NASA OFFICE OF INSPECTOR GENERAL

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

January 28, 2015

The Honorable Richard C. Shelby
Chairman
Subcommittee on Commerce, Justice,
Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Barbara A. Mikulski
Ranking Member
Subcommittee on Commerce, Justice,
Science and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

Subject: *Review of NASA's Compliance with Federal Export Control Laws*

Dear Mr. Chairman and Senator Mikulski,

The National Aeronautics and Space Administration Authorization Act of 2000 directs the NASA Inspector General annually to assess NASA's compliance with Federal export control laws and reporting requirements regarding cooperative agreements between the Agency and China or any Chinese company.[1]

The NASA Office of Inspector General (OIG) last reported to you regarding these issues in January 2014. Since that date, NASA engaged in three bilateral science activities with the Chinese Academy of Sciences (Chinese Academy) relating to space geodesy, glacier research in the Himalaya Region,

[1] Public Law 106-391, codified at 51 U.S.C. § 30701(a)(3).

and lunar science.[2] The space geodesy project resumed activities outlined in a 1992 agreement with the Chinese Academy that NASA suspended in 2011. The other two activities involved exchanging publicly available NASA science information and NASA entered into no bilateral agreement concerning them. NASA made notifications of each activity in accordance with the congressional certification process established in Public Law 113-76.[3]

During the past year, the OIG completed a special review examining International Traffic in Arms Regulations (ITAR) and foreign national access issues at Ames Research Center (Ames) in California and conducted five audits examining NASA's controls for its information technology (IT) assets and security systems, many of which contain data subject to export control laws. In addition, during this period our Office of Investigations assisted with an investigation involving a Chinese national's efforts to obtain and export U.S. technology products, closed an investigation related to the security of NASA's export-controlled assets, and assisted the Federal Bureau of Investigation (FBI) with an investigation of computer intrusion, fraud, and money laundering. We summarize this work below.

SPECIAL REVIEW

Review of International Traffic in Arms Regulations and Foreign National Access Issues at Ames Research Center (February 26, 2014)

Beginning in 2009, Federal law enforcement agencies received complaints that foreign nationals working as contractors at Ames had been given improper access to information subject to ITAR, which control the transfer of military and space-related technology.[4] Under these regulations, foreign nationals are not permitted access to controlled information unless they receive a license from the U.S. Department of State.

These complaints led to a 4-year criminal investigation by the FBI, Department of Homeland Security, and NASA OIG. In February 2013, the U.S. Attorney for the Northern District of California closed the matter without bringing criminal charges. Following this decision, the OIG continued to investigate the allegations as an administrative matter.

In sum, we did not find intentional misconduct by any Ames civil servants but believe some Ames managers exercised poor judgment in their dealings with foreign nationals who worked on Center. For example, with respect to ITAR issues we found that several foreign nationals without the required licenses worked on projects that were later determined to involve ITAR-restricted information. In addition, on two occasions a senior Ames manager inappropriately shared documents with unlicensed foreign nationals that contained ITAR markings or had been identified

---

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

[3] The law requires NASA to certify to the Committees on Appropriations that the activities pose no risk of resulting 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 hardware and technical data subject to these rules are listed on the Department of State's U.S. Munitions List at 22 C.F.R. § 121.1 and the Department of Commerce's Commerce Control List at 15 C.F.R. § 774.1 et seq.

as containing ITAR-restricted information by NASA export control personnel. We concluded that these incidents resulted more from carelessness and disagreement over whether the information qualified for ITAR protection rather than an intentional effort to bypass ITAR restrictions.

We also found that a foreign national working at Ames inappropriately traveled overseas with a NASA-issued laptop containing ITAR-restricted information, although we were unable to substantiate concerns that the foreign national shared ITAR-protected information while overseas. In addition, a senior official at Ames knew about and failed to stop a foreign national from recording conversations with Ames coworkers without their knowledge or consent, a practice that violated NASA regulations and California law. Finally, we found that security rules designed to protect NASA property and data were not consistently followed in a rush to bring foreign nationals on board at Ames.

