NASA OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS
SUITE 8U71, 300 E ST SW
WASHINGTON, D.C. 20546-0001

January 25, 2017

The Honorable Richard Shelby
Chairman
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Jeanne Shaheen
Vice Chairwoman
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

Subject: *NASA's Compliance with Federal Export Control Laws* (IG-17-008)

Dear Mr. Chairman and Madame Vice Chairwoman,

The National Aeronautics and Space Administration (NASA) Authorization Act of 2000 directs the NASA Office of Inspector General (OIG) to annually assess the Agency's compliance with Federal export control laws and reporting requirements regarding cooperative agreements between NASA and China or any Chinese company.[1]

The NASA OIG last reported to you regarding these issues in February 2016. Since then, NASA entered into a bilateral agreement with the Chinese Aeronautical Establishment in September 2016 to cooperate on aeronautics research that will advance air traffic management and improve safety and efficiency for

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

U.S. and Chinese aviation operations in China.[2] NASA also continued its engagement with the Chinese Academy of Science and the China National Space Administration regarding bilateral science activities relating to space geodesy, glacier research in the Himalaya Region and High Mountain Asia, and lunar science, as well as China's plans for the carbon-monitoring TanSat satellite, which was launched on December 21, 2016.[3] In addition, NASA officials met with the Chinese Manned Space Agency to better understand their plans for human space exploration. Lastly, NASA participated in Department of State-led discussions with Chinese officials on the topics of orbital debris mitigation, satellite collision avoidance, and the peaceful exploration and use of outer space. For each of these activities, the Agency made the appropriate notifications in accordance with the certification process established in Public Law 114-113.[4]

With regard to work by our office, during the past year we completed an audit examining NASA's implementation of recommendations made in reviews completed in 2013 and 2014 by the OIG, Government Accountability Office (GAO), and the National Academy of Public Administration (NAPA) designed to improve the Agency's export control and foreign national access management procedures. We also completed three audits examining NASA's controls over its information technology (IT) assets and security systems, many of which contain data subject to export control laws, and initiated three additional audits related to IT security. In addition, our Office of Investigations closed four investigations related to website intrusions and hacking by foreign nationals that could have exposed export-controlled information to loss or misuse. We summarize this work below.

EXPORT CONTROL AUDIT

NASA's Implementation of Export Control and Foreign National Access Management Recommendations (IG-16-022, May 26, 2016)

Throughout its history, NASA has been at the forefront of science and space exploration and responsible for numerous scientific and technological discoveries and innovations. In the course of this work, the Agency partners with foreign countries and foreign nationals on projects and research, some of which may contain sensitive space-related technology and information. The challenge for NASA has been to sustain and nurture these partnerships while protecting the Agency's sensitive information.

Beginning in 2009, Federal law enforcement agencies received complaints that foreign nationals working as contractors at NASA's Ames Research Center (Ames) had been given improper access to export-controlled information. Furthermore, in 2013 questions arose regarding a Chinese national's access to Agency data and information technology systems at the Langley Research Center (Langley).

---

[2] The Chinese Aeronautical Establishment was created in the early 1960s to further development of aeronautical science and technology, carry out major aeronautical experiments and assessments, and train aviators.

[3] Space geodesy uses space-based observations to monitor, map, and understand changes in the Earth's shape, rotation, and mass distribution. Although China ultimately chose a different orbit, it had originally planned to launch and operate TanSat in the same orbit as the A-train, a collection of six Earth-observing satellites (five operated by NASA and one by Japan) that fly in a polar orbit within seconds or minutes of each other.

[4] Public Law 114-113, "Consolidated Appropriations Act, 2016," December 18, 2015, requires NASA to certify to the Senate and House Committees on Appropriations and the Federal Bureau of Investigation that the activities pose no risk of resulting transfer of technology, data, or other information with national security or economic security implications and that the activities will not involve knowing interactions with officials who have been determined to have direct involvement with violations of human rights.

The OIG subsequently investigated and issued reports regarding the Ames and Langley matters.[5] In addition, the GAO and NAPA issued reports in 2014 examining NASA's Export Control Program and foreign national access management.[6] Collectively, the OIG, GAO, and NAPA made 40 recommendations to improve NASA's export control and foreign national access processes and procedures.

In our May 2016 report, we found NASA had taken significant steps to address the recommendations made by the OIG, GAO, and NAPA. As of December 31, 2015, the Agency implemented all of the OIG's recommendations, 5 of GAO's 7 recommendations, and 18 of NAPA's 27 recommendations. However, some Center officials raised concerns that several requirements in draft Agency policy that would address several of the NAPA recommendations – specifically those requiring fingerprints from foreign nationals not living in or likely to visit the United States – were not practical and would impose undue burdens on their projects and programs. We found that due to a lack of effective collaboration and communication, NASA did not fully capitalize on opportunities to address these and other concerns with the draft policies. Consequently, completion of policy revisions and the foreign national access manual needed to address several recommendations had taken longer than expected.

