NASA OFFICE OF INSPECTOR GENERAL

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

February 10, 2021

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 Matt Cartwright
Chairman
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-21-012)

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 2020. Since then, NASA has not established any new bilateral agreements with China. That said, 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 Himalayan Region.[2] In addition, NASA's cooperative agreement with the Chinese Aeronautical

[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.

Establishment to collaborate on aeronautics research intended to advance air traffic management and improve safety and efficiency for U.S. and Chinese aviation operations in China remains in force. Lastly, in December 2020 NASA officials informed Congress that they plan to initiate discussions with the China National Space Administration and exchange limited information to ensure the safety of NASA's robotic Mars science missions and our 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 116-93.[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 two new audits related to IT security. In addition, our Office of Investigations closed seven investigations related to inappropriate associations with China (we currently have 20 active cases) 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 2020 export control and IT security systems audits and investigations below.

AUDIT REPORTS ISSUED

NASA's Management of Distributed Active Archive Centers (IG-20-011, March 3, 2020)

Data generated by the Agency's Earth science missions is stored at 12 Distributed Active Archive Centers (DAAC) across the country. Located at NASA Centers, universities, and other federal agencies, DAACs are responsible for processing, archiving, and distributing data. Over the next 6 years, the volume of Earth observation data NASA will need to archive is expected to increase from 32 petabytes to 247 petabytes (1 petabyte of storage is the equivalent of 1.5 million CD-ROM discs) when several high-data-volume missions, such as the NASA-Indian Space Research Organization Synthetic Aperture Radar (NISAR) and the Surface Water and Ocean Topography (SWOT), come online.[4]

One of the objectives of this audit was to evaluate the extent to which NASA addressed data integrity risks. We found that while DAAC security plans generally followed NASA and National Institute of Standards and Technology (NIST) requirements, the Agency deviated from the NIST-recommended "moderate" impact level for data integrity. When conducting its security assessment, the Agency assessed a DAAC's impact level based on its ability to reprocess data in the event it was improperly

[3] Consolidated Appropriations Act, 2020, Pub. L. No. 116-93 (2019) requires NASA to certify to the Senate and House Committees on Appropriations and the Federal Bureau of Investigation 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] NISAR is scheduled to launch in 2022 and will measure Earth's changing ecosystems, dynamic surfaces, and ice masses providing information about biomass, natural hazards, sea level rise, and groundwater, and will support a host of other applications. SWOT is also scheduled to launch in 2022 and is designed to make the first-ever global survey of Earth's surface water and will collect detailed measurements of how water bodies on Earth change over time.

modified or destroyed rather than on the overall value of the DAAC and its underlying data. In addition, managers excluded critical information types when conducting impact determinations. This occurred because responsible individuals misinterpreted NASA and NIST categorization guidance due to a lack of close Office of Chief Information Officer (OCIO) involvement. To help ensure data processed by a DAAC is adequately protected, NIST provides guidance for system categorization, including a library of information types with recommended impact levels to determine whether a system should operate at a low, moderate, or high impact level. Failure to appropriately categorize systems and data can result in inadequate controls for protecting the confidentiality, integrity, and availability of the system and/or its data.

To address this risk, we recommended that NASA specify in Agency guidance that coordination with OCIO occur early in a mission's life cycle during data management plan development and ensure all applicable information types are considered during DAAC categorization. NASA management concurred with the recommendations and anticipates completing the corrective action in June 2021.

To view the full report, visit NASA's Management of Distributed Active Archive Centers.

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019 (IG-20-017, June 25, 2020)

In fiscal year (FY) 2019, NASA spent approximately $2.3 billion on computer systems, networks, and IT services used to control spacecraft, collect and process scientific data, and provide security for critical Agency infrastructure, among other things. Given NASA's mission and the valuable technical and intellectual capital it produces, the information maintained within the Agency's IT infrastructure presents a high-value target for hackers and criminals.

