National Aeronautics and Space Administration

Office of Inspector General
Washington, DC 20546-0001

January 29, 2014

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
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 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 2013. Since that date, NASA has not entered into any cooperative agreements with China or any Chinese company. During the past year, the OIG conducted four audits examining the Agency's controls for its information technology (IT) assets and security systems, many of which contain data subject to export control laws. In addition, during this period we completed a special review examining a Chinese national's access to NASA's Langley Research Center and our Office of Investigations closed two investigations related to the security of NASA's IT assets or concerns about Chinese-manufactured parts. We summarize this work below.

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

Audit Reports

NASA's Information Technology Governance (IG-13-015, June 5, 2013)

IT governance is a process for designing, procuring, and protecting IT resources. For this reason, effective IT governance must balance compliance, cost, risk, security, and mission success to meet the needs of internal and external stakeholders. In this audit, we examined whether NASA's IT governance structure appropriately aligns authority and responsibility to support the Agency's overall mission.

We found that the decentralized nature of NASA's operations and its longstanding culture of autonomy hinder the Agency's ability to implement effective IT governance. NASA's Chief Information Officer (CIO) has limited visibility and control over a majority of the Agency's IT investments, operates in an organizational structure that marginalizes the authority of the position, and cannot enforce security measures across NASA's computer networks. Specifically, although the CIO is responsible for developing IT security policies and procedures and implementing an Agency-wide IT security program, because the position lacks authority and control over the majority NASA's networks, the CIO is unable to enforce the implementation of IT security programs across all NASA IT assets.

NASA's ability to secure its networks is further complicated because the Agency lacks a complete inventory of IT assets. For example, five Center CIOs told us they could not account for 100 percent of the IT systems and hardware at their Centers. To overcome the barriers that have resulted in inefficient and ineffective management of the Agency's IT assets and IT security, we made eight recommendations to the CIO. The CIO generally concurred with our recommendations and proposed appropriate corrective actions.

To view the full report, visit http://oig.nasa.gov/audits/reports/FY13/IG-13-015.pdf.

NASA's Progress in Adopting Cloud-Computing Technologies (IG-13-021, July 29, 2013)

The adoption of cloud-computing technologies has the potential to improve IT service delivery and reduce the costs associated with managing NASA's diverse IT portfolio. Specifically, 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. NASA was a pioneer in cloud computing having established its own private cloud computing data center called Nebula in 2009 at the Ames Research Center. In 2012, NASA shut down Nebula based on the results of a 5-month test that benchmarked Nebula's capabilities against those of Amazon and Microsoft. The test found that public clouds were more reliable and cost effective and offered much greater computing capacity and better IT support than Nebula.

In our audit, we examined whether NASA evaluated the security of and risks in moving Agency data and services to the cloud. We found that weaknesses in NASA's IT governance and risk management practices have impeded the Agency from fully realizing the benefits of cloud computing and potentially put NASA systems and data stored in the

cloud at risk. For example, several NASA Centers moved Agency systems and data into public clouds without the knowledge or consent of the CIO. Moreover, on five occasions NASA acquired cloud-computing services using contracts that failed to fully address the business and IT security risks unique to the cloud environment. Finally, NASA moved a system to a public cloud and it operated for 2 years without authorization, a security or contingency plan, or a test of the system's security controls.

We made eight recommendations to the CIO to help strengthen NASA's cloud computing practices, mitigate business and IT security risks, and improve contractor oversight. The CIO concurred with our recommendations and proposed appropriate corrective actions.

To view the full report, visit http://oig.nasa.gov/audits/reports/FY13/IG-13-021.pdf.

NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools (IG-13-006, March 18, 2013)

NASA spends more than $1.5 billion annually on IT assets, including approximately 550 information systems the Agency uses to control spacecraft, collect and process scientific data, provide security for its IT infrastructure, and enable personnel to collaborate with colleagues around the world. However, the Agency's use of advanced technology coupled with the large size of its networks makes NASA an attractive target to cyber-attacks. To thwart such attacks, NASA must ensure that its IT systems and their associated components are regularly safeguarded, assessed, and monitored. The Agency's CIO spends at least $58 million annually on IT security, a portion of which is used to acquire and manage security assessment and monitoring tools. In this audit, we examined NASA's policies and procedures related to its acquisition of IT security assessment and monitoring tools.

We found that the Agency has not fully implemented a process for identifying its IT security assets. Because NASA does not have a process that captures, consolidates, and assesses IT security tool requirements across the Agency, centralized purchases of tools do not regularly occur. This inability to consolidate requirements and centralize purchases limits NASA's efforts to reduce cost and improve program efficiencies on critical IT investments. To improve NASA's process for acquiring Agency-wide IT security assessment and monitoring tools, we made four recommendations to NASA's CIO. The CIO concurred with our recommendations and proposed appropriate corrective actions.

To view the full report, visit http://oig.nasa.gov/audits/reports/FY13/IG-13-006.pdf.

Federal Information Security Management Act: Fiscal Year 2013 Evaluation (IG-14-004, November 20, 2013)

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 2013, the OIG reviewed a sample of eight Agency IT systems and two contractor IT systems. We also reviewed NASA's progress in implementing prior OIG recommendations.