In addition, we concluded that NASA should improve the Export Control Program's self-assessment process and sharing of lessons learned, including those resulting from voluntary disclosures, actions that could reduce the risk of future violations of export control and foreign national access rules and procedures. Our review of the annual export control audits from the three Centers we visited found that auditors concentrated primarily on administrative requirements rather than evaluating the effectiveness of the functional and procedural components. Furthermore, although NASA policy encourages sharing knowledge and best practices, Center personnel were generally unaware of actions other Centers had taken to improve their export control and foreign national access processes and procedures.

In order to improve NASA's Export Control and Foreign National Access Management Programs, we made six additional recommendations. NASA initially agreed to take action on five of the recommendations and disagreed with our recommendation to combine the Export Control and Foreign National Access Operations Manuals. However, the Agency later proposed alternative action that met the intent of that recommendation.

To view the full report, visit https://oig.nasa.gov/audits/reports/FY16/IG-16-022.pdf.

[5] The Ames report was the administrative culmination of a multi-year criminal investigation into allegations that ended without criminal charges. The Langley report resulted from an administrative investigation to examine the process by which a Chinese national came to work at Langley and the IT resources to which he was given access. NASA OIG, "Review of International Traffic in Arms Regulations and Foreign National Access Issues at Ames Research Center," February 26, 2014, and "Bo Jiang's Access to NASA's Langley Research Center," October 22, 2013, respectively.

[6] GAO, "Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the Risk of Unauthorized Access to Its Technologies" (GAO-14-315, April 15, 2014). The NAPA report was commissioned by NASA in July 2013 in response to the Langley incident. NAPA, "An Independent Review of Foreign National Access Management," January 2014.

OTHER COMPLETED AUDIT REPORTS

NASA's Management of the Near Earth Network (IG-16-014, March 17, 2016)

NASA's Near Earth Network provides tracking, telemetry, and command services to NASA science missions operating in low Earth orbit and will be used to support the Space Launch System and Orion Multi-Purpose Crew Vehicle scheduled to launch before the end of the decade. The Network also supports other Federal agencies, including launch and contingency support for National Oceanic and Atmospheric Administration satellites that assist with weather forecasting for the United States. To provide these services, the Near Earth Network uses NASA-owned antennas and transmitters, as well as equipment owned by other U.S. or foreign government agencies or commercial providers. Using non-Government entities to transmit Network data presents significant security challenges. Moreover, NASA's Network assets are located in extreme environments, such as Alaska and Antarctica, making maintenance on the aging structures more difficult.

We found NASA, Goddard Space Flight Center, and the Near Earth Network Project Office deviated from and failed to consider fundamental elements of Federal and Agency IT and physical security risk management policies and standards for protecting the Network. Specifically, the security categorization NASA assigned to the Network did not reflect its mission-essential nature and the Agency did not include the Network in its Critical Infrastructure Protection Program; external information system connections were not being managed in accordance with Federal and Agency policy; technical security controls were not in place or functioning as intended; and physical security controls had not been implemented on NASA-owned and supporting contractor facilities in accordance with Federal or Agency standards. These deficiencies increased the likelihood that the Network's IT and physical infrastructure were susceptible to compromise.

We made 14 recommendations to ensure the Near Earth Network was properly protected, IT security risk management practices complied with Federal and Agency requirements, Network locations met federally mandated physical security standards, and stations remained operational and met future mission requirements. The Agency agreed to take corrective action to address all 14.

To view the full report, visit https://oig.nasa.gov/audits/reports/FY16/IG-16-014.pdf.

Review of NASA's Information Security Program (IG-16-016, April 14, 2016)

NASA depends on a large number of IT systems to carry out its missions and business functions. As highlighted by data breaches at the Office of Personnel Management and the Internal Revenue Service, Federal agencies face an evolving cybersecurity landscape.[7] To improve cybersecurity and address the increasing sophistication of attacks, the Government relies on a variety of initiatives. First, the Federal Information Security Management Act requires Federal agencies maintain an information security program commensurate with their risk profile. Second, the National Institute of Standards and Technology issues security standards and guidelines for information systems utilized by Federal agencies. Finally, as the operational lead for Federal civilian cybersecurity, the Department of Homeland

[7] In June 2015, the Office of Personnel Management reported an intrusion into its systems that affected the personnel records of about 4 million current and former Federal employees. In June 2015, the Internal Revenue Service Commissioner testified that unauthorized third parties had gained access to taxpayer information, including Social Security numbers, dates of birth, and street addresses, for approximately 100,000 tax accounts.

Security operates a number of protection programs on behalf of the Government. This report focused on whether NASA had implemented programmatic, Agency-wide information security requirements independent of any particular information system.

We found although NASA had made progress in meeting requirements in support of an Agency-wide information security program, it had not fully implemented key management controls essential to managing that program. Specifically, NASA lacked an Agency-wide risk management framework for information security and an information security architecture. In our judgment, this condition existed because the Office of the Chief Information Officer had not developed an information security program plan to effectively manage its resources. In addition, the Office was experiencing a period of transition with different leaders acting in the Senior Security Officer role, which caused uncertainty surrounding information security responsibilities at the Agency level.

