some better responses across the board as far as I am concerned.

What insight does the CIO have into contractor compliance with NASA IT security standards, and who is responsible for providing contractor information and security oversight, Ms. Cureton?

Ms. CURETON. The responsibility would go to the owner of the contract. So if it is in the mission directorate, that is where it would be.

Chairman BROUN. Okay. Mr. Martin, do you have any suggestions or thoughts?

Mr. MARTIN. I think what we do is we audit and we investigate. Because I think this is the fundamental issue facing IT security at NASA: are we going to have a CIO's Office and what structure would best implement a strong security function at NASA, because we have discussed the limited authority that she has over the institutional side of the house as opposed to the mission side of the house.

So we have opened an audit that is going to look at the governing structure that NASA currently employs in its CIO Office, vis-&-vis its mission directorates to try to find where that balance, where the best balance of authority and responsibility would be.

Chairman BROUN. When will that audit be available for us?

Mr. MARTIN. We have just begun it. I would think that we are probably looking nine months down the road.

Chairman BROUN. Well, please get it to us as quickly as you get it. This committee is very interested in hearing that.

NASA has conflicting priorities when it comes to information management. On one hand it has to protect sensitive information associated with dual use, proprietary data from release, but on the other hand it has to facilitate scientific collaboration which requires open access and transparency.

Ms. Cureton, how does the CIO manage these competing cultural priorities?

Ms. CURETON. One of the key enablers of this is with our I3P Infrastructure Program. One of the contracts awarded was to SAIC to manage networks. We have many networks at NASA. We have wide area networks, and we have many, many local area networks. So the network service provider will be moving through the agency and assuming operational responsibility over existing networks. That will take some work in terms of working with mission directorates and looking at responsibilities where they are separated and where they are joint. And then once we do that then we are able to have an awareness of what is out there.

Chairman BROUN. Thank you, Ms. Cureton and Mr. Martin. I thank you all for you all's testimonies today. This is a huge issue. I see a tremendous vulnerability for a very sensitive underbelly of our own economic security as well as potential defense security through NASA. As I have stated before to both of you all, cybersecurity is extremely important to me as an individual, and I think it is important to Mr. Tonko and all of us here on this committee.

I hope that we can find some way to make sure that we have better cybersecurity, IT security within the Department, and I am looking forward to working with both of you as we go forward and helping to develop a better security infrastructure within NASA. You all have been great.

The Members of this Subcommittee may have additional questions for you all to answer, and we will ask you to respond to those in writing. In fact, I have a number myself that I will submit to you all, and I am sure all of us will probably do so. The record will remain open for two weeks for additional comments from Members.

The witnesses are excused. I thank you all very much, and the hearing is now adjourned.

[Whereupon, at 3:21 p.m., the Subcommittee was adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ms. Linda Y. Cureton, Chief Information Officer, NASA

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

Reply to Attn of:
OLIA/2012-00223:MDC:eel

May 15, 2012

The Honorable Paul Broun
Chairman
Subcommittee on Investigation and Oversight
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Broun:

Enclosed are the responses to written questions submitted by you, resulting from the February 29, 2012, hearing at which Linda Cureton testified regarding "*NASA Cybersecurity: An Examination of the Agency's Information Security.*" This information completes the material requested during this hearing.

Sincerely,

Seth Statler

L. Seth Statler
Associate Administrator
for Legislative and Intergovernmental Affairs

Enclosures

SUBCOMMITEE ON INVESTIGATIONS AND OVERSIGHT
HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Questions for the Record

"NASA Cyber Security: An Examination of the Agency' Information Security"

Questions for Ms. Linda Cureton,
Chief Information Officer, National Aeronautics and Space Administration

Questions submitted by The Honorable Dr. Paul Broun, Chairman

1. What are the greatest threats facing NASA IT Security?

Answer: The greatest threats facing NASA IT Security (in no particular order) are:

- IT Governance complexities (fragmented enterprise; no direct authority);
- Difficulty in maintaining a secure posture in a diverse physical environment (multiple operating systems, platforms, mobile devices, etc.);
- Lack of enterprise visibility into assets, system configuration, network traffic and patch status in a fragmented environment;
- Well-resourced, motivated and skilled adversaries and attackers that view NASA as an enticing target;
- Poor execution of security practices by individuals, organizational entities, contractors, and service providers.

a. What is NASA doing to address those threats?