Overall, we found that NASA has established a program to address the challenges in each of the 11 areas designated by the Office of Management and Budget for review: continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning. However, we also found that the Agency needs to enhance its efforts with regard to configuration management, risk management, and contractor systems.

To view a summary of this report, visit http://oig.nasa.gov/audits/reports/FY14/IG-14-004.pdf.

Special Review

Bo Jiang's Access to NASA's Langley Research Center (October 22, 2013)

In March 2013, a member of Congress publicly questioned whether NASA had inappropriately afforded Bo Jiang, a Chinese national working as a NASA contractor, access to the Langley Research Center (Langley) and to Agency data and IT. The Congressman's concerns were prompted at least in part by internal NASA documents suggesting it had been improper for Langley to hire Jiang as a contractor, allow him unescorted access to the Center, and provide him with data related to his research. On March 16, 2013, after being terminated from his position, Jiang was in the process of returning to China when agents from the Department of Homeland Security searched him at Dulles International Airport as part of an investigation of potential export control violations. After questioning him about the electronic media he had in his possession, agents took Jiang into custody and charged him with making a false statement to Federal authorities because a search of his belongings revealed media he had not declared. Subsequent to Jiang's guilty plea to a misdemeanor security offense, the OIG opened an administrative investigation to examine the process by which Jiang came to work at Langley and the information and IT resources to which he was given access.

In 2002, Langley and the National Institute of Aerospace (NIA), a nonprofit research and graduate education organization located in Hampton, Virginia, entered into a cooperative agreement pursuant to which Langley frequently hired NIA personnel as contractors to work on NASA research projects. Jiang originally came to the United States in 2007 as a Ph.D. student at Old Dominion University in Norfolk, Virginia, before becoming a postdoctoral research assistant for the NIA. Jiang began working at Langley in January 2011.

In November 2011 and again in November 2012, Jiang visited family in China taking with him a NASA-provided laptop computer. It was during the second visit that an export control professional at Langley learned that Jiang had taken the laptop to China and raised concerns with attorneys at Langley and personnel in the Headquarters' Export Control Office about Jiang's travel and access to NASA information without prior review by export control officials. The Langley export control official also claimed that Jiang's work as a paid NASA contractor violated funding restrictions in NASA's appropriations legislation. Jiang returned to the United States in December 2012 and Center computer security

personnel examined his NASA-provided laptop to determine whether it contained export-controlled information. In January 2013, NIA terminated Jiang's employment for violating NIA policy by taking the laptop to China and because NASA had ended the agreement under which Jiang had been hired.

We found that NASA did not violate appropriations restrictions by hiring Jiang as a paid contractor through the NIA cooperative agreement. Moreover, while Langley's process for requesting access for foreign nationals was structured pursuant to NASA regulations, we found the process overly complex, required input from numerous Center and Headquarters employees, and not sufficiently integrated to ensure that responsible personnel had access to all relevant information. In addition, we determined that several employees who had roles in the screening process made errors that contributed to the confusion about the proper scope of Jiang's access to Langley facilities and IT resources and the appropriateness of Jiang taking his NASA-provided laptop to China.

In the wake of the Jiang incident and at the request of the NASA Administrator, Langley management has taken a number of steps to strengthen its foreign national access process, including increased education and training for Langley employees, revising the form used to request access for foreign nationals, ensuring the Center CIO's Office is involved in the foreign visitor request process, and contracting with the National Academy of Public Administration to assess the effectiveness of NASA's Agency-wide foreign national access program. We made six recommendations in our review to improve NASA's foreign visitor approval process. The NASA Administrator concurred with our recommendations and proposed appropriate corrective actions.

To view the full report, visit http://oig.nasa.gov/Special-Review/OIG_Investigative_Summary.pdf.

Investigations

Romanian National Arrested and Indicted

On January 17, 2013, a Romanian national was indicted in U.S. District Court for the Southern District of New York on multiple counts of criminal conspiracy. The Romanian national allegedly ran a "bulletproof hosting" service that enabled cybercriminals to distribute malicious software and conduct sophisticated cybercrimes. Malware distributed by this hosting service has infected over one million computers worldwide, including computers belonging to NASA, causing tens of millions of dollars in losses to individuals, businesses, and government entities. The OIG is working jointly with the FBI on this investigation.

Civil Settlement with Government Contractor

In February 2013, World Wide Technology, Inc., agreed to pay $735,000 to settle allegations that it violated the Trade Agreements Act, which requires that goods provided to the Federal Government be manufactured in designated countries. The investigation began after the company self-disclosed that it may have incorrectly certified that products sold to NASA and the Department of Defense were in compliance with the Act. A joint investigation by OIG and the Department of Defense confirmed that the company had improperly filled 174 orders, including 29 NASA orders worth $255,000, using Chinese-manufactured products.

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

David Radzanowski
Chief of Staff

Larry Sweet
Chief Information Officer

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

Richard Keegan
Associate Administrator, Mission Support Directorate

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 Ted Cruz
United States Senate

The Honorable Thomas R. 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 John Mica
U.S. House of Representatives

The Honorable Gerry Connolly
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 F. Edwards
U.S. House of Representatives