NASA OFFICE OF INSPECTOR GENERAL

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

March 7, 2019

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

The Honorable José Serrano
Chairman
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Subject: *NASA's Compliance with Federal Export Control Laws* (IG-19-012)

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]

We last reported to you regarding these issues in February 2018. Since then, NASA has not established any new bilateral agreements with China. The Agency has continued its work with the Chinese Academy of Sciences on bilateral science activities relating to space geodesy and glacier research in the Himalaya Region.[2] NASA also participated in U.S. Department of State-led discussions with Chinese officials from

[1] Pub. L. No. 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.

the China National Space Administration about orbital debris mitigation and satellite collision avoidance. In addition, the NASA cooperative agreement 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 is still in force. Lastly, NASA officials continued engagement and information exchanges with its counterparts from the Chinese Academy of Science and China National Space Administration regarding their respective planetary exploration programs with a particular focus on lunar exploration. For each of these activities, the Agency made the appropriate notifications in accordance with the requirements outlined in Public Law 115-141.[3]

With regard to export control-related oversight work by our office, during the past year we completed four audits that examined NASA's controls over sensitive information and information technology (IT) assets and security systems, many of which contain data subject to export control laws. We also initiated two new audits related to IT security. In addition, our Office of Investigations closed three investigations related to the misuse and unauthorized access to export-controlled information. Furthermore, we are an active member of the U.S. 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 2018 export control and IT security systems work below.

ISSUED AUDIT REPORTS

NASA's Management of GISS: The Goddard Institute for Space Studies (IG-18-015, April 5, 2018)

Since its establishment in 1961, NASA's Goddard Institute for Space Studies (GISS) has collaborated with the world science community to research the structure of the Earth, Moon, and other planetary bodies; the atmospheres of Earth and the other planets; the origin and evolution of the solar system; the properties of interplanetary plasma; Sun-Earth relations; and the structure and evolution of stars. In fiscal year (FY) 2016, NASA provided 96 percent of GISS' $19.1 million annual funding, enabling the Agency's efforts to improve climate change predictions by better understanding the roles and interactions of the ocean, atmosphere, land, and ice in the climate system.

We examined NASA's management of GISS and found, among other issues, that contrary to NASA policy, 43 of 66 (65 percent) new GISS scientific publications publicly released from October 2015 through September 2017 were not approved by GISS or Goddard Space Flight Center officials prior to release. NASA policy requires a technical review, export control review, and a series of supervisory approvals and, if needed, a legal review for possible copyright or third-party information prior to release of scientific information. NASA's review procedures are designed to ensure the accuracy of scientific information released to the public and to prevent the inadvertent release of sensitive information.

[3] Consolidated Appropriations Act, 2018, Pub. L. No. 115-141 (2018) 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 order to ensure accurate scientific information is released to the public and to prevent sensitive information from inadvertent release, we recommended NASA's Chief Information Officer and the Chief of GISS ensure all NASA and GISS-generated publications must undergo a thorough and independent pre-publication review and approval process prior to release. NASA management partially concurred, stating that it will work with GISS management to leverage the review and approval process to prevent the release of restricted and sensitive information.

To view the full report, visit NASA's Management of GISS: The Goddard Institute for Space Studies.

Audit of NASA's Security Operations Center (IG-18-020, May 23, 2018)

NASA spends approximately $1.4 billion per year on IT investments for 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. Managing IT security incidents at NASA is a highly decentralized activity involving the Agency's Headquarters and nine Centers. In November 2008, NASA created the Security Operations Center (SOC) at Ames Research Center to identify and respond to Agency-wide security threats to NASA networks and IT systems. The SOC is staffed by 10 NASA civil service and 36 contractor personnel and received $14.7 million in funding for FY 2018.

We assessed NASA's management of the SOC and found the SOC has fallen short of its original intent to serve as NASA's cybersecurity nerve center. Due in part to the Agency's failure to develop an effective IT governance structure, the lack of necessary authorities, and frequent Office of the Chief Information Officer turnover in key leadership positions, these shortcomings have detrimentally affected SOC operations, limiting its ability to coordinate the Agency's IT security oversight and develop new capabilities to address emerging cyber threats. As a result, the SOC lacks the key structural building blocks necessary to effectively meet its IT security responsibilities.

We made six recommendations to ensure the SOC is best positioned to serve as the Agency's front line of cyber defense and better monitor, detect, and mitigate cyber incidents across NASA, to which the Agency concurred and described planned corrective actions.

To view the full report, visit Audit of NASA's Security Operations Center.

Audit of NASA's Information Technology Supply Chain Risk Management Efforts (IG-18-019, May 24, 2018)

Counterfeit IT and communications products represent an increasing threat to nations, governments, and companies around the world. According to industry estimates, 1 in 10 such products sold are counterfeit, equating to approximately $100 billion in counterfeit IT products. NASA spent approximately $1.4 billion in FY 2017 on computer systems, networks, and IT services used to control spacecraft, collect and process scientific data, and provide security for critical Agency infrastructure. The risk that IT and communications products entering the Agency's supply chain could be counterfeit presents a significant threat to NASA operations and could impair the Agency's ability to protect the confidentiality, integrity, and availability of its data, systems, and networks.

