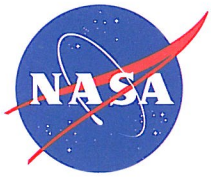
National Aeronautics and
Space Administration

Office of Inspector General
Washington, DC 20546-0001



January 29, 2013

The Honorable Barbara A. Mikulski
Chairwoman
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Richard C. Shelby
Ranking Member
Committee on Appropriations
United States Senate
Washington, DC 20510

Dear Madam Chairwoman and Senator Shelby:

The National Aeronautics and Space Administration (NASA) Authorization Act of 2000 directs the NASA Inspector General to conduct an annual audit to assess the extent to which NASA is complying with Federal export control laws and with the Act's requirement that NASA report to Congress any cooperative agreements between the Agency and China or any Chinese company.[1]

The NASA Office of Inspector General (OIG) last reported to you regarding these issues in January 2012. Since that date, NASA has not entered into any cooperative agreements with China or any Chinese company. During the past year, the OIG conducted two audits examining the Agency's security controls for its information technology (IT) systems, many of which contain data subject to export control laws, and a special review examining NASA's efforts to encrypt the hard drives of the Agency's laptop computers. The results of our special review examining laptop encryption and summaries of the two IT audits are available on the OIG's website at http://oig.nasa.gov/. In addition, the OIG's Office of Investigations closed four investigations during the past year into the potential loss or sale of export-controlled data or technology. Below we summarize this work.

[1] Public Law 106-391, codified at 51 U.S.C. § 30701(a)(3).

Audit Reports

Review of NASA's Computer Security Incident Detection and Handling Capability (IG-12-017, August 7, 2012)

NASA's computer security incident detection and handling program is designed to prevent unauthorized intrusions into Agency networks. In November 2008, NASA consolidated the separate security incident detection and handling programs at its various Centers into a singular Security Operations Center (SOC) in an effort to improve the Agency's ability to detect and respond to cyber-attacks. In this audit, we examined the effectiveness of the SOC.

In general, we found that the SOC has improved NASA's computer security incident handling capability by providing continuous incident detection coverage for all NASA Centers. In addition, NASA implemented an effective information system that enables Agency-wide management and reporting of IT security incidents. However, we found that the SOC does not monitor all of NASA's computer networks and that NASA needs to increase its readiness to combat sophisticated but increasingly common forms of cyber attack known as Advanced Persistent Threats (APTs).[2] To enhance NASA's capability to detect and prevent sophisticated cyber attacks and improve overall SOC availability, the OIG report made three recommendations to the Chief Information Officer (CIO). The CIO concurred with our recommendations and proposed appropriate corrective actions.

Annual Report, "Federal Information Security Management Act: Fiscal Year 2012 Evaluation" (IG-13-001, October 10, 2012, summary)

This annual report, submitted as a memorandum from the Inspector General to the NASA Administrator, provides the OIG's independent assessment of NASA's IT security posture. For fiscal year 2012, the OIG adopted a risk-based approach under which we reviewed a sample of 129 system components monitored by automated tools across NASA and performed a manual review of five mission systems (two Agency internal and three external information systems).

Overall, we found that NASA has established a program to address the challenges in each of the eleven areas designated by the Office of Management and Budget for review – risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, continuous monitoring management, contingency planning, contractor systems, and security capital planning. However, we concluded that IT security will remain a significant challenge for the Agency as it moves from a compliance-focused, "snapshot" approach for measuring the security of its IT systems to using tools and techniques to perform real-time monitoring.

---

[2] APTs are tailored to the systems of the target organization, typically designed to bypass the target's firewalls, intrusion detection system, and other perimeter defenses, and are launched by well-organized and well-funded individuals or entities.

Special Review

NASA's Efforts to Encrypt its Laptop Computers (December 17, 2012)

On October 31, 2012, a laptop containing hundreds of files and e-mails with the Social Security numbers and other forms of personally identifiable information (PII) for more than10,000 current and former NASA employees and contractors was stolen from the vehicle of a NASA Headquarters employee. Although the laptop was password protected, neither the laptop itself nor the individual files were encrypted. As a result of this loss, NASA contracted with a company to provide credit monitoring services to the potentially affected individuals, an action that will cost the Agency between $500,000 and $700,000. In addition, the Agency accelerated its timeline for encrypting all Agency laptops by setting a deadline of December 21, 2012. In this expedited review, we examined NASA's efforts to encrypt its laptops and to meet this deadline.

