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.