Answer: Threats and cyber attacks are a constant factor to consider as NASA manages its enterprise infrastructure. NASA is taking prudent steps to improve the security posture of the Agency networks and applications:

- NASA is focusing enterprise IT Security assets on the greatest threats – hackers, nation-states, foreign intelligence services, malware, and web applications.
- NASA is working with the owners of IT Systems to ensure asset data, system configuration/patch data, and network traffic is available for correlation and examination to continuously assess the security posture of the enterprise.
- NASA is tracking the campaigns of attackers based on collective attack methods. Analysis and intelligence will provide data to mitigate the spread of future incidents and implement a prevention method.
- NASA is working with external sources, both public and private, on the sharing of threat and intelligence information focused on its mission space.
- While the NASA Office of the CIO (OCIO) doesn't directly control or manage mission systems, the OCIO is actively engaging the Mission Directorates through the governance process to participate in IT Management Board and IT Security Advisory Board activities. In addition, the OCIO is working to gain access to Mission Directorate systems to perform vulnerability scans, asset discovery, and patch management activities.

- NASA is exploring innovative solutions that can provide collaborative web services to NASA scientists and engineers.

2. IT Security funding is often bundled with mission funding, which you have limited visibility into. Can you provide a better estimate of what NASA spends protecting its systems overall?

Answer: 5.7 percent ($82.2M) of the Agency's $1.4B IT Budget (NASA FY 2013 President's budget submission) is allotted for IT Security. The CIO directly controls $15M of that $82.2M.

NASA IT and IT Security Funding ($M)*				
	FY10	FY11	FY12 Estimate	FY13 President's Budget
Agency Budget	18,724.3	18,448.0	17,770.0	17,711.4
Agency IT Budget	2,070.0	1,686.9	1,442.1	1,440.2
IT Security Budget	72.5	88.7	86.2	82.2
IT Security Budget as a % of the Agency IT Budget	3.5%	5.2%	5.9%	5.7%

*Comparative estimate of OMB Congressional and Annual OMB Exhibit 53 submissions

3. Given your limited insight into the Mission Directorates, how do you currently work with them to ensure that adequate security measures are undertaken to safeguard their networks and protect mission operations?

Answer: The OCIO has requested participation from the Mission Directorates in NASA's IT Security Advisory Board, where Agency information security professionals collaborate on solving the IT Security issues across the enterprise. Each Mission Directorate manages risk within their operational boundary. To improve the collective effort to mitigate risk across the enterprise, the OCIO is working with the Mission Directorates; to ensure that NASA's enterprise IT Security tools are deployed to monitor Internet-connected devices.

The OCIO publishes well defined polices, standards, and procedures requiring all IT assets meet specific security principles. The OCIO also publishes several baselines and

standards for hardware (i.e., Federal Desktop Computer Checklist (FDCC - replaced by the United States Government Computing Baseline - USGCB), Center for Internet Security (CIS) benchmarks, and other computer and server Operating System baselines) and software (i.e., Internet Explorer, Adobe, Microsoft Office, etc.) configurations for Centers and Missions to follow. NASA also requires testing of security controls in accordance with the systems risk profile.

The OCIO is monitoring the networks the OCIO has access to for known hostile activity. NASA is sharing and receiving threat information related to NASA's domain that is improving the Agency's ability to manage the vulnerabilities on the Agency's networks.

4. What information does the Systems Operations Center (SOC) have access to?

Answer: The SOC has access to Agency enterprise institutional/administrative network traffic via Intrusion Detection Systems and packet capture devices that include:

- Network logs, such as firewalls and Domain Naming Servers;
- System asset data, patch status, vulnerability status, and limited anti-virus data; and
- US-CERT threat reports.

a. Is it simply enterprise systems, or do they have access to Mission Directorates systems?

Answer:

- The SOC's information is collected from the Agency's institutional/administrative systems.
- In addition, the SOC collects and analyzes IT Security incidents when these incidents are reported by mission IT security personnel through the SOC's Incident Management System.
- The SOC has limited access to mission networks through a limited number of Intrusion Detection Systems placed on those networks.

5. Now that the Security Operations Center has been operational for a few years, what lessons have you learned and what are your future plans to enhance or modify the capabilities at the SOC.