We examined the effectiveness of NASA's supply chain risk management efforts and found that while NASA has made improvements since the supply chain risk management process was first mandated in 2013, there remains pervasive weaknesses in the Agency's internal controls and risk management practices that lead us to question the sufficiency of its current efforts. Overall, the Agency's weak

controls have resulted in the purchase of non-vetted IT and communication assets, some of which we found present significant security concerns to Agency systems and data. In addition to our longstanding concerns about NASA's IT governance and security practices, the Agency compounds its security vulnerabilities by relying on ineffectual processes and information in its efforts to prevent risky IT products from entering its network environment.

We made seven recommendations for NASA management to strengthen security controls over the Agency's supply chain risk management, to which the Agency concurred and described planned corrective actions.

To view this report, visit Audit of NASA's Information Technology Supply Chain Risk Management Efforts.

Audit of NASA's Fiscal Year 2018 Financial Statements (IG-19-004, November 15, 2018)

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 2018 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, as it did last year, CLA also reported a significant deficiency related to the Agency's IT management.

CLA noted that while NASA was able to remediate several prior year findings, the Agency 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 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 eight key tasks that NASA should focus on to enhance its efforts to analyze and prioritize remediation efforts to address security and control deficiencies. The Agency responded by stating that it continues to improve the vulnerability management program and continues the deployment of improved system management and patching tools while continuing to address and strengthen other IT security controls.

To read the full report, see the Financial Section of NASA FY 2018 Agency Financial Report.

ONGOING AUDIT WORK

Review of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2018

In this required annual review, we are evaluating NASA's IT security program against the 2018 Federal Information Security Modernization Act (FISMA) metrics. Specifically, we are reviewing a sample of NASA- and contractor-owned information systems to assess the effectiveness of information security policies, procedures, standards, and guidelines. Additionally, we are evaluating whether NASA has addressed the deficiencies we identified in our prior FISMA reviews.

Audit of the Jet Propulsion Laboratory's Network Security

Protecting NASA's technical information housed at the Jet Propulsion Laboratory (JPL) is dependent in part on the strength of JPL's system and application control environment and its system configuration and patching process. This audit is assessing whether JPL has adequate processes in place to identify, control, and protect its IT systems and whether personnel responsible for those applications have the necessary training and expertise.

INVESTIGATIONS

Inappropriate Disclosure of Sensitive Information at the Jet Propulsion Laboratory

In February 2018, the OIG closed a case originating from the JPL Export Administrator's July 2017 report which indicated that export-controlled documents appeared to have been intentionally left unsecured, after a JPL security officer found such documents in plain view in an office. The security officer observed a sign that instructed individuals to avoid locking the office, and the office door lock had been tampered with to prevent it from locking. At the recommendation and approval of the OIG and NASA Management Office, JPL updated annual security training to ensure all employees understood the importance of safeguarding sensitive information and materials.

Export of Potentially Sensitive Technology

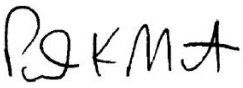
In April 2018, the NASA Headquarters Export Control Administrator made a full disclosure to the Department of State regarding the potential release of International Traffic in Arms Regulations (ITAR)-controlled technical data on a NASA computer. In December 2017, the NASA SOC notified the OIG of an incident regarding a NASA computer for sale on eBay potentially containing ITAR information. The OIG investigation revealed the seller, a Canadian citizen, acquired the computer in 2017 from a collector who is believed to have purchased it legally from the General Services Administration in 2006. The seller returned the computer hard drive to NASA and files related to older launch vehicle telemetry were removed. The Department of State accepted NASA's corrective actions and closed the case without further action or imposing a civil penalty.

Contractor Charged for Transferring Sensitive NASA Data to Personal Computer

In May 2018, a contractor employee was charged with violating NASA regulations for transferring ITAR and Export Administration Regulation data from his NASA-issued laptop to his personal computer and allowing a computer repair company access to the data. As a result of the violation, the contractor employee served 6 months of probation and paid a $500 fine in exchange for the charges being dismissed.

If you or your staff have any questions or 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: James Bridenstine
Administrator

James Morhard
Deputy Administrator

Stephen Jurczyk
Associate Administrator

Melanie Saunders
Deputy Associate Administrator

Janet Karika
Chief of Staff

Renee Wynn
Chief Information Officer

Sumara Thompson-King
General Counsel

Albert Condes
Associate Administrator for International and Interagency Relations

Daniel J. Tenney
Associate Administrator for Mission Support Directorate

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 Reform
Committee on Science, Space, and Technology