NASA OFFICE OF INSPECTOR GENERAL

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

February 8, 2018

The Honorable Richard C. 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-18-013)

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 2017. Since then, NASA has not established any new bilateral agreements with China. The Agency has continued its engagement with the Chinese Academy of Science and the China National Space Administration regarding bilateral science activities relating to space geodesy and glacier research in the Himalaya Region and High Mountain Asia,

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

as well as China's plans for the carbon-monitoring TanSat satellite launched on December 21, 2016.[2] NASA also continued its engagement with the Chinese Aeronautical Establishment to cooperate on aeronautics research intended to advance air traffic management and improve safety and efficiency for U.S. and Chinese aviation operations in China.[3] 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 requirements outlined in Public Law 115-31.[4]

With regard to export control-related oversight work by our office, during the past year we verified Agency actions taken in response to our May 2016 report on NASA's Export Control and Foreign National Access Management Programs and, satisfied with these actions, we closed the recommendations. We also completed four 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 two additional audits related to IT security. In addition, our Office of Investigations closed two investigations related to the misuse and unauthorized access to export-controlled information. Furthermore, the OIG has been an active member of the Department of Homeland Security's Export Enforcement Coordination Center (E2C2). The E2C2 coordinates export enforcement efforts and intelligence activities among Federal agencies to identify and resolve conflicts involving violations of U.S. export control laws.

We summarize our 2017 export control work below.

EXPORT CONTROL AUDIT

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

In this May 2016 report, we found NASA had taken significant steps to address past recommendations made by the OIG, Government Accountability Office, and the National Academy of Public Administration. However, several Agency officials raised concerns that requirements in draft NASA policy designed to address the oversight entities' recommendations 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.

---

[2] 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.

[3] 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.

[4] Public Law 115-31, "Consolidated Appropriations Act, 2017," May 5, 2017, 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 a 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.

In addition, we found that NASA needed to improve its Export Control Program's self-assessment process and sharing of lessons learned.

During the past year, NASA completed its proposed actions to implement the six recommendations we made to improve the Agency's Export Control and Foreign National Access Management Programs. These actions included expanding annual audits to assess the effectiveness and efficiency of export control and foreign national access processes and ensuring annual audit reports are standardized to evaluate progress across NASA's numerous Centers around the country. In addition, the results of the OIG audit were discussed at the Agency's annual Export-Import Compliance Program Review and during quarterly training sessions.

The OIG report can be found at https://oig.nasa.gov/audits/reports/FY16/IG-16-022.pdf.

OTHER ISSUED AUDIT REPORTS

Security of NASA's Cloud Computing Services (IG-17-010, February 7, 2017)

NASA's IT portfolio includes systems that control spacecraft, collect and process scientific data, provide security for critical infrastructure, and enable Agency personnel to collaborate with colleagues around the world. In fiscal year (FY) 2016, the Agency spent approximately $1.4 billion on IT investments. Among these investments was the acquisition of cloud computing services from commercial companies.

In 2013, we reported that weaknesses in NASA's IT risk management and governance practices had impeded the Agency from fully realizing the benefits of cloud computing and potentially put NASA systems and data stored in the cloud at risk.[5] While NASA has made improvements since our 2013 audit, in the 2017 audit we found continuing weaknesses related to the Agency's move to the cloud environment. Specifically, NASA had not completed the necessary steps to ensure all approved services were registered with the Federal Risk and Authorization Management Program. Further, several of the services on the registry lacked authorizations to operate and were not covered by an IT system security plan. We also discovered an additional 20 cloud services in use at NASA not on the registry. Although 14 of these services had been approved and authorized by Center officials, 6 lacked authorizations to operate or system security plans and had not been tested for appropriate security controls. In addition, we identified numerous instances in which Agency personnel acquired cloud services using contracts that lacked provisions intended to address key business and IT security risks associated with cloud environments.

We made six recommendations to strengthen NASA's security controls over cloud computing. Although the Agency described corrective actions it would take to address the recommendations, several proposed actions lacked the specificity required to be fully responsive. After additional discussions with the OIG, NASA managers provided acceptable action plans.

To view the full report, visit https://oig.nasa.gov/audits/reports/FY17/IG-17-010.pdf.

[5] NASA OIG, "NASA's Progress in Adopting Cloud-Computing Technologies" (IG-13-021, July 29, 2013).