Answer: A few of the lessons learned by the NASA SOC after being operational for a few years are:

- The SOC needs to improve its operational visibility and situational awareness relative to network monitoring, system assets, system vulnerabilities, system patch and configuration status, and enterprise coverage.
- Log data acquired and analyzed in near real-time is a critical element toward reducing the damage caused by adversaries. Reviewing log information enables the SOC to provide Centers and Programs with recommended actions to mitigate and possibly prevent repeats of events.

The future plans for the SOC include improved efficiency through a proactive engagement strategy to better prevent, protect against, and predict attacks by:

- Developing a working partnership with Agency IT service providers to proactively block or re-direct hostile attacks.
- Improving the collection and analysis of data from external sources.
- Improving threat data delivery to Agency stakeholders.
- Expanding network monitoring to include the Mission Network.
- Instituting a means to research, develop and deploy a distributed intelligence framework.
- Enhancing SOC capabilities by continuously evolving services to improve defense of the IT infrastructure.

6. What is the greater threat to NASA information security – outside network penetrations, or internal leaks and spillage?

Answer: The greater threat to NASA is from external penetrations.

a. Does your current budget similarly prioritize these threats?

Answer: The current budget sets network boundary protection and network monitoring as a priority.

7. Based on the observed intrusions, can you identify the motivations for attacking NASA systems –theft, espionage, sabotage, and vandalism?

a. How do these intrusion types rank?

Answer: From the perspective of the impact to the Agency, NASA would rank the intrusions in the following order:

1) Espionage
2) Theft
3) Vandalism
4) Sabotage

- *Espionage is considered to be NASA information that is obtained via overt, covert, or clandestine activity with intent, or reason to believe, that the information will be used to the injury the United States, or to the advantage of a foreign nation.*
- *Theft is considered to be an unlawful taking (as by embezzlement or burglary) of NASA property or information.*
- *Vandalism is considered to be a willful or malicious destruction or defacement of property, including NASA websites.*
- *Sabotage is considered an act with intent to injure, interfere with, or obstruct the mission of NASA by willfully injuring or destroying, or attempting to injure or destroy, any NASA mission or materiel, premises, utilities, including human, or information resources.*

8. How effective are you in assessing compliance with security configuration baselines within Mission Directorates? Do the FISMA reporting requirements help you better understand the security posture at the Mission Directorates?

Answer: The OCIO has limited authority to impose cyber security solutions across Mission Directorates. This includes limited visibility into security configuration baselines across a wide array of operating systems, many of which may be obsolete and/or specifically configured for Mission requirements.

Most Mission Directorate sensitive information is stored in 'air gapped' network environments. In most cases, the OCIO does not have access to these network environments in order to assess compliance.

The OCIO uses a set of automated tools to prepare the data for the Federal Information Security Management Act (FISMA) report. The use of these tools assists the OCIO in understanding the security posture of the Mission Directorates.

9. With government-wide efforts to move information to the "Cloud," how will NASA ensure that information is appropriately secured - particularly when it is experiencing so many challenges already?

Answer: To ensure the security posture of Cloud service providers is properly understood, a new NASA Agency team has been tasked with developing the process that will be used to authorize NASA clouds providers by leveraging the work done through the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. (Members of the NASA team were also members of the Cloud Computing Security Working Group that advised GSA on Security Control Parsing for the FedRAMP approach.) The team will create a process to understand exactly which security controls are being addressed by a Cloud provider and which security controls will remain the responsibility of NASA. The team will subsequently execute the process developed to authorize new Cloud providers for use by NASA. The process findings will also be used to ensure each new Cloud provider's services interface and integrate as needed with existing NASA security processes and mechanisms. Additionally, the findings will be used to create Cloud provider-specific security guidance for NASA employees.

10. How long would you estimate it would take the Office of the CIO to close out all of the 18 open NASA IG recommendations?

Answer: The estimate based upon current resources to close out all of the 18 open NASA IG recommendations is June 2013.

11. Shortly after the hearing, press reports indicated that Administrator Bolden circulated a memo outlining steps to address IT security weaknesses. Please provide a copy of that memo to the committee.