To determine the effectiveness of an agency's information security program, the Federal Information Security Modernization Act of 2014 (FISMA) requires each agency's Inspector General or an independent external auditor to conduct an annual independent evaluation and report the results to the Office of Management and Budget (OMB). In October 2019, we reported to OMB that for FY 2019 NASA's information security program was rated at Level 2, "Defined," out of five levels, with Level 5, "Optimized," being the most effective. In this evaluation, we further examined NASA's information security program based on the FISMA guidance and assessed NASA's cybersecurity documentation and practices, analyzed the Agency's inventory of network and information systems, and reviewed six NASA information systems for compliance with FISMA requirements.

We found that NASA has not implemented an effective Agency-wide information security program. Documentation for all six information systems we reviewed contained numerous instances of incomplete, inaccurate, or missing information. We also performed a limited review of the NASA system that aggregates and manages common controls across all Agency information systems and found that many controls were classified as "other than satisfied," indicating they had been assessed as less than effective. Moreover, the OCIO has not addressed these deficiencies. These weaknesses occurred because Center Chief Information Security Officers are responsible for managing large portfolios of information systems and do not always have resources available to ensure the data for each system is accurate and complete. Further, NASA information security personnel are not sufficiently aware of Agency information security policies and procedures, and the current oversight process does not ensure that delinquent information security assessments are identified and mitigated. As a result, information

systems throughout the Agency face an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of NASA's information.

We made nine recommendations to strengthen the Agency's information security program, all of which Agency management agreed to and anticipates implementing by the end of October 2021.

To view the full report, visit Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019.

NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices (IG-20-021, August 27, 2020)

Smartphones, tablets, and laptops are integral to the work of NASA employees and their contractor, academic, federal, and international partners. However, use of this equipment to connect to NASA non-public networks and systems increases opportunities for individuals and organizations to improperly access Agency data. Although NASA does not generally permit personally-owned mobile devices and laptops to access Agency networks and systems, certain authorized mobile devices and users are allowed to access NASA's enterprise email system if they adhere to specified business rules. Additionally, based on the terms of their respective agreements with NASA, partners may be allowed to use their own computers to access the Agency's enterprise and mission networks and systems with proper authorization.

We conducted this audit to assess the Agency's policy and practices regarding the use of non-NASA devices to conduct Agency business. Specifically, we evaluated whether NASA (1) addressed challenges related to non-NASA IT devices gaining unauthorized access to its networks and systems; (2) adequately monitored connection of authorized mobile devices to its enterprise email system; and (3) adequately implemented policy and procedures for non-NASA IT devices accessing NASA networks and systems.

We found that NASA is not adequately securing its networks from unauthorized access by IT devices. Although OCIO has deployed technologies to monitor unauthorized IT device connections, it has not fully implemented controls to remove or block these devices from accessing NASA's networks and systems. The initial December 2019 target date for NASA to complete installation of these controls has been delayed due to technological challenges and changes in OCIO mission priorities and requirements.

In addition, while OCIO established a process to enable secure email access on personal mobile devices, it is not adequately monitoring and enforcing the business rules necessary for granting such access. For example, NASA does not adequately assess whether users accessing its email system have a business need to use a personal mobile device or if the mobile device is ineligible for participation in the service because it violates supply chain controls—all of which increases the risk of the device being exploited. This is because OCIO did not establish monitoring and enforcement requirements when planning development and implementation of the project.

Further, while NASA has improved its overall IT security posture in recent years, we found OCIO's visibility into IT authorization practices at its numerous Centers and facilities around the country remains limited. Although NASA's Chief Information Officer (CIO) is responsible for developing, documenting, and implementing the Agency-wide information security program, OCIO relies on Center-based CIOs and staff to implement and enforce the Agency's information security policies. This practice has allowed Centers to tailor processes to meet their own priorities, which has in turn led to inconsistent implementation of NASA's enterprise-wide IT security management and could also

hinder NASA-wide efforts to gauge unauthorized access to Agency networks and systems and render Agency IT assets more vulnerable to cybersecurity attacks. For example, according to a NASA Security Operations Center FY 2019 fourth quarter threat report, 12 NASA Centers and facilities experienced incidents that involved individuals gaining unauthorized access from IT devices to the Agency's non-public networks, systems, and data. This was a 36-percent increase in incidents from the previous quarter and resulted in the loss and exposure of personally identifiable information, International Traffic in Arms Regulations data, Export Administration Regulation data, and sensitive but unclassified data, costing NASA $92,737 to mitigate the damages.

