NASA OFFICE OF INSPECTOR GENERAL

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

February 3, 2022

The Honorable Jeanne Shaheen
Chair
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 Matt Cartwright
Chair
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

The Honorable Robert B. Aderholt
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-22-008)

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 2021. Since then, NASA has not established any new bilateral agreements with China. The Agency's cooperative agreement with the Chinese Aeronautical Establishment to collaborate on aeronautics research that we disclosed last year expired in September 2021 and was not renewed. That said, NASA has continued its work with the Chinese Academy of Sciences on bilateral science activities relating to space geodesy and glacier research in the

[1] Pub. L. No. 106-391, codified at 51 U.S.C. § 30701(a)(3).

Himalaya Region.[2] In addition, 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' missions in orbit around Mars. NASA anticipates these discussions will continue through July 2022. For each of these activities, the Agency made the appropriate notifications in accordance with the requirements outlined in Public Law 116-260.[3]

With regard to export control-related oversight work conducted by our office, during the past year we completed five 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 one new audit related to IT security. In addition, our Office of Investigations closed six investigations related to 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 2021 export control and IT security systems audits and investigations below.

AUDIT REPORTS ISSUED

Fiscal Year 2020 Federal Information Security Modernization Act Examinations

The Federal Information Security Modernization Act of 2014 (FISMA) requires that we conduct annual independent evaluations of information security programs and practices at NASA and report the results to the Office of Management and Budget (OMB). In October 2020, we reported to OMB that NASA's information security program was not fully effective for FY 2020. Since we last reported to you, we issued three memoranda based on our review of a sample of NASA- and contractor-owned information systems.[4] The results of the examinations are summarized below:

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Communications System (IG-21-013, February 16, 2021)

Our examination of an Agency-operated information system known as a Center Communications System operated at Marshall Space Flight Center found that NASA had not taken corrective action to address information security control deficiencies in a timely manner. Specifically, we found that NASA failed to

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

[3] 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.

[4] The specific names of the NASA- and contractor-owned information systems tested during these evaluations have been generalized to protect their operational security. We issued a fourth FISMA memorandum in December 2020 and reported those results in last year's export control letter. NASA OIG, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – An Agency Common System* (IG-21-010, December 22, 2020).

prepare a Plan of Action and Milestones or Risk-Based Decision documents for information security controls that were deemed ineffective during recent security assessments, which are performed periodically by NASA as part of its continuous monitoring process. As a result, information security controls for the Center Communications System face unnecessary risks that—until the ineffective controls have been properly mitigated—may threaten the confidentiality, integrity, and availability of information that is processed, stored, or transmitted by the system. We made two recommendations to improve NASA's management of the Center Communications System; the Agency concurred and implemented corrective action, and the recommendations are now closed.

To view the full report, visit Fiscal Year 2020 Federal Information Security Modernization Act Evaluation-A Center Communications System

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Command and Control System (IG-21-014, March 2, 2021)

We also examined an Agency-operated information system known as a Center Command and Control System, located at Kennedy Space Center. We found that approximately 11 percent of the security controls we reviewed were overdue for independent assessment. As a result, NASA lacks assurance that system security controls are implemented correctly, operating as intended, and are producing the desired security outcomes. We made two recommendations that the Agency concurred with and plans to implement by August 2022.

To view the full report, visit Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Center Command and Control System

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Contractor-Operated Communications System (IG-21-015, March 24, 2021)

We examined an information system known as a Contractor-Operated Communications System, managed for Glenn Research Center. We found that NASA failed to update or maintain significant portions of required security information and documentation for the system in the Risk Information Security Compliance System (RISCS) database. Further, for the system security documentation maintained outside of RISCS, we identified numerous instances of security controls that contained inaccurate or missing information, including missing Plan of Action and Milestones, Risk-Based Decision documents, and contingency plans. As a result, Agency stakeholders do not have complete and accurate information when making information security decisions about this system—decisions that could affect the confidentiality, integrity, and availability of NASA-maintained information in the Contractor-Operated Communications System. We made three recommendations; the Agency concurred and implemented corrective action, and the recommendations are now closed.

To view the full report, visit Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – A Contractor-Operated Communications System

NASA's Cybersecurity Readiness (IG-21-019, May 18, 2021)

Given its high-profile mission and broad connectivity with the public, educational institutions, and outside research facilities, NASA presents cybercriminals a larger potential target than most government agencies. NASA's vast online presence of approximately 3,000 websites and more than 42,000 publicly

accessible datasets also makes it highly vulnerable to intrusions. In recent years, the Agency has worked to improve its cybersecurity readiness with efforts led by the Office of the Chief Information Officer (OCIO). Nonetheless, in the last 4 years alone NASA experienced more than 6,000 cyber-attacks, including phishing scams and introduction of malware into Agency systems. Consequently, it is vital that the Agency continue to develop strong cybersecurity practices to protect itself from current and future threats.

To assess NASA's cybersecurity readiness, we examined whether: (1) the OCIO enterprise architecture is designed to appropriately assess cybersecurity risks and threats; (2) NASA's cybersecurity protection strategy is risk-based; (3) cybersecurity resource allocations are adequate and appropriately prioritized; and (4) Agency cybersecurity risks are effectively assessed using sound IT security practices.