We found that NASA's full-disk encryption effort had been repeatedly delayed due to slow implementation of its computer services contract, the highly decentralized nature of information technology management at the Agency, and a lack of sufficient internal controls. We also reported the Agency did not have a reliable accounting of the number of laptops in its possession and therefore was not likely to ensure that encryption software was installed on 100 percent of required machines by the deadline. We made five recommendations to the Administrator to help protect NASA's information and prevent unauthorized access to data stored on its laptop computers. As of January 22, 2013, NASA was reporting that 98.9 percent of Agency laptops requiring encryption have been encrypted.

Investigations

Arrest of a Romanian National

An investigation conducted by the OIG, Romanian authorities, the Federal Bureau of Investigation (FBI), and the U.S. Army Criminal Investigation Division led to the arrest in January 2012 of Romanian national Cernaianu Manole Razvan, for illegally accessing numerous NASA, Pentagon, Romanian government, and commercial computer systems. Prior to his arrest, Razvan had eluded law enforcement authorities for many years and had hacked into websites belonging to the British Royal Navy and the European Space Agency, among others.

Former NASA Scientist Sentenced for Espionage, Conspiracy, and Tax Evasion

In March 2012, Stewart Nozette, a former NASA scientist was sentenced in U.S. District Court for the District of Columbia to 13 years in prison for attempted espionage, conspiracy to defraud the United States, and tax evasion. Between January 2000 and February 2006, the scientist entered into agreements with several Government agencies to develop highly advanced technology. He performed some of this research at the U.S. Naval Research Laboratory in Washington, D.C., the Defense Advanced Research Projects Agency in Arlington, Virginia, and NASA Goddard Space Flight Center in

Greenbelt, Maryland. In addition, he admitted providing classified information to a person he believed to be an Israeli intelligence officer, making more than $265,000 in fraudulent reimbursement claims, and willfully evading paying taxes.

Romanian National Admits to Hacking NASA Systems

An investigation by the OIG, in coordination with the Romanian Directorate for Investigating Organized Crime and Terrorism, resulted in the arrest of Romanian national Robert Butyka. Butyka admitted to hacking more than 20 information technology systems at NASA's Jet Propulsion Laboratory and was charged with accessing a computer without authorization; modifying, damaging, and restricting access to data without authorization; and possessing hacking programs.

Foreign Nationals Hijack Computers Worldwide

A joint investigation by the OIG, the FBI, and the Estonian Police and Border Guard Board, with support from numerous private sector and academic partners, resulted in the arrest and indictment of six Estonians and the indictment of one Russian national who remains at-large on multiple charges including wire fraud, computer intrusion, and conspiracy. The suspects are accused of taking part in an international computer crime network that compromised over 4 million computer systems worldwide, including NASA systems that may have contained export controlled data. The crime network is suspected of producing malware that redirected the domain name requests of infected computers to servers it controlled for the purposes of injecting fraudulent advertising banners or malware into the viewer's browser, thereby manipulating Internet advertising and in the process generating at least $14 million in illicit fees.

If you or your staff would like to meet with us to discuss any of the reports or investigations discussed in this letter, please contact me or Renee Juhans, OIG Executive Officer, at (202) 358-1220.

Sincerely,

Paul K. Martin
Inspector General

cc: Charles F. Bolden, Jr.
NASA Administrator

Lori B. Garver
Deputy Administrator

David Radzanowski
Chief of Staff

Linda Cureton
Chief Information Officer

Joseph S. Mahaley
Assistant Administrator, Office of Protective Services

Michael F. O'Brien
Associate Administrator, International and Interagency Relations

Michael Wholley
General Counsel

Identical letter to:

The Honorable John D. Rockefeller, IV
United States Senate

The Honorable John Thune
United States Senate

The Honorable Bill Nelson
United States Senate

The Honorable John Boozman
United States Senate

The Honorable Thomas Carper
United States Senate

The Honorable Tom Coburn
United States Senate

The Honorable Frank Wolf
U.S. House of Representatives

The Honorable Chaka Fattah
U.S. House of Representatives

The Honorable Darrell Issa
U.S. House of Representatives

The Honorable Elijah Cummings
U.S. House of Representatives

The Honorable Lamar Smith
U.S. House of Representatives

The Honorable Eddie Bernice Johnson
U.S. House of Representatives

The Honorable Paul Broun
U.S. House of Representatives

The Honorable Dan Maffei
U.S. House of Representatives

The Honorable Steven Palazzo
U.S. House of Representatives

The Honorable Donna Edwards
U.S. House of Representatives