NASA OFFICE OF INSPECTOR GENERAL

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

February 2, 2016

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

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

Subject: *Review of NASA's Compliance with Federal Export Control Laws* (IG-16-012)

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 January 2015. Since that date, NASA has engaged in three bilateral science activities with the Chinese Academy of Science relating to space geodesy, glacier research in the Himalaya Region and High Mountain Asia, and lunar science.[2] The space geodesy project resumed activities outlined in a 1992 agreement with the Chinese Academy that NASA

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

[2] Space geodesy uses space-based observations to monitor, map, and understand changes in the Earth's shape, rotation, and mass distribution.

suspended in 2011. In the other two instances, NASA shared publicly available science information and received similar information from the Chinese. The Agency also engaged with the Chinese Academy and the Chinese National Space Agency to discuss China's plans to launch the TanSat satellite into the Afternoon Constellation, or "A-Train," a NASA-managed international satellite constellation of Earth-observing satellites.[3] NASA also held discussions with the Chinese Aeronautical Establishment on research into mutually beneficial air traffic management issues.[4] Finally, in 2015 NASA participated in an interagency delegation to the U.S.-China Civil Space Cooperation Dialogue led by the Department of State. During 2015, NASA entered into no new bilateral agreements and made the appropriate notifications regarding each of the preceding activities in accordance with the certification process established in Public Law 113-235.[5]

During the past year, the OIG completed two audits examining NASA's controls over its information technology (IT) assets and security systems, many of which contain data subject to export control laws. We also initiated three audits related to IT security, export control, and foreign national access procedures. In particular, in July 2015 we initiated a review examining NASA's implementation of 40 recommendations made in reviews completed in 2013 and 2014 by the OIG, Government Accountability Office, and the National Academy of Public Administration designed to improve the Agency's export control and foreign national access management procedures. We anticipate completing this review in mid-2016.

In addition, during this period our Office of Investigations closed two investigations related to website intrusion and hacking by foreign nationals that could have exposed export-controlled information to loss or misuse. We summarize this work below.

COMPLETED AUDIT REPORTS

NASA's Management of the Deep Space Network (IG-15-013, March 26, 2015)

NASA's Deep Space Network (DSN or Network) is a central component of the Agency's space communications and navigation capability, providing deep space missions with tracking, telemetry, and command services needed to control spacecraft and transmit data. Part of NASA's Space Communications and Navigation Program, DSN operates antennas and transmitters at communications complexes in three locations: Goldstone, California; Madrid, Spain; and Canberra, Australia. NASA has contracts with the Spanish and Australian governments to manage day-to-day operations at the foreign sites and with the Jet Propulsion Laboratory (JPL), a federally funded research and development center in Pasadena, California, for the Goldstone site. DSN has significant IT and physical infrastructure components that must be protected against compromise from cyber attack, espionage, and terrorism.

---

[3] The A-train is a collection of six Earth-observing satellites that fly in a polar orbit within seconds or minutes of each other. NASA operates five of the six satellites, one in collaboration with France, while the sixth is operated by Japan. The close proximity of these satellites requires frequent communication among the operators and operational precision to ensure the continued safety of the satellites.

[4] 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.

[5] The law requires NASA to certify to the Committees on Appropriations 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.

To this end, the JPL, Madrid, and Canberra agreements require each contractor to follow specified Federal and NASA security policies.

In our report, we found NASA, JPL, and DSN have significantly deviated from Federal and Agency policies, standards, and governance methodologies for the security of the Network's IT and physical infrastructure. For example, the Network's system security categorization process did not consider all DSN mission functions, vulnerability identification and mitigation practices and IT security configuration baseline application did not comply with Federal and Agency policy, and NASA's Security Operations Center is not adequately integrated into JPL's computer network operations.[6] Further, required physical security controls were missing or inconsistently implemented at the three Complexes, procedures to assign security level designations did not comply with NASA policy, required facility security assessments had not been completed, and security waivers or other risk acceptance documentation were not consistently in place. As a result, DSN's IT and physical infrastructure may be unnecessarily vulnerable to compromise.

We made eight recommendations to NASA management to ensure DSN follows established IT security policies, standards, and governance methodologies, and the physical security requirements are implemented consistently across the three Complexes. The Agency agreed to take corrective action.

To view the full report, visit https://oig.nasa.gov/audits/reports/FY15/IG-15-013.pdf.

Federal Information Security Management Act: Fiscal Year 2015 Evaluation (IG-16-002, October 19, 2015)

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 2015, the OIG used past audit results as well as a risk-based approach to evaluate a sample of 29 Agency and contractor IT systems.

Overall, we found that NASA has established a program to address the challenges in each of the 10 areas designated by the Office of Management and Budget for review: (1) continuous monitoring management, (2) configuration management, (3) identity and access management, (4) incident response and reporting, (5) risk management, (6) security training, (7) plan of action and milestones, (8) remote access management, (9) contingency planning, and (10) contractor systems. However, we also found that NASA needs to make more progress in addressing the Agency's continuous monitoring, configuration management, and risk management issues.

To view a summary of this report, visit https://oig.nasa.gov/audits/reports/FY16/IG-16-002.pdf.

[6] NASA's Security Operations Center, located at Ames Research Center, is responsible for monitoring Agency network traffic for suspicious activity.

ONGOING AUDIT WORK

Review of NASA's Implementation of Export Control and Foreign National Access Program Recommendations (A-15-011, July 28, 2015)

The OIG is assessing whether NASA is: (1) effectively implementing OIG, Government Accountability Office, and National Academy of Public Administration recommendations to improve the Agency's export control and foreign national access programs; and (2) taking prudent actions to protect export control-restricted information.

Audit of Industrial Control System Security within NASA's Critical and Supporting Infrastructure (A-16-001, 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, 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.

INVESTIGATIONS

French Citizen Sentenced for Website Intrusion

In December 2014, a French citizen was arrested and subsequently prosecuted for compromising numerous government and private websites worldwide, including a website maintained by NASA's Glenn Research Center. In April 2015, a French court sentenced the individual to 6 months in prison. This investigation was conducted by the NASA OIG, the U.S. Army Criminal Investigation Command, the U.S. Air Force Office of Special Investigations, the Department of Energy OIG, the German Bundeskriminalamt, and the French Ministry of the Interior's Cybercrime Unit.

Nigerian Hacker Convicted and Sentenced

In June 2015, a Nigerian hacker was convicted in his home country of two counts of possessing a document obtained under false pretenses and sentenced to 2 years in prison on each count. The OIG's investigation revealed numerous NASA e-mail accounts were accessed and used by hackers in Nigeria to perpetrate a fraud scheme. The subject was arrested by Nigeria's Economic and Financial Crimes Commission based upon a petition received from the OIG.

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.

Sincerely,

Paul K. Martin
Inspector General

cc: Charles F. Bolden, Jr.
Administrator

Dava Newman
Deputy Administrator

Robert Lightfoot
Associate Administrator

Michael French
Chief of Staff

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

The Honorable John Thune
The Honorable Bill Nelson
The Honorable Ted Cruz
The Honorable Gary Peters
The Honorable Ron Johnson
The Honorable Thomas R. Carper

U.S. House of Representatives

The Honorable John Culberson
The Honorable Michael Honda
The Honorable Jason Chaffetz
The Honorable Elijah Cummings
The Honorable Mark Meadows
The Honorable Gerald Connolly
The Honorable Lamar Smith
The Honorable Eddie Bernice Johnson
The Honorable Barry Loudermilk
The Honorable Don Beyer
The Honorable Brian Babin
The Honorable Donna Edwards