National Aeronautics and
Space Administration

Office of Inspector General
Washington, DC 20546-0001

January 31, 2011

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

Dear Madam Chairwoman and Senator Shelby:

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 February 2010. Since that date, NASA has not entered into any cooperative agreements with China or any Chinese company. In addition, 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 two exceptions, all of these audits are available in full or redacted form on the OIG's website at oig.nasa.gov.[2] In addition to this audit work, the OIG's Office of Investigations closed five

[1] Public Law 106-391, codified at 42 U.S.C. § 2475a(a)(3).

[2] The exceptions are "Federal Information Security Management Act: Fiscal Year 2010 Report from the Office of Inspector General" (IG-11-005, November 10, 2010) and "Review of the Information Technology Security of [a NASA Computer Network]" (IG-10-013, May 13, 2010).

investigations into the potential loss or sale of export-controlled data or technology. Below we summarize our work during the past year.

Audit Reports

Preparing for the Space Shuttle Program's Retirement: A Review of NASA's Disposition of Information Technology Equipment (Report No. IG-11-009, December 7, 2010)

As part of a larger audit examining NASA's controls over the disposition of various types of Space Shuttle Program property, we examined NASA's internal controls for the sanitization and disposal processes for information technology (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, we determined that 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. We also found a lack of accountability for excessed hard drives at two Centers. The most serious of these issues was the discovery of hard drives removed from excessed computers stored in an unsecured dumpster accessible to the public.

Due to the importance of the issues we found at one Center, we immediately notified Center managers, who took action to address the issues. However, because we also found weaknesses at the three other Centers we visited, we made several recommendations to NASA's Chief Information Officer (CIO) related to immediate review of the adequacy of sanitization procedures and documentation of sanitization. In response to our recommendations, the CIO stated that NASA's policies would be updated and a new IT security handbook created. We did not consider the CIO's proposed actions responsive to our recommendations because we did not believe reviewing policy and procedures and drafting a handbook was adequate to identify and correct potential serious deficiencies at the Centers. Moreover, the CIO's response did not reflect the sense of urgency we believed was required to address the serious security issues uncovered by our audit. After publication of our final report, the CIO sent us an updated response proposing actions we considered responsive to our recommendations. Specifically, the CIO proposed meeting with all Center CIOs to identify deficiencies and best practices, issuing a NASA-wide directive to address sanitizing IT equipment prior to release to the public, reviewing applicable guidance and establishing a methodology for verification testing, and updating NASA directives and operating procedures.

Review of the Information Technology Security of [a NASA Computer Network] (Report No. IG-10-013, May 13, 2010, summary)

We evaluated the processes for continuously monitoring selected IT security controls on a NASA mission-critical computer network and found that NASA did not adequately protect the network from potential security breaches and did not always ensure that key IT security

controls were monitored. We recommended that the CIO designate a NASA Directorate or Center to immediately establish an oversight process for the network to include monitoring the systems connected to the network for the presence of critical patches and technical vulnerabilities and review all other Agency mission network IT security programs to determine whether each contains an effective oversight process. The CIO concurred with our recommendations and outlined specific actions to be taken to address the deficiencies and a timeline for when those actions would occur.

Audit of Cybersecurity Oversight of [a NASA] System (Report No. IG-10-018, August 5, 2010, redacted for public release)

After a prior audit revealed that NASA did not adequately protect a mission-critical network from potential security breaches or consistently ensure that key IT security controls were monitored, we evaluated the processes for continuously monitoring selected IT security controls on another NASA computer system. We found that the Agency's security controls included security awareness training for personnel; contingency planning related to safeguarding data, to include file backups and alternative processing sites in case of a disaster; procedures to protect system and information integrity, such as malicious code protection; and comprehensive access controls. However, we also found several significant security control weaknesses that could threaten the confidentiality, integrity, and availability of critical information on the system we reviewed. We recommended that NASA review security plans annually for completeness and eliminate internal control weaknesses related to vulnerability scans, local administrator accounts, installation of unauthorized software, and hardware and software inventories on servers. In addition, we recommended that a review of systems managed by contractors be completed to identify and correct similar security control weaknesses that may exist in those systems. The CIO generally concurred with our recommendations.

Information Technology Security: Improvements Needed in NASA's Continuous Monitoring Processes (Report No. IG-10-019, September 14, 2010)

We reviewed continuous monitoring processes at four Centers and found that those Centers did not have effective processes in place to ensure their computer servers remained securely configured over time. We also found that the Agency lacked complete and up-to-date inventories, which could provide a means to verify that 100 percent of the computers in the Agency's network are subject to configuration, vulnerability, and patch monitoring. We recommended that the CIO require the Centers to continuously monitor computer server operating system configuration settings and implement a process to verify that vulnerability monitoring includes 100 percent of applicable network devices such as cell phones and smart phones. Although the CIO's response to our draft report did not adequately address our concerns, following release of our final report the CIO proposed actions we considered responsive to our recommendations.