Answer: A copy of the memo is attached

12. After the hearing, Administrator Bolden appeared before another Committee and addressed many of the issues brought to light at our hearing. Specifically, Administrator Bolden indicated that the theft of a laptop containing algorithms used to command and control the International Space Station never put the orbiting laboratory at risk because "[t]hey would still have to get through another set of firewalls at the Johnson Space Center because everything that goes to the International Space Station, as it did with the shuttle, is encrypted prior to transmission..." During our hearing, the NASA IG stated:

> *"In FY 2011, NASA reported it was the victim of 47 advanced persistent threats (APT) attacks, 13 of which successfully compromised Agency computers. In one of the successful attacks, intruders stole user credentials for more than 150 NASA employees - credentials that could have been used to gain unauthorized access to NASA systems. Our ongoing investigation of another such attack at the Jet Propulsion Laboratory (JPL) involving Chinese-based Internet protocol (IP) addresses has confirmed that the intruders gained full access to key JPL systems and sensitive user accounts. With full system access the intruders could: (1) modify, copy, or delete sensitive files; (2) add, modify, or delete user accounts for mission-critical JPL systems; (3) upload hacking tools to steal user credentials and compromise other NASA systems; and (4) modify system logs to conceal their actions. In other words, the attackers had full functional control over these networks."*

The IG also stated, "Moreover, even after NASA fixes the vulnerability that permitted the [ATP] attack to succeed, the attacker may covertly maintain a foothold inside NASA's system for future exploits."

I hope that NASA did not dismiss the risk simply because ISS control algorithms are encrypted and transmitted by a NASA center. I understand that JPL is not a NASA center (and presents unique IT security challenges itself), but the JPL intrusion demonstrates that NASA facilities are not immune to attack. Similarly, the U.S. China Economic and Security Review Commission recently noted in its annual report to Congress, the Terra and Landsat-7 satellites "have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems." Although the Commission did not attribute this interference to any specific actor, it does demonstrate that encrypted transmissions do not guarantee the safety of command and control systems.

While it is reassuring that NASA believes that the ISS was never at risk, I am interested in understanding what lead NASA to this conclusion.

a. Please provide any and all analysis that demonstrates that the March 2011 theft of an unencrypted NASA notebook computer, which resulted in the loss of the algorithms used to command and control the International Space Station, was never a risk to mission operations or safety.

Answer: The Johnson Space Center (JSC) Mission Operations Directorate (MOD) performed a review of the file contents of the stolen laptop and determined there were two items of interest:

1. Copies of displays used on the Space Station's Portable Computer System (PCS). The displays are more than just a screenshot, but in an Extensible Markup Language (XML) format that is both human readable and machine readable, independent of computer platform (windows PC, Macintosh, or UNIX). For comparison purposes, the latest versions of Microsoft Word use a version of XML. These displays were on the laptop as needed for task assignments. These displays on a standard laptop are non-functional displays and cannot receive telemetry from the ISS and/or send commands to the ISS.
2. Although not actual software, the Software Requirements Specifications for the Command and Control Software was another document found on the stolen laptop. This document contains specification on the software and is used to understand how the software works and interfaces with other software on the ISS.

Next, the MOD evaluated the risk to the International Space Station due to the loss and concluded the following:

- The stolen laptop was a general purpose, office laptop used primarily for reading email, reviewing documents, and managing task assignments. The laptop was not a specialized laptop to support mission operations.
- Although the laptop had software specifications, it did not contain actual software code that could be used to command and control the ISS.
- By design, mission systems do not permit commanding to a spacecraft from any office-IT device (laptop, desktop, personal digital assistant (PDA), etc.) that is not physically located inside the mission systems firewall at Johnson Space Center (JSC) or a small number of other NASA locations that connect directly to the JSC mission Local Area Network (LAN).
- Even with the correct network connection, several layers of credentials in several different network security systems are required.
- Under no circumstance is a remotely connected office-IT device permitted command access.

b. Was this determination made by the CIO or the Human Exploration and Operations Mission Directorate?

Answer: The determination that the International Space Station was not at risk was made by JSC's Mission Operations Directorate with concurrence from the Human Exploration and Operations Mission Directorate (HEOMD) and not by the NASA CIO.

Once the Incident Response Team identified what specific data was lost and identified the data as belonging to the Mission Operations Directorate (MOD) completed an assessment regarding the risk to the International Space Station resulting from the exposure of this information. It was determined that the technical information contained on the laptop posed no risk of sabotage, terrorism, hacking or malicious interference by any entity to any person, vehicle, agency or company.

a. Was the Science Mission Directorate (SMD) consulted prior to this determination?

