NASA OFFICE OF INSPECTOR GENERAL

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

February 6, 2023

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

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

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

The Honorable Matthew Cartwright
Ranking Member
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-23-009)

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 2022. Since then, NASA has not established any new bilateral agreements with China. NASA 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] In June 2021, NASA began to exchange limited information with the China National Space Administration to ensure the safety of NASA's robotic Mars science missions and international partners'

[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.

missions in orbit around Mars. NASA anticipates these discussions will continue for the life of the Tianwen-1 mission.[3] For each of these activities, the Agency made the appropriate notifications in accordance with the requirements outlined in Public Law 116-260.[4]

With regard to export control-related oversight work conducted by our office, during the past year we completed two 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 three new audits related to IT security. In addition, our Office of Investigations closed three investigations related to inappropriate associations with China and the misuse of and unauthorized access to NASA computer systems and 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 sharing activities among federal agencies to identify and resolve conflicts involving violations of U.S. export control laws.

We summarize our 2022 export control and IT security systems audits and investigations below.

AUDIT REPORTS ISSUED

NASA's Insider Threat Program (IG-22-009, March 14, 2022)

Cybersecurity threats posed by an organization's employees and contractors are commonly referred to as insider threats. Insiders typically fly under the radar of traditional security defenses, making it difficult to detect and prevent any improper activities. According to government and industry experts, the most common insider threats arise from: accidental leaks, which might originate from a phishing attack or from an employee forwarding a sensitive email to the wrong person; misuse of network access or database privileges, where an employee intentionally circumvents cybersecurity policies or procedures; and data theft, where an employee removes data from an organization with the intent of selling or otherwise inappropriately releasing it.

Given NASA's high-profile mission and broad connectivity with educational institutions, research facilities, and international partners, its risk exposure from insider threats is significant and varied. In this audit, we examined whether NASA has implemented an effective insider threat program in accordance with federal and Agency policies and cybersecurity leading practices. Specifically, we examined whether: (1) NASA's insider threat strategy provides an adequate framework for identifying malicious and unintentional insider threats; (2) NASA implemented appropriate procurement controls to identify and prevent intellectual data theft from foreign adversaries, and (3) NASA developed adequate cybersecurity controls to prevent, detect, and respond to the extraction or manipulation of data and intellectual property.

---

[3] Tianwen-1 is an interplanetary mission by the China National Space Administration that launched in July 2020 and landed a rover on Mars in May 2021.

[4] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260 (2020) requires NASA to certify to the Senate and House committees on Appropriations and the Federal Bureau of Investigation (FBI) no later than 30 days prior to the event 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.

NASA, like all federal agencies, is required to address insider threats on its classified systems, and we found the Agency has taken appropriate steps to implement an insider threat program for those systems. Specifically, we determined that NASA established user activity monitoring, developed mandatory Agency-wide insider threat training, and created an insider threat reference website that assists employees and contractors with identifying threats, risks, and follow-up information. Additionally, the Agency is strengthening procurement controls by expanding disclosure requirements and updating procedures to address the risks of foreign influence.

While NASA has a fully operational insider threat program for its classified systems, the vast majority of the Agency's IT systems—including many containing high-value assets or critical infrastructure—are unclassified and are therefore not covered by its current insider threat program. Consequently, the Agency may be facing a higher-than-necessary risk to its unclassified systems and data. While NASA's exclusion of unclassified systems from insider threat programs is common among federal agencies, adding those systems to a multi-faceted security program could provide an additional level of maturity to the program and better protect agency resources. According to Agency officials, expanding the insider threat program to unclassified systems would benefit the Agency's cybersecurity posture if incremental improvements, such as focusing on IT systems and people at the most risk, were implemented. However, ongoing concerns including staffing challenges, technology resource limitations, and lack of funding to support such an expansion would need to be addressed prior to enhancing the existing program.

The cross-discipline challenges surrounding cybersecurity expertise further amplify the complexities of insider threats. At NASA, responsibilities for unclassified systems are largely shared between the Office of Protective Services and the Office of the Chief Information Officer. In addition, the Office of Procurement manages Agency contracts, while the Office of the Chief Financial Officer manages grants and cooperative agreements. Nonetheless, in our view, mitigating the risk of an insider threat is a team sport in which a comprehensive insider threat risk assessment would allow the Agency to gather key information on weak spots or gaps in administrative processes and cybersecurity. At a time when there is growing concern about the continuing threats of foreign influence, taking the proactive step to conduct a risk assessment to evaluate NASA's unclassified systems ensures that gaps cannot be exploited in ways that undermine the Agency's ability to carry out its mission.

We made two recommendations to strengthen the insider threat program; the Agency concurred with both of them. One recommendation is now closed, and the Agency plans to implement corrective action for the second by December 2023.

To view the full report, visit NASA's Insider Threat Program.