We made five recommendations to improve NASA's management of non-NASA IT device access to Agency networks and systems, with which the Agency concurred and anticipates implementing by the end of December 2021.

To view the full report, visit Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices.

Audit of NASA's Fiscal Year 2020 Financial Statements (IG-21-005, November 16, 2020)

The OIG contracted with the independent public accounting firm CliftonLarsonAllen LLP (CLA) to audit NASA's fiscal year 2020 financial statements, which resulted in a "clean" or unmodified opinion 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 the past 5 years, CLA also reported a significant deficiency related to the Agency's IT security management.

CLA noted that NASA has remediated several prior year findings related to specific vulnerabilities and has incorporated a program aimed at reducing vulnerability totals and meeting vulnerability remediation timelines. However, NASA's vulnerability management program has not matured to the extent that vulnerabilities associated with the financial application and general support systems are remediated consistently and in a timely manner, in accordance with NASA-established risk prioritization and security policies and procedures. Specifically, CLA found that (1) systems, applications, and networks supporting financial applications were not patched in accordance with NASA guidelines; (2) operating systems and applications were inadequately configured; and (3) systems and programs that were no longer fully supported by the associated software vendors remained in place. CLA stated that these weaknesses expose NASA to a significant risk of exploitation.

CLA also noted specific deficiencies in NASA's defense-in-depth approach intended to implement security controls at each layer of the IT environment in order to comprehensively address security risks from vulnerabilities. Furthermore, NASA did not follow internal and federal standards in implementing configuration management and access controls as required by its IT security handbook, OMB, and NIST.

CLA identified seven 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 as well as its defense-in-depth approach related to its financial systems' general application controls, and will continue to evaluate the need for additional improvements.

To read the full report, see the Financial Section of FY 2020 Agency Financial Report.

Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – An Agency Common System (IG-21-010, December 22, 2020)

The Federal Information Security Modernization Act of 2014 (FISMA) requires that we conduct annual independent evaluations of information security programs and practices at NASA. As part of this year's evaluation of NASA's information security program, we examined the security policies, procedures, practices, and controls for an Agency-operated information system known as an Agency Common System (ACS), an information system that is responsible for the administration and management of all NASA information system common controls.[5]

NASA has not taken corrective action to address a longstanding deficiency regarding controls previously assessed as ineffective. We also found that a software error permitted an unauthorized data change in the Agency's information security database affecting the accuracy of the assessment status of a control. Further, we found that NASA faced delays in its plans to authorize the Agency's new hybrid common controls system, which serves as the central repository for the Agency's hybrid common controls.[6] Lastly, NASA did not develop cost estimates for the remediation of these control deficiencies. As a result, information systems throughout the Agency face unnecessary risks that may threaten the confidentiality, integrity, and availability of NASA's information.

We made five recommendations to improve NASA's management of the ACS. Although Agency management concurred with only three of the recommendations, we assessed the information provided and the proposed actions being taken as responsive to all the recommendations. NASA management anticipates implementing the corrective actions by the end of March 2022.

To view the full report, visit Fiscal Year 2020 Federal Information Security Modernization Act Evaluation – An Agency Common System.

ONGOING AUDIT WORK

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2020

In this required annual review, we are evaluating NASA's IT security program against the FY 2020 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 identified in our prior FISMA reviews.

NASA's Cybersecurity Readiness

NASA's high-profile and advanced technology makes the Agency's computer systems and networks an attractive target for cyber intruders. In this audit, we are assessing whether NASA is adequately

[5] The specific name of the NASA information system tested during this evaluation was generalized to protect its operational security.