NASA's Efforts to Improve the Agency's Information Technology Governance (IG-18-002, October 19, 2017)

For more than two decades, NASA has struggled to implement an effective IT governance framework, a critical component to making IT procurement and security decisions that balance compliance, cost, risk, and mission success. This ineffective IT governance can result in security breaches, increased costs, missed deadlines, and provision of low quality IT products and services.

In a 2013 report, we found that the decentralized nature of Agency operations and longstanding culture of autonomy hindered NASA's ability to implement effective IT governance.[6] We made eight recommendations and NASA agreed to take action to address our concerns. In our 2017 follow-up audit, we evaluated NASA's progress in implementing changes to its IT governance structure and found that in the 4 years since issuance of our report and the 3 years since completion of its own internal review, the Agency's Office of the Chief Information Officer (OCIO) has made insufficient progress to improve NASA's IT governance, casting doubt on the office's ability to effectively oversee the Agency's IT assets. Specifically, the NASA Chief Information Officer (CIO) continues to have limited visibility into IT investments across the Agency and the process NASA developed to correct this shortcoming is flawed.

In 2016, NASA established the Annual Capital Investment Review (ACIR) as its formal response to a Federal mandate that CIOs have approval authority over all agency IT spending. The ACIR process is designed to collect IT investment data across NASA, including institutional, mission, and highly specialized IT, for review and approval by the Agency's senior IT governance board – a process expected to help increase the Agency CIO's authority in IT acquisition planning throughout NASA. Despite these efforts, the OCIO's insight into and control over the bulk of the Agency's nearly $1.4 billion in annual IT funding remains limited. In fact, NASA Mission Directorates and Centers still controlled $739 million (53 percent) and $311 million (22 percent), respectively, of IT spending in FY 2017. This lack of authority and visibility over the majority of the IT budget limits the Agency's ability to consolidate IT expenditures, realize cost savings, and drive improvements in the delivery of IT services.

In addition, we found the Agency's current enterprise architecture remains immature after a decade-long effort, a situation that contributes to the undisciplined manner in which NASA makes IT investments. Moreover, despite changes to two of the Agency's three top-level IT governance boards, IT managers across the Agency remain unsure of board functions and their decision making processes and the boards have yet to make strategic decisions that substantively impact how IT at NASA is managed. In addition, as of August 2017 the roles and responsibilities associated with NASA's IT governance structure have not been finalized by the OCIO – one of the most basic and critical pieces of the Agency's Business Services Assessment (BSA) Implementation Plan.

Lingering confusion about security roles coupled with poor IT inventory practices continues to negatively impact NASA's security posture. For example, while NASA's Senior Agency Information Security Officer (SAISO) is responsible for managing Agency-wide IT security, the Mission Directorates and Centers operate hundreds of networks and have their own IT security personnel responsible for security, risk determination, and risk acceptance on those systems – yet none of these personnel report to the SAISO. In addition, high turnover of senior IT managers, including the Agency CIO and the SAISO, have impacted NASA's IT operations, affected the Agency's ability to execute its IT governance structure, and hindered the Agency's ability to significantly improve NASA's IT security posture.

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

Finally, the OCIO continues to exercise limited ability to influence IT management within the Mission Directorates and Centers due to the autonomous nature of NASA operations and the office's lack of credibility on IT issues in the eyes of its customers.

To increase transparency, accountability, and oversight of NASA's IT investments and strengthen its governance framework, we made five recommendations to the CIO, which after further consultation, the Agency described acceptable corrective action to address them.

To view the full report, visit https://oig.nasa.gov/audits/reports/FY18/IG-18-002.pdf.

Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation (IG-18-003, November 6, 2017)

This annual report, submitted as a memorandum to the NASA Administrator, provides the OIG's independent assessment of NASA's information security posture. For FY 2017, we assessed NASA's information security policies, procedures, and practices by examining seven information systems. We also assessed the Agency's overall cybersecurity posture using a variety of techniques and leveraged work performed by other oversight organizations and by NASA. Finally, we evaluated the Agency's progress in addressing deficiencies identified in prior FISMA and information security reviews.

We found that information security remains a significant challenge for NASA. Although the Agency continues to make progress in implementing cybersecurity initiatives, its cybersecurity program remains ineffective when judged using the Office of Management and Budget criteria, which requires agencies to achieve a maturity level of 4 on a 5-point scale to be considered effective. In the five specific functions deemed essential for effective information security programs, NASA achieved maturity Level 2, indicating the Agency's information systems remain vulnerable to serious security threats.