Answer: Due to the distinct difference between the operational and scientific missions of the Human Exploration and Operations Mission Directorate (HEOMD) and Science Mission Directorate (SMD), in addition to the type of data lost – data related to operational requirements and planning, SMD was not consulted in determining the risk to the International Space Station.

b. Were the Terra and Landsat -7 satellites ever at risk?

Answer: There were attempts made to establish command of the Terra spacecraft through radio frequency communications. None was successful. This was not a cyber-attack but a command-link intrusion attempt over radio frequency communications. US Space Command and associated organizations were consulted, and found no evidence of NASA IT infrastructure being used in the command-link intrusion attempts.

NASA provides support to the United States Geological Survey (USGS) for the Landsat-7 spacecraft; USGS is responsible for the Landsat-7 spacecraft and associated risk.

13. At the hearing, you indicated that the Mission Directorates are responsible for IT security of their operations. Who is responsible for ensuring that the Mission Directorates comply with Agency IT security directives? Does your office have the appropriate expertise to evaluate threats to the Mission Directorate operations?

Answer: The CIO is responsible for ensuring compliance with NASA and Federal IT security program requirements across the enterprise and in advising senior NASA officials of their associated responsibilities. The OCIO provides governance, and compliance oversight of the Mission Directorates; provides security services for Center and Mission use; and, provides security practices, standards, and guidelines for the Agency. The Mission Directorates are responsible for the application of OCIO policies, procedures, processes, and guidelines as they apply to government-wide regulations and NASA policy. In order to ensure an enterprise wide approach to evaluating threats and risks, OCIO is completing a comprehensive Risk Management Framework (RMF) which will include mission activities.

14. On March 5, 2012, a NASA laptop computer containing sensitive Personally Identifiable Information (PII) was stolen from a NASA KSC employee.

NPR 1382.1 states that "[a]ny PII on mobile computers/devices shall, at a minimum, be encrypted by users with Entrust or native encryption in Microsoft and Apple operating systems or any other NASA CIO-approved encryption solution. It also states that "[w]hen any mobile storage device contains PII, users shall label the device, at a minimum, with 'NASA Privacy Information; Protect Accordingly.'" Further, NPR 1382.1 states that "Employees shall only remove PII from NASA premises or download and store PII remotely under conditions prescribed in NPR 1600.1"

NPR 1600.1 states that "Laptop computers and other media containing SBU information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with NPR 2810.1."

NPR 2810.1 states that the Center CISO shall "[e]nsure that portable and removable digital media devises are guarded using encryption solutions which are compliant with federal encryption algorithm standards and NIST guidance, and are in accordance with NASA requirements regarding the protection of sensitive information. NPR 2810.1 also states that "[t]he NASA user shall mitigate the risks of data loss by securing and protecting media under their control, and the information contained on/within those devices, through the use of encryption, access restrictions, and/or sanitation."

a. Was the laptop in question encrypted?

Answer: No, the laptop in question was not encrypted.

b. Did that encryption satisfy the requirements in NPR 2810.1 and NPR 1382.1?

Answer: No, the laptop in question was not encrypted, and therefore did not satisfy the requirements in NPR 2810.1 and NPR 1382.1.

c. Was the laptop in question appropriately labeled as outlined in NPR 1382.1?

Answer: No, the laptop in question was not labeled as required in NPR 1382.1.

d. Was the laptop in question removed from NASA premises under conditions prescribed by NPR 1382.1, NPR 1600.1, NPR 2810.1?

Answer: No. Although the employee has an active Entrust PKI account, which gives the ability to encrypt, Entrust was not used to protect the PII information stored on the stolen laptop.

The OCIO has a plan to implement a Data-At-Rest (DAR) solution to protect the entire hard drive of a laptop.

Additionally, the stolen laptop was not appropriately stored and protected – as the employee left the laptop in an unlocked, car parked in the driveway of her house.

e. Are you, the Center Chief of Security, or the Assistant Administrator of the Office of Protective Services responsible for ensuring the implementation of media protection security protocols?

Answer: OCIO and Center CIO's work together to establish the policy and implementation of media protection security protocols related to Information Technology systems.

f. Who is responsible for ensuring the protection of Agency PII?

