NASA OFFICE OF INSPECTOR GENERAL

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

February 20, 2020

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

The Honorable Jeanne Shaheen
Ranking Member
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

The Honorable Robert 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-20-010)

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 March 2019. 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

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

Region.[2] NASA also participated in a forum involving 11 space agencies that was attended by representatives from the Chinese Academy of Sciences, the China Academy of Space Technology, the China Astronautics Standards Institute, and several Chinese universities to discuss developing international standards for space data and information transfer systems. 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 remains in force. Lastly, NASA officials continued engagement and information exchanges with their 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 116-6.[3]

With regard to export control-related oversight work conducted by our office, during the past year we completed three 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 six investigations related to the misuse 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 2019 export control and IT security systems work below.

AUDIT REPORTS ISSUED

Review of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2018 Evaluation (ML-19-002, March 6, 2019)

In this annual review, we were required to assess 61 metrics in 5 IT security function areas and test a subset of information systems to determine the maturity of NASA's information security program. We assessed NASA's information security policies, procedures, and practices by examining seven judgmentally selected Agency information systems along with their corresponding security documentation.

For the second year in a row, we rated NASA's cybersecurity program at a Level 2, which falls short of the Level 4 rating agency cybersecurity programs are required to meet by the Office of Management

[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, 2019, Pub. L. No. 116-6 (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.

and Budget in order to be considered effective.[4] We also found that system security plans contained missing, incomplete, and inaccurate data, and information system control assessments were not conducted in a timely manner. We consider the issue of missing, incomplete, and inaccurate information security plan data to be an indicator of a continuing control deficiency we identified in past audits. Likewise, the untimely performance of information security control assessments could indicate control deficiencies and possibly significant threats to NASA operations, which could impair the Agency's ability to protect the confidentiality, integrity, and availability of its data, systems, and networks. We communicated these issues to NASA management and plan to more fully explore them during our fiscal year 2019 evaluation.

To view the full report, visit Review of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2018 Evaluation.

Cybersecurity Management and Oversight at the Jet Propulsion Laboratory (IG-19-022, June 18, 2019)

NASA's Jet Propulsion Laboratory (JPL) is a federally funded research and development center in Pasadena, California. Since 1959, the California Institute of Technology (Caltech) has been under contract with NASA to manage JPL, most prominently its research and development activities, but also its network security controls. JPL's IT systems maintain a wide public internet presence while supporting missions and networks that control spacecraft, collect and process scientific data, and perform critical operations. Over the past 10 years, JPL has experienced several notable cybersecurity incidents that have compromised major segments of its IT network. For example, in 2011 cyber intruders gained full access to 18 servers supporting key JPL missions and stole 87 gigabytes of data. More recently, in April 2018 JPL discovered an account belonging to an external user had been compromised and used to steal approximately 500 megabytes of data from 23 files, 2 of which contained International Traffic in Arms Regulations (ITAR) information related to the Mars Science Laboratory mission.[5]

We assessed the effectiveness of JPL's network security controls for externally facing applications and systems and examined elements of JPL's Cybersecurity Program and NASA's interaction with and oversight of the IT security control responsibilities assigned to Caltech under its contract to manage JPL. We found multiple IT security control weaknesses reduce JPL's ability to effectively prevent, detect, and mitigate attacks targeting its systems and networks and the NASA information on those systems and networks. In addition, multiple JPL incident management and response practices such as the staffing of its Security Operations Center and the maturity of its operating plans deviated from NASA and recommended industry practices. Furthermore, NASA's contract with Caltech does not provide the Agency with proper oversight of JPL's IT environment to ensure the protection and management of NASA data, applications, and systems. Taken together, these shortcomings expose Agency systems, data, and applications to exploitation by hackers and cyber criminals.

---

[4] U.S. Department of Homeland Security, *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0* (April 11, 2018). Available at https://www.cisa.gov/federal-information-security-modernization-act (accessed February 19, 2020).

[5] The U.S. Department of State administers ITAR, which restricts and controls the export of defense and military-related articles and services. The Mars Science Laboratory Curiosity Rover is a roving science laboratory operating on Mars since August 2012 designed to collect Martian soil and rock samples, analyze surface radiation, and make detailed measurements of element composition and organic compounds.

To improve JPL network security controls and NASA oversight, we made 10 recommendations to the Agency, including that it instruct the JPL Chief Information Officer to segregate shared network environments for all partners accessing the JPL network and monitor partner activity when accessing the network; review and update security agreements for all partners connected to the network gateway to ensure they are up-to-date; clarify the division of responsibility between the JPL Office of Chief Information Officer and system administrators for conducting routine log reviews and monitor their compliance with this requirement; and develop and implement a comprehensive strategy for institutional IT knowledge and incident management that includes the dissemination of lessons learned to system administrators and other appropriate personnel. We also recommended the NASA Chief Information Officer implement requirements in NASA's contract with Caltech for continuous monitoring tools that will provide the NASA Security Operations Center with oversight of JPL network security practices to ensure they adequately protect NASA data, systems, and applications. Although NASA management did not initially concur with all the recommendations, after further discussion they proposed appropriate corrective actions to address our concerns regarding all of the recommendations.