NASA Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2022 (IG-23-006, December 19, 2022)

The Federal Information Security Modernization Act of 2014 (FISMA) requires the NASA Office of Inspector General (OIG), or an independent external auditor, to conduct an annual evaluation of NASA's information security program. The OIG selected the independent public accounting firm RMA Associates, LLC (RMA) to evaluate NASA's information security program in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* and against the fiscal year 2022 Inspector General FISMA Reporting Metrics (IG Metrics). The evaluation rated NASA's information security program at a Level 3 (Consistently Implemented), which means

policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking. This rating fell short of the Office of Management and Budget's goal that agency cybersecurity programs should be considered "Effective."

RMA determined the maturity level for all five cybersecurity functions (Identify, Protect, Detect, Respond, Recover) based on testing of 20 questions in the 2022 IG Metrics. The Identify and Detect functions were rated at a Level 2 (Defined) while the remaining three functions were rated at a Level 3 (Consistently Implemented).

For the Identify function, information contained in NASA's Risk Information Security Compliance System—the system of record for information systems—was not consistently current. Specifically, for the operational systems tested, NASA did not have up-to-date authorizations to operate, perform business impact analyses, or complete system inventory information. The Agency also did not have policies, procedures, and processes for risk framing, response, and monitoring to manage cybersecurity risks and comply with federal requirements.

NASA made progress in implementing its supply chain risk management processes measured as part of the Identify function; however, the Agency did not provide sufficient evidence of completed supply chain risk reviews. In addition, NASA needs to include its supply chain risk reviews in the continuous monitoring practices noted in its Information Security and Continuous Monitoring (ISCM) strategy. The lack of a process for supplier risk evaluation leads to an increase in supplier-related risks where adversaries could target and compromise weaknesses in the supply chain for both commercial off-the-shelf and custom information systems and components, leading to the denial, disruption, or degrading of the function of NASA systems.

For the Detect function, while NASA developed an ISCM strategy, the strategy was not updated in accordance with the latest federal requirements. Additionally, the Agency did not have a formal process to document and implement ISCM lessons learned to improve its existing control effectiveness. Finally, NASA did not consistently perform ongoing authorization and assessment.

RMA made 17 recommendations to address deficiencies across all 5 functions. NASA concurred or partially concurred with 16 and plans to take correction action by November 2023. Management did not concur with one recommendation, which will be followed up by RMA during the fiscal year 2023 evaluation.

To view the full report, visit NASA Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2022.

ONGOING AUDIT WORK

NASA's Software Asset Management

NASA uses thousands of unique software products from hundreds of vendors in its efforts to advance science, technology, aeronautics, Earth studies, and space exploration. Each software application and program comes with a license governing its use—a contract between the entity creating or supplying the software and the end user. In this audit, we assessed whether NASA is managing its software assets in an effective and efficient manner while maintaining compliance with applicable requirements and security best practices. We issued our report in January 2023, outside the reporting timeframe for this 2022 letter. To view the full report, visit NASA's Software Asset Management.

Audit of NASA's Artificial Intelligence Capabilities

NASA deploys artificial intelligence applications to conduct space research—such as automating image analysis for galaxy, planet, and star classifications—and to develop autonomous space probes that can avoid space junk without human involvement. This audit is reviewing NASA's progress in developing its artificial intelligence governance frameworks and policies and will assess whether security controls have been implemented to protect artificial intelligence data and technologies.

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2023

Required by the Federal Information Security Modernization Act of 2014, the fiscal year 2023 evaluation of NASA's information security program will be conducted by the independent public accounting firm RMA Associates, LLC, with oversight by OIG staff.

INVESTIGATIONS

University of Arkansas Professor Sentenced

A University of Arkansas professor and principal investigator on a NASA grant was sentenced to 12 months in prison, 12 months of supervised release, and a $5,000 fine after conviction on one count of making a false statement to the FBI about the existence of patents for his inventions in China.

Former Senior NASA Scientist Debarred for Three Years

A former chief scientist at Ames Research Center was debarred for three years after being convicted and sentenced to 30 days of imprisonment and ordered to pay a $100,000 fine for making false statements to the FBI and NASA OIG regarding his employment by a Chinese government-funded program that recruited individuals with access to foreign technologies and intellectual property.

Former University Professor Pleads Guilty to Concealing Ties to Chinese Entities

A former professor at a Texas university pled guilty to not disclosing his association with entities in China while receiving NASA grant funds, which violated the NASA China Funding Restriction. The professor was sentenced to time served (approximately 12 months) and ordered to pay a $20,000 fine and $86,876 in restitution to NASA.

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.

PAUL MARTIN

Digitally signed by PAUL MARTIN
Date: 2023.02.03 12:58:19 -05'00'

Paul K. Martin
Inspector General

cc: Bill Nelson
Administrator

Pamela Melroy
Deputy Administrator

Robert Cabana
Associate Administrator

Susie Perez Quinn
Chief of Staff

Jeff Seaton
Chief Information Officer

Charles Polen
Acting General Counsel

Karen Feldstein
Associate Administrator for International and Interagency Relations

Robert Gibbs
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 Accountability
Committee on Science, Space, and Technology