Answer: The NASA CIO is tasked with the overall responsibility of protecting Agency PII and other sensitive information in collaboration with all of NASA's employees, contractors and volunteers.

Message from the Administrator

The Importance of Securing NASA Laptops, iPads, and Smart Phones

By now, many of you have either read or heard about the most recent IG report on alleged deficiencies in how we handle and control IT portable devices issued to our NASA employees. I take the issue of IT security very seriously – both for our equipment and the information stored on it. Information security maintains the integrity of our programs, and ultimately keeps our missions and people safe.

The nature of NASA work makes laptops and other portable IT devices important to our program delivery. Many employees use these devices outside the standard office environment during travel and when routine work occurs outside of an office. Therefore, the risk level is increased, and our need to protect the equipment, and the information stored on that equipment is even more elevated than ever before.

We have made significant progress to better protect the agency's IT systems and are in the process of implementing the recommendations made by the NASA Inspector General in this area.

While the cost to replace lost or stolen IT devices is a concern, the real damage is done through the loss of NASA program information, including personal and other sensitive information. Losses such as these have the potential to harm NASA's credibility, can diminish the public trust, and have adverse effects on our ability to deliver and manage agency programs.

Information security is not the sole responsibility of a few individuals or offices at NASA; it is critical that every member of the NASA team take appropriate steps to keep sensitive information safe and protect equipment from theft.

I'm asking every NASA employee today to review the IT policies set forth by the Chief Information Officer, identify areas that require improvement in accordance with those policies, and work with your supervisor and IT team to remedy the situation so that the equipment and information you are using meets the prescribed requirements for security. As a best practice for protecting and safeguarding laptops and other portable IT devices and sensitive data they may contain, I ask that you review and follow the below policies and directives:

- NPD 4200.1E, Equipment Management
  http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=4200&s=1E
- NPR 2810.1A, Security of Information Technology
  http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=2810&s=1A
- NID 1600.55, Sensitive But Unclassified Information (SBU)
  http://nodis3.gsfc.nasa.gov/OPD_Docs/NID_1600_55_.pdf

- NPR 1382.1, NASA Privacy Procedural Requirements
  http://nodis3.gsfc.nasa.gov/displayDir.cfm?
  Internal_ID=N_PR_1382_0001_&page_name=Chapter1

Policies are just a guideline for action. It is essential that each of us not only familiarizes ourselves with the relevant IT security policies, but also adopts them into our daily practice – to make them an integral part of our habitual behavior and personal discipline.

As a reminder, any equipment losses must be reported to the NASA Security Operations Center Hotline at 1-877-627-2732 or via email at soc@nasa.gov within 1 hour of occurrence.

If you have any questions or concerns, please contact Valarie Burks, deputy chief information officer for IT security, at valarie.j.burks@nasa.gov or 202-358-3716.

The NASA CIO's office has set up a mailbox at Agency-IT-Security@mail.nasa.gov where you can send specific questions, suggestions or recommendations about how NASA can continue to improve its information security.

Thank you for all the work you do every day to help us achieve NASA's mission.

Charlie B.

ANSWERS TO POST-HEARING QUESTIONS

Responses by The Honorable Paul K. Martin, Inspector General, NASA

Subcommittee on Investigations and Oversight
Committee on Science, Space, and Technology

Questions for the Record

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

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

Paul K. Martin
Inspector General, National Aeronautics and Space Administration

Questions submitted by Dr. Paul Broun, Chairman

1. What are the greatest threats facing NASA IT Security?

Answer: The greatest threat facing NASA information technology (IT) security is a type of sophisticated cyber attack known as an Advanced Persistent Threat (APT), which targets sensitive data on the Agency's computer networks. Although NASA has implemented processes and technologies such as firewalls and signature-based intrusion detection systems for preventing and detecting common forms of cyber attacks, these measures are not effective against APTs. For example, in fiscal year (FY) 2011 only one of the 47 APT-type cyber attacks NASA reported was prevented by NASA's perimeter defenses. A review of the 47 APTs shows that e-mails to NASA employees containing malicious content (known as phishing e-mails), accounted for 40 of 47 (85 percent) of the reported APTs. Phishing e-mails are able to pass through NASA's firewalls and remain undetected by Agency intrusion detection systems because e-mails are considered normal traffic and a link or file inside an e-mail is unlikely to trigger a security alert. Once inside NASA's network, the attacker can search the Agency's computer systems for sensitive data to steal and maintain a foothold for future intrusion exploits.