Review of NASA's Management and Oversight of Its Information Technology Security Program (Report No. IG-10-024, September 16, 2010)

We found that NASA's IT security program had not fully implemented key requirements of the Federal Information Security Management Act (FISMA) that are needed to adequately secure Agency information systems and data. Of the 29 NASA systems we reviewed, only 7 met FISMA requirements for annual security controls testing and 15 met FISMA requirements for annual contingency plan testing, and only 2 of the 5 external systems we reviewed were certified and accredited. These deficiencies occurred because NASA did not have an independent verification and validation function for its IT security program to ensure its effectiveness. We also found that NASA's Office of the CIO (OCIO) had not effectively managed corrective action plans used to prioritize the mitigation of IT security weaknesses. This occurred because OCIO did not have a formal policy for managing the plans. Another factor was that the information system that OCIO purchased to facilitate Agency-wide management of IT corrective action plans was underutilized and it contained corrective action plans for only 2 percent of the 29 systems we reviewed. This occurred because OCIO did not follow recognized best practices, such as getting customer buy-in, when it purchased the information system.

We recommended that the CIO (1) establish an independent verification and validation function to ensure that all FISMA and Agency IT security requirements are met; (2) develop a written policy for managing IT security corrective action plans; and (3) adopt industry system acquisition best practices, including documenting detailed requirements prior to system selection and conducting user acceptance testing before system implementation. The CIO concurred with our recommendations.

Federal Information Security Management Act: Fiscal Year 2010 Report from the Office of Inspector General (Report No. IG-11-005, November 10, 2010, 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 2010, we adopted a risk-based approach in which we selected high- and moderate-impact non-national security Agency systems for review. We examined 40 systems that included systems from all 10 NASA Centers, NASA Headquarters, and the NASA Shared Services Center. We reported to OMB that NASA established a program for certification and accreditation, security configuration management, incident response and reporting, security training, Plans of Actions and Milestones, remote access, account and identity management, continuous monitoring, business continuity/disaster recovery, and overseeing systems operated by contractors. However, we found that internal controls for these areas needed improvement.

Investigations

ITAR-Restricted Data Posted on a Public Website

An OIG investigation revealed that data subject to restriction under the International Traffic in Arms Regulations (ITAR) had been posted to the pay-for-access portion of a public website. Criminal prosecution was declined due to the lack of evidence pinpointing specifically who had released the data and the absence of any monetary motive for the release. We made NASA management aware of the release.

Attempted Sale of Saturn V Engines

OIG investigators found that the widow of a former NASA employee was attempting to sell two Saturn V rocket engines. When confronted, the widow agreed to return the engines to NASA.

Computer Intrusion of a JPL Shared Server

An OIG investigation uncovered the infiltration of a Jet Propulsion Laboratory (JPL) shared server through the compromised e-mail account of a JPL employee. The infiltration caused an unknown amount of damage and compromised approximately 22 gigabytes of data. The shared server contained proprietary computer-aided design data and potential ITAR-restricted information. A referral to NASA management from the OIG highlighted the internal weaknesses that allowed the infiltration.

Attempted Sale of Rocket Propellant Technology to a Foreign Country

An undercover investigation revealed that an individual was seeking to obtain U.S. Government rocket propulsion technology for the purpose of exporting the technology to the Republic of South Korea. The individual was arrested and charged with engaging in prohibited brokering activities related to defense articles. The individual pled guilty and was sentenced to 57 months in prison followed by 3 years of supervised release.

Inappropriate Access to Export-Controlled Data Granted to Australian Citizen

A citizen of Australia was inappropriately given access to the Kepler Mission Control Facilities' website maintained by an Ames Research Center contractor. Access was granted because the NASA employee responsible for requesting access mistakenly assumed that the Australian was a U.S. citizen based on the fact that he had been issued a NASA e-mail account. Access was revoked 4 months after being granted and it was determined that no adverse impacts to national security or foreign policy objectives resulted from the incident. Training and procedural improvements were implemented to prevent recurrence.

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

Jack Forsythe
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 Kay Bailey Hutchison
United States Senate

The Honorable Bill Nelson
United States Senate

The Honorable David Vitter
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 Donna Edwards
U.S. House of Representatives

The Honorable Steven Palazzo
U.S. House of Representatives

The Honorable Jerry Costello
U.S. House of Representatives