To view the full report, visit Cybersecurity Management and Oversight at the Jet Propulsion Laboratory.

Audit of NASA's Fiscal Year 2019 Financial Statements (IG-20-006, November 15, 2019)

The OIG contracted with the independent public accounting firm CliftonLarsonAllen LLP (CLA) to audit NASA's fiscal year 2019 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 4 years, CLA also reported a significant deficiency related to the Agency's IT security management.

CLA noted that NASA was able to remediate several prior year findings related to specific vulnerabilities and has incorporated a program aimed at reducing vulnerability totals and meeting vulnerability remediation timelines. Nevertheless, NASA did not sufficiently and consistently address the timely remediation of vulnerabilities associated with the financial application and general support systems. 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 use for an extended period of time. CLA stated that these weaknesses expose NASA to 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, Office of Management and Budget, and the National Institute of Standards and Technology.

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 work with the auditors to address and resolve outstanding issues in the coming year.

To read the full report, see the Financial Section of FY 2019 Agency Financial Report.

ONGOING AUDIT WORK

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019

In this annual review, we are evaluating NASA's IT security program against the 2019 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.

NASA's Policies and Practices Regarding the Use of Non-Agency IT Devices

Smartphones, tablets (mobile devices), and laptop computers are integral to NASA employees' and partners' work; however, the use of non-Agency devices to access NASA non-public networks and systems increases opportunities for attackers to breach sensitive Agency data stored on or accessed from these devices. This audit is assessing NASA's policies and practices regarding the use of non-NASA IT devices to conduct Agency business.

NASA's Management of Its Distributed Active Archive Centers

For more than 50 years, NASA has launched satellites and other scientific instruments into space to observe Earth and collect data on climate, weather, and natural phenomena such as earthquakes, droughts, floods, and wildfires. The data generated by these Earth science missions is stored at 12 Distributed Active Archive Centers (DAAC) that are located at NASA Centers, universities, and other federal agencies, and are responsible for processing, archiving, and distributing the data. This audit is assessing NASA's management of the DAACs and the Agency's initiative to transition the data to a cloud storage environment.

INVESTIGATIONS

Foreign Nationals Indicted for System Intrusion

Following a joint investigation by NASA OIG and Defense Criminal Investigative Service (DCIS), two Chinese nationals were indicted for gaining unauthorized access to a NASA computer system. Both were charged with one count of conspiracy to commit computer intrusions, one count of conspiracy to commit wire fraud, and one count of aggravated identity theft.

Employees Sent ITAR-Marked Documents to Personal Email Accounts

In two separate incidents, a civil servant and an intern sent unencrypted email containing ITAR data to their non-NASA, personal email address. In both cases, the employees deleted the sensitive information and management took appropriate corrective actions.

Export Controlled Information Found on Excessed Computers

During a joint investigation with the General Services Administration OIG into the alleged abuse of the federal Computers for Learning program, the suspects were found to be obtaining excess computer equipment for illegal resale and personal gain. NASA OIG's forensic examination of an external hard drive revealed numerous zip files, one of which contained NASA export-controlled documents. The suspect completed 6 months of probation and paid a $500 fine in accordance with his pretrial agreement related to violating NASA export control regulations.

NASA Computer Accounts Compromised

NASA OIG received information from the Federal Bureau of Investigation's Legal Attaché in Budapest, Hungary, via the NASA Counter Intelligence Division, that several NASA portal accounts had been compromised. We determined that all identified portals were public facing and instructed users to reset their passwords and delete any inactive accounts.

Jet Propulsion Laboratory Employee's Computer Found to Be Hacked

Following a DCIS request for assistance to recover email from a JPL employee's account, NASA OIG found evidence of a keystroke logger installed on the government computer that likely originated from China. The subjects in this case remain fugitives, likely in China, and evidence has been turned over to DCIS as the lead investigating agency for efforts relating to computer intrusions by Chinese nationals.

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: Jim Bridenstine
Administrator

Jim Morhard
Deputy Administrator

Stephen Jurczyk
Associate Administrator

Cathy Mangum
Acting Deputy Associate Administrator

Gabe Sherman
Chief of Staff

Renee Wynn
Chief Information Officer

Sumara M. Thompson-King
General Counsel

Mike Gold
Acting Associate Administrator for International and Interagency Relations

Bob 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