A second IT security threat facing NASA is the lack of progress to date in the Agency's efforts to encrypt its mobile computing devices. As described in our written statement, as of February 1, 2012, only 1 percent of NASA's notebook computers were encrypted compared to a government-wide average of 54 percent. Until NASA successfully addresses this situation the likelihood of future release of sensitive data remains high.

1a. What is NASA doing to address those threats?

Answer: In an effort to improve NASA's capability to thwart APT-type attacks, the Agency initiated a pilot project in the Fall of 2010 to monitor employee e-mail for potentially malicious content. This new initiative prevented 28 of 47 (60%) of the APTs NASA reported in FY 2011. Other measures such as re-directing persistent cyber attacks and enlisting the assistance of outside agencies helped prevent six other APT attacks in 2011. NASA's success in defending against APTs depends on the Agency's ability to: (1) attract and retain highly-

skilled and experienced technical staff; (2) create, customize, and deploy network monitoring and active defense tools; and (3) obtain senior management support and the necessary resources to adequately protect NASA's computer networks.

2. **What is a greater threat to NASA information security - outside network penetrations, or internal leaks and spillage?**

   Answer: Outside network penetrations, especially sophisticated cyber attacks that may be sponsored by foreign governments. As mentioned previously, a lesser but still significant threat is NASA's slow pace of encrypting its mobile computing devices.

3. **Based on the observed intrusions, can you identify the motivations for attacking NASA systems - theft, espionage, sabotage, vandalism?**

   Answer: Our experience leads us to conclude that many of the cyber criminals who have compromised NASA systems were motivated by some form of financial gain. Our investigative efforts continue to disclose new and increasingly elaborate schemes toward this end, including schemes that compromise NASA systems as part of a larger effort to leverage expansive networks of compromised systems across the globe in what are generally referred to as "botnets" (short for robot networks). The criminal elements controlling these botnets use them to conduct advertisement fraud, to store and sell illicit materials, and to facilitate various forms of theft by stealing credit cards and bank account information. That said, we also continue to see sophisticated, well-resourced, and persistent attacks on NASA networks that are suggestive of state-sponsored activity.

3a. How do these intrusion types rank?

   Answer: Regardless of type, all intrusions into NASA systems are cause for concern -- particularly the level of access gained by the attacker. By gaining sufficiently high access to key network infrastructure, attackers are able to initiate harmful activities ranging from data theft to actions that could be disruptive to current or future operations.

4. **Your testimony at the hearing characterized FISMA as an "expensive paperwork exercise that fails to accurately measure an organization's IT security posture." What can the Congress do to make this Act more effective?**

   Answer: We note that recent FISMA guidance has shifted the focus of Agency oversight from periodic assessments and compliance reporting to using tools and techniques to conduct ongoing monitoring of IT security controls. Specifically, ensuring that federal information systems are adequately protected against evolving threats requires mechanisms to establish and then continuously monitor key security controls. Moreover, automating the control monitoring process is essential because of the size, complexity, volatility, and interconnected nature of federal information systems. Congress can make FISMA more effective by adding language stressing the importance of continuous security control monitoring programs for strengthening IT security across the federal government.

5. **With government-wide efforts to move information to the "Cloud," how will NASA ensure that information is appropriately secured - particularly when it is experiencing so many challenges already?**

   Answer: We are currently planning a review of NASA's adoption of cloud-computing technologies. As part of this audit, we will evaluate whether NASA has adequately addressed key IT security issues for safeguarding Agency data moved to the "cloud."

6. **How will the NASA OIG retain access to Agency information maintained by cloud computing providers?**

   Answer: OIG access to Agency information maintained by cloud-computing providers is a key equity that needs to be addressed as the Agency continues to explore contracted cloud-computing as part of its IT management efforts. We are continuing to work this issue with Agency officials.

6a. **Will your office have full access to these data storage facilities that are outside the Agency's infrastructure and merged with other corporate or private data storage servers?**

   Answer: That remains to be seen. We feel strongly that we need full and timely access to Agency records, regardless of the mode and method of storage, to adequately perform OIG oversight functions. We will keep the Congress informed if our discussions with NASA officials to maintain appropriate access to this type of Agency information encounter resistance.