To improve management of NASA's information security program, we recommended the NASA Chief Information Officer direct the Senior Security Officer to develop and disseminate an Agency-wide information security program plan that met National Institute of Standards and Technology requirements. NASA concurred with our recommendation.

To view the full report, visit https://oig.nasa.gov/audits/reports/FY16/IG-16-016.pdf.

Federal Information Security Management Act: Fiscal Year 2016 Evaluation (IG-17-002, November 7, 2016)

This annual report, submitted as a memorandum from the Inspector General to the NASA Administrator, provides the OIG's independent assessment of NASA's information security posture. For fiscal year 2016, we used a risk-based approach to examine a sample of five Agency and contractor information systems. We also considered findings from previous OIG audit work in reaching our conclusions.

We determined NASA lacked an effective program in each of the five functions designated by the Office of Management and Budget for review – identify, protect, detect, respond, and recover. Specifically, NASA lacked formalized programs and performed activities in a reactive rather than proactive manner in the protect and detect functional areas. For the other the three functions, NASA had formalized programs but failed to consistently implement those programs Agency-wide. That said, we noted NASA had several efforts underway in each of the functional areas to improve its information security program.

To view this report, visit https://oig.nasa.gov/audits/reports/FY17/IG-17-002A.pdf.

ONGOING AUDIT WORK

Audit of Industrial Control System Security within NASA's Critical and Supporting Infrastructure (A-16-001-00, November 18, 2015)

The OIG is evaluating whether NASA has appropriately identified and protected critical and supporting IT infrastructure. Specifically, we are evaluating whether NASA has implemented effective physical and logical security controls necessary to protect these systems against physical and cybersecurity threats.

Audit of Information Security Controls over NASA's Cloud Computing Services (A-16-002-00, November 18, 2015)

The OIG is examining the effectiveness of NASA's information security controls relating to cloud computing services. Specifically, we are determining whether NASA has established and implemented Agency-wide plans, procedures, and controls to meet Federal and Agency information technology security requirements to protect the confidentiality, integrity, and availability of NASA data maintained by cloud service providers.

Audit of NASA's Efforts to Improve the Agency's Information Technology Governance (A-16-013-00, March 31, 2016)

For more than 2 decades, NASA has struggled to implement an effective approach to IT governance that appropriately aligns authority and responsibility consistent with the Agency's overall mission. In 2013, the OIG examined NASA's IT governance and made eight recommendations for improvement.[8] This follow-on audit is assessing the efforts NASA has made since then to improve the Agency's IT governance.

INVESTIGATIONS

Estonian Cybercriminal Sentenced for Infecting Computers

In April 2016, an Estonian national was sentenced for his role as ringleader in a cybercriminal scheme that infected millions of computer systems worldwide, including NASA systems. He was sentenced to 7 years and 3 months imprisonment and ordered to forfeit $2.5 million. The OIG worked the case jointly with the Federal Bureau of Investigation.

Romanian Sentenced for Conspiracy to Commit Computer Intrusion

In May 2016, a Romanian national was sentenced for conspiracy to commit computer intrusion and bank fraud. The violations stemmed from the spread of Gozi Malware, which infected numerous Government computer systems including some at NASA. The subject was sentenced to 3 years and 1 month imprisonment and forfeited $6.9 million. This case was investigated by the OIG and Federal Bureau of Investigation.

Nigerian Sentenced for Involvement in Cyber Scheme to Steal Government Computer Credentials

In May 2016, a Nigerian national was convicted and sentenced to 7 years imprisonment by the Benin High Court of Nigeria for his involvement in a cyber scheme. An OIG investigation revealed numerous NASA email accounts were accessed and used by hackers in Nigeria to perpetrate fraud schemes.

[8] NASA OIG, "NASA's Information Technology Governance" (IG-13-015, June 5, 2013).

Italian Sentenced for Hacking Computer Systems

In July 2016, an Italian national was convicted and sentenced to 1 year in prison and payment of court fees for unlawful access into and retaining codes to a computer system. In coordination with Italian authorities, the OIG found that the hacker had gained access and removed files from a Jet Propulsion Laboratory server.

If you or your staff would like further information on any of the audit reports or investigations discussed in this letter, please contact me or Renee Juhans, OIG Executive Officer, at 202-358-1220 or renee.n.juhans@nasa.gov.

Sincerely,

Paul K. Martin
Inspector General

cc: Robert Lightfoot
Acting Administrator

Lesa Roe
Deputy Associate Administrator

Renee Wynn
Chief Information Officer

Al Condes
Associate Administrator, International and Interagency Relations

Krista Paquin
Associate Administrator, Mission Support Directorate

Sumara Thompson-King
General Counsel

Enclosure – 1

ENCLOSURE I: CONGRESSIONAL RECIPIENTS

United States Senate

Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Commerce, Science, and Transportation
Committee on Homeland Security and Governmental Affairs

U.S. House of Representatives

Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Oversight and Government Reform
Committee on Science, Space, and Technology