[6] The OCIO manages Agency-wide common controls that provide a security capability for multiple information systems at NASA's various locations, as well as other Agency-wide common controls that have both system-specific and common characteristics. These latter controls are known as "hybrid common controls."

prepared to identify and respond to cyberattacks and has the IT infrastructure in place to deal with new and emerging threats while maintaining cyber resiliency in light of the evolving threat landscape.

INVESTIGATIONS

Company Found to Engage in Illegal Transfer of International Traffic in Arms Regulations (ITAR) Material

A shell company was used to evade a 2-year government-wide suspension of the owner's legitimate company. Our investigation revealed that the shell company used ghost employees—a type of payroll fraud—and engaged in illegal transfer of ITAR material and associated payments with overseas banks. Although criminal and civil actions against the owners were ultimately declined, information provided to NASA prevented the award of new contracts.

Contract Employee Debarred for Concealing Chinese Origin of Materials

A former employee of a contractor that supplied steel tubing to transport rocket fuel to the Space Launch System and Orion was indicted and found guilty of one count of mail fraud and two counts of false statements and subsequently debarred for 3 years for concealing that the tubing materials was of Chinese origin in violation of contract requirements. NASA tested the suspect tubing and it failed to meet contractual specifications.

Senior Scientist Pleads Guilty to Making False Statements Related to Chinese Thousand Talents Program

The Chief Scientist, Exploration Technology at the Center for Nanotechnology at Ames Research Center pled guilty to making false statements, a charge that carries a maximum sentence of 5 years in prison and a maximum fine of $250,000. The scientist, who was prevented from conducting further NASA research, participated in China's Thousand Talents Program, which was established by the Chinese government to recruit individuals with access to or knowledge of foreign technology or intellectual property. He also held professorships at universities in China, South Korea, and Japan, and failed to disclose these associations and positions to NASA.

Suspect Pleads Guilty to Stealing Laptops that Contained Export Control Data

A warehouse employee plead guilty to stealing 43 laptop devices owned by Hewlett-Packard under the NASA Agency Consolidated End-user Services contract. The employee, who was subsequently fired, worked at the subcontractor facility in Brunswick, Ohio, where the laptops were taken for disposition. Our analysis of the recovered laptops found that five of them contained export control, proprietary, personally identifiable information, and other sensitive data. NASA remediated potential security risks to the data owners and offered identity protection to those individuals whose information was exposed.

University Researcher Indicted for Concealing Affiliation with a Chinese University

A researcher at the University of Tennessee was indicted on three counts of wire fraud and three counts of false statements in an attempt to defraud NASA. He was also fired by the University and suspended from federal government contracting. The researcher allegedly committed these crimes to conceal his

affiliation with the Beijing University of Technology. Federal law prohibits the use of appropriated funds on collaborative projects with China or its universities. As a result of the researcher's actions, the University of Tennessee unknowingly falsely certified its compliance with the law.

University Researcher Indicted for Concealing Affiliation with China-based Companies

A University of Arkansas researcher was indicted on 42 counts of wire fraud and 2 counts of passport fraud and suspended from federal government contracting for concealing his affiliation with various companies based in China while simultaneously receiving grants from the U.S. government. The researcher has been fired by the University and suspended from government contracting pending resolution of the criminal case.

University Researcher Indicted for Concealing Affiliation with a Chinese University

A Texas A&M University researcher was indicted on one count of conspiracy, seven counts of wire fraud, and nine counts of making false statements for concealing his affiliation with a university in China while receiving grants from NASA. The researcher is alleged to have personally benefited from his affiliation with Texas A&M and NASA, gaining increased access to unique NASA resources, such as the International Space Station. This access allegedly allowed him to further his standing in China at Guangdong University of Technology and other universities.

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 K. Martin
Inspector General

cc: Stephen G. Jurczyk
Acting Administrator

Melanie Saunders
Deputy Associate Administrator

Bhavya Lal
Acting 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