National Aeronautics and
Space Administration

Office of Inspector General
Washington, DC 20546-0001

January 25, 2012

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 Kay Bailey Hutchison
Ranking Member
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

Dear Madam Chairwoman and Senator Hutchison:

The National Aeronautics and Space Administration 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 regarding 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 2011. Since that date, NASA has not entered into any cooperative agreements with China or any Chinese company. During the past year, the OIG has conducted several audits relating to NASA's compliance with Federal export control laws, including a series of audits examining the Agency's security controls for its information technology systems, many of which contain data subject to export control laws. With one exception, all of these audits are available in full or redacted form on the OIG's website at http://oig.nasa.gov/.[2] In addition to this audit work, the OIG's Office of Investigations closed seven investigations into the potential loss or sale of export-controlled data or technology. Below we summarize our work during the past year.

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

[2] The exception is "Federal Information Security Management Act: Fiscal Year 2011 Evaluation" (IG-12-002, October 17, 2011).

Audit Reports

Preparing for the Space Shuttle Program's Retirement: Review of NASA's Controls over Public Sales of Space Shuttle Property (Report No. IG-11-016, March 15, 2011)

This audit examined NASA's controls over the disposition of Space Shuttle Program property, particularly vulnerabilities created when Space Shuttle property is sold to the public. We found that NASA had not fully integrated its export control and property disposition processes to reduce the risk that public sales of Space Shuttle property could result in the prohibited release of export-controlled items and technology. Moreover, property disposal managers did not fully recognize how the domestic sale of Space Shuttle property could result in an export, and NASA's policies did not include the internal controls necessary to fully protect export-controlled property from unauthorized release. We recommended that NASA revise its policy to clarify how property disposition activities can result in a violation of export control laws and require coordination between property disposal and export control personnel to ensure that export determinations are made, buyer citizenship is verified, and buyer identities are compared with lists of individuals who have been denied export privileges by the Departments of State or Commerce. In addition, we recommended that the Centers' export-controlled property disposition activities be reviewed during annual Export Control Program audits. NASA generally concurred with our recommendations.

Inadequate Security Practices Expose Key NASA Network to Cyber Attack (Report No. IG-11-017, March 28, 2011)

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 information technology (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 revealed encryption keys, encrypted passwords, and user account information to potential attackers. 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.

Annual Report, "Federal Information Security Management Act: Fiscal Year 2011 Evaluation" (IG-12-002, October 17, 2011, summary)

This annual report, submitted as a memorandum from the Inspector General to the NASA Administrator, provides the Office of Management and Budget (OMB) 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 established a program for the 11 required areas

of 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 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)

We evaluated NASA's efforts to transition from a legacy security posture assessment process to a new approach that emphasizes the need to continuously monitor components connected to NASA's 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 its transition. 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.

Investigations

NASA Computer Systems Compromised by a Chinese National

An OIG investigation into several compromised NASA computer systems revealed that a Chinese national had infiltrated the systems through a Government contractor's website. When NASA employees visited the site, they were redirected to a Taiwanese server. The investigation found that seven NASA systems had been compromised, leaving a significant amount of data vulnerable to unauthorized access and theft. As a result of the investigation, the Chinese national was detained by the Chinese Ministry of Public Service for violations of Chinese Administrative Law.

NASA Data Compromised by a British Citizen

OIG investigators assisted in the prosecution of a British citizen for his role in the distribution of malware that caused NASA data to be compromised. The OIG provided information related to compromised NASA e-mail accounts that resulted in the citizen receiving an 18-month jail sentence.

NASA Computers Hacked by a Swedish National

From December 2003 to February 2005, a Swedish hacker compromised six NASA networks causing the Agency to suffer $1 million in supercomputing "downtime." A Swedish court determined that the hacker, a minor at the time of the intrusion activity, was at fault for a variety of offenses. Consequently, a formal criminal history record for him will be maintained in international law enforcement databases.

RL-10 Rocket Engine Recovered by Investigators

The OIG recovered a Pratt & Whitney RL-10 rocket engine valued at approximately $200,000 that had been advertised for sale on an Internet auction site. The owner said that he purchased the engine from an individual who had received it from an unknown NASA employee. The 1960s-era RL-10 is subject to the International Traffic in Arms Regulations (ITAR) and, accordingly, may not be sold or released to the public.

Two Computers Hacked by a Texas Man

A Texas man pleaded guilty to one count of wire fraud in U.S. District Court, District of Minnesota, for hacking a local company's computer network. As part of his plea, he also admitted to hacking into two NASA computer servers at Goddard Space Flight Center. He was sentenced to 2 years in prison and ordered to pay $66,400 in restitution.

Space Shuttle Tiles Stolen by a Former Contractor Employee

An OIG investigation was initiated when an individual purchased a Space Shuttle Thermal Protection System tile on eBay and submitted a Freedom of Information Act request to NASA to determine the origin of the tile. OIG investigators subsequently traced the tile, which is subject to ITAR, to a former NASA contractor employee at Kennedy Space Center. The OIG determined that the contractor employee had sold 12 stolen Shuttle tiles on eBay for prices ranging from $41 to $912. He was charged with third degree felony theft and trafficking in stolen property, sentenced to 12 months of probation, ordered to pay $5,353 in restitution and $742 in fines and fees, and perform 50 hours of community service.

Space Shuttle Thermal Blanket Recovered by Investigators

OIG investigators recovered a Thermal Horse Collar Blanket fragment from a foreign national in England who was attempting to sell it on eBay. The Blanket is an accessory to a launch vehicle and therefore subject to ITAR and may not be sold or released to the public. The Englishman alleged he purchased the item from a third party on the same auction site. OIG investigators determined that the Blanket fragment was removed from the Space Shuttle Discovery in February 1992 and was supposed to have been processed for destruction.

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

Jay Henn
Acting Assistant Administrator, Office of Protective Services

Michael 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 Bill Nelson
United States Senate

The Honorable John Boozman
United States Senate

The Honorable Joseph I. Lieberman
United States Senate

The Honorable Susan M. Collins
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 Ralph Hall
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 Paul Tonko
U.S. House of Representatives

The Honorable Steven Palazzo
U.S. House of Representatives

The Honorable Jerry Costello
U.S. House of Representatives