That said, NASA has launched multiple initiatives over the past several years to improve its information security program, including the Risk Information Security Compliance System, Continuous Diagnostics and Monitoring program, and the Security Operations Center. Once fully implemented, these initiatives should help to address gaps in NASA's current IT cybersecurity posture and strengthen its risk management strategy.

To view this report, visit https://oig.nasa.gov/audits/reports/FY18/IG-18-003-R.pdf.

Audit of NASA's Fiscal Year 2017 Financial Statements (IG-18-005, November 15, 2017)

The OIG contracted with the independent public accounting firm CliftonLarsonAllen LLP (CLA) to audit NASA's FY 2017 financial statements. This audit resulted in an unmodified opinion on NASA's FY 2017 financial statements, meaning the financial statements present fairly, in all material respects, the financial position and results of NASA's operations in conformity with U.S. generally accepted accounting principles; however, CLA also reported a significant deficiency related to the Agency's IT management.

CLA found NASA did not substantially address deficiencies in its vulnerability management program identified in the prior year. The vulnerability management program continued to insufficiently address the monitoring, detection, and timely remediation of vulnerabilities associated with the financial application and general support systems. Specifically, a substantial number of critical and high severity

vulnerabilities (as well as medium and low vulnerabilities) remained outstanding for an excessive length of time, contrary to NASA policies and procedures. These weaknesses expose NASA to significant risk of exploitation.

CLA identified six key tasks that NASA should focus on to enhance its efforts to analyze and prioritize remediation efforts to address security and control deficiencies.

To read the full report, see the Financials section of NASA's FY 2017 Agency Financial Report at https://www.nasa.gov/sites/default/files/atoms/files/afr_fy2017_final_11_15_17.pdf.

ONGOING AUDIT WORK

Audit of NASA's Information Technology Supply Chain Risk Management Efforts (A-17-008-00, March 2, 2017)

NASA's IT operations rely on global supply chains to fulfill mission needs. Such reliance can pose a significant risk as foreign-developed or -manufactured technology may be compromised. The OIG is examining the effectiveness of NASA's security controls related to its IT supply chain risk management efforts. Specifically, we are assessing whether NASA has implemented Agency-wide controls to meet IT security requirements to protect the confidentiality, integrity, and availability of NASA data, computer systems, and networks.

Audit of NASA's Security Operations Center (A-17-009-00, March 2, 2017)

NASA's Security Operations Center (SOC) serves as the Agency's nerve center for detecting and monitoring security incidents and providing continuous event detection, situational awareness, and incident management and tracking. The OIG is assessing NASA's management of the SOC, including its capability, workload, and resource management.

INVESTIGATIONS

Export Restricted Software Released to Unauthorized Individuals

In June 2017, the OIG notified NASA of systematic weaknesses found in its software request and release processes. Specifically, NASA Counterintelligence and OIG investigators identified several instances in which individuals misrepresented themselves and illegally obtained export-restricted software from the Agency's *software.nasa.gov* website. Investigators also identified instances whereby export-restricted software was released to unknown individuals using foreign-registered Internet Protocol addresses.

In response, NASA temporarily removed 51 software codes controlled under the International Traffic in Arms Regulations from the website until it developed an improved vetting process. The Agency is also working with the Department of Homeland Security's remote identity verification vendor to enhance the proofing process for all remote non-NASA personnel who require access to NASA software. These improvements are anticipated to be completed in late FY 2018. Furthermore, a designee of the Agency's Senior Agency Information Security Officer will be part of the Software Release Working Group to ensure cybersecurity concerns are addressed.

University Professor Traveled Internationally with Export-Controlled Material

In August 2017, the OIG closed a case stemming from information obtained during Department of Homeland Security border searches of a university professor who on two separate occasions was found to be in possession of NASA export-controlled material subject to International Trafficking in Arms Regulations during international travel. Although the professor denied knowing any of the data was export-controlled and authorities declined to prosecute, the university said it had implemented corrective action to prevent future unauthorized release of export-controlled information.

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

Krista Paquin
Acting Deputy Administrator

Renee Wynn
Chief Information Officer

Al Condes
Associate Administrator, International and Interagency Relations

Daniel Tenney
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