Attacks on NASA networks are not a new phenomenon, although attempts to steal critical information are increasing in both complexity and severity. As attackers become more aggressive, organized, and sophisticated, managing and mitigating cybersecurity risk is critical to protecting NASA's vast network of IT systems from malicious attacks or breaches that can seriously inhibit the Agency's ability to carry out its mission. Although NASA has taken positive steps to address cybersecurity in the areas of network monitoring, identity management, and updating its IT Strategic Plan, it continues to face challenges in strengthening foundational cybersecurity efforts.

We found that NASA's ability to prevent, detect, and mitigate cyber-attacks is limited by a disorganized approach to Enterprise Architecture. Enterprise Architecture and Enterprise Security Architecture—the blueprints for how an organization analyzes and operates its IT and cybersecurity—are crucial components for effective IT management. Enterprise Architecture has been in development at NASA for more than a decade yet remains incomplete while the manner in which the Agency manages IT investments and operations remains varied and ad hoc. Unfortunately, a fragmented approach to IT, with numerous separate lines of authority, has long been a defining feature of the environment in which cybersecurity decisions are made at the Agency. The result is an overall cybersecurity posture that exposes NASA to a higher-than-necessary risk from cyber threats.

We also noted that NASA conducts its assessment and authorization (A&A) of IT systems inconsistently and ineffectively, with the quality and cost of the assessments varying widely across the Agency. These inconsistencies can be tied directly to NASA's decentralized approach to cybersecurity. NASA plans to enter into a new Cybersecurity and Privacy Enterprise Solutions and Services (CyPrESS) contract intended to eliminate duplicative cyber services, which could provide the Agency a vehicle to reset the A&A process to more effectively secure its IT systems.

We made five recommendations to strengthen NASA's cybersecurity readiness and provide process continuity and improved security posture for NASA's systems, all of which Agency management concurred with and plans to implement by December 2022.

To view the full report, visit NASA's Cybersecurity Readiness.

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2021 (ML-22-001, November 9, 2021)

For the FY 2021 FISMA evaluation, Inspectors General were required to assess 66 metrics in 5 security function areas and test a subset of information systems to determine the maturity of their agency's

information security program. To fulfill this requirement, we assessed NASA's information security policies, procedures, and practices by examining four judgmentally selected Agency information systems along with their corresponding security documentation.

In sum, we rated NASA's cybersecurity program at a Level 3 (Consistently Implemented), which marks an increased maturity level over the past four years. However, this year's maturity level still falls short of the Level 4 rating (Managed and Measurable) that OMB requires for an agency's cybersecurity program to be considered effective. As required, we submitted the results of this review through the Department of Homeland Security web portal on October 26, 2021. We did not make any recommendations but encouraged the Agency to continue to mature its information security program and strengthen its cybersecurity efforts.

To view the full report, visit Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2021.

ONGOING AUDIT WORK

Audit of NASA's Insider Threat Program

Threats posed by an organization's employees and contractors are commonly referred to as "insider threats," and detecting those threats is one of the biggest challenges that cybersecurity programs face. Space is both a collaborative and competitive business; given its high-profile mission and broad connectivity with the public, educational institutions, research facilities, international partners, and other outside organizations, NASA's potential insider threats are as varied as its missions. This audit is examining to what extent NASA has implemented an effective insider threat program in accordance with federal policies, Agency policies, and best practices.

INVESTIGATIONS

Jet Propulsion Laboratory Employee Terminated for Export Control Violations

As the result of our investigation, a former NASA Jet Propulsion Laboratory employee was terminated for allowing a foreign national to work on a project involving export-controlled information despite having certified to the contrary.

Former Contractor Barred from Center Access Due to IT Security Violations

A former Langley Research Center contractor used an Australian firm for data processing without obtaining proper approvals from NASA and willfully circumvented export control regulations to do so. Our investigation resulted in Langley management indefinitely suspending the contractor's Center access and taking remediation steps to prevent similar incidents from occurring.

Senior NASA Scientist Sentenced for Making False Statements Related to Chinese Thousand Talents Program Participation

A former chief scientist at Ames Research Center was 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 NASA Contractor Sentenced for Theft of Laptops

As the result of a NASA OIG investigation, a former NASA contractor employee pleaded guilty to one count of theft for stealing 43 contractor-owned laptops, some of which contained export control and proprietary information, and was ordered to pay $1,247 in restitution to the NASA contractor.

University Researcher Removed from Cooperative Agreement for Ties to China

A researcher was removed from working on a cooperative agreement between the University of California San Diego and NASA due to his membership in the Chinese Academy of Surveying and Mapping. Our investigation determined the cooperative agreement prohibited bilateral participation with China or China-owned entities. Although the case was declined for prosecution, the University of California San Diego reversed payments of $46,124 made to the researcher and removed him from the project.

Marshall Space Flight Center Employee Shares Export Controlled Data

A former Marshall Space Flight Center employee potentially violated export control laws by collaborating and sharing data with a researcher in Taiwan. At the time, NASA did not have any agreements in place with the country. Although the case was declined for prosecution, NASA management terminated the employee's access to Agency systems and the employee has since retired.

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: 2022.02.03 08:37:16 -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

Sumara M. Thompson-King
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 Reform
Committee on Science, Space, and Technology