In the wake of the allegations examined in our report and a March 2013 incident at Langley Research Center, NASA has taken a series of actions to strengthen its foreign national access process. In addition, in January 2014 NASA received the results of a study it commissioned from the National Academy of Public Administration (NAPA) assessing the effectiveness of the Agency's foreign national access and export control processes.[5] We encouraged NASA to consider the information in the OIG investigations together with the NAPA review and previous OIG reports as it examines and adjusts its foreign national and export control programs.

To view a summary of the Ames report, visit http://oig.nasa.gov/Special-Review/Ames_ITAR.pdf. NASA's response can viewed at http://oig.nasa.gov/Special-Review/NASA_Response_AMES.pdf.

AUDIT REPORTS

Review of NASA's Agency Consolidated End-User Services Contract (IG-14-013, January 30, 2014)

In December 2010, NASA awarded the Agency Consolidated End-User Services (ACES) contract to HP Enterprise Services (HP) to provide desktop computers, laptops, mobile devices, printers, and other computing equipment as well as end-user services such as help desk and data backup to NASA employees and contractors. The ACES contract is a firm-fixed price, indefinite-delivery/indefinite-quantity contract with a maximum value of $2.5 billion. The 4-year contract runs from November 2011 through October 2015, after which NASA may extend the contract under two, 3-year options. With the ACES contract, NASA moved from a Center-based end-user services delivery model under which the individual Centers had greater control over products and services to a centrally managed, Agency-wide end-user model. By adopting this enterprise model for its most common IT services, NASA hoped to save money and enhance the security of Agency IT systems through leveraging economies of scale and standardizing institutional IT architecture.

Overall, we found NASA's lack of adequate preparation prior to deploying the ACES contract together with HP's failure to meet important contract objectives has resulted in the contract falling short of Agency expectations. Among the issues contributing to this finding was that NASA did not

[5] An executive summary is available at https://www.nasa.gov/sites/default/files/files/NAPA_Executive_Summary FNAM_Review_2014_Outlined-TAGGED-Final.pdf (accessed December 29, 2014).

have an accurate database to track the services and associated equipment ordered through the ACES contract. More specifically, a cumbersome, multi-step process to account for services and invoices resulted in unreliable inventory that was further complicated by outdated and incomplete inventory of legacy equipment purchased by HP. Because an organization needs to know what equipment is connected to its network for security purposes, this lack of an accurate and complete inventory poses a significant risk to NASA's IT security.

To view the full report, visit http://oig.nasa.gov/audits/reports/FY14/IG-14-013.pdf.

NASA's Management of its Smartphones, Tablets, and Other Mobile Devices (IG-14-015, February 27, 2014)

Mobile electronic devices, including smartphones and tablets, are key components of NASA's IT strategy to provide its employees and contractors flexibility in accessing Agency networks from anywhere at any time. Although mobile devices with computing capabilities offer greater workplace flexibility, they are also susceptible to security compromise. Mobile devices pose unique security threats because of their size, portability, constant wireless connection, physical sensors, and location services. Further, the diversity of available mobile devices, operating systems, carrier-provided services, and applications present additional security challenges.

Similar to our findings from the ACES contract review, we found NASA does not have a complete and accurate inventory of Agency-issued smartphones, tablets, cell phones, and AirCards that provide internet connectivity. This occurred because the information system NASA uses to order these devices from its IT contractor is not fully functional or integrated with the database NASA uses to track IT assets. Although NASA took actions to address information security risks associated with personal mobile devices connecting to NASA's e-mail systems, the Agency needed to implement a technical tool to mitigate risks when those devices connect to NASA networks other than Agency e-mail systems.

We made two recommendations, including that NASA implement a third-party tool or tools that would enable the Agency to centrally manage personally owned smartphones and tablets that connect to NASA networks. NASA's Chief Information Officer concurred with our recommendations and proposed appropriate corrective actions.

To view the full report, visit http://oig.nasa.gov/audits/reports/FY14/IG-14-015.pdf.

Security of NASA's Publicly Accessible Web Applications (IG-14-023, July 10, 2014)

NASA manages approximately 1,200 publicly accessible web applications – or about half of all publicly accessible non-military Federal Government websites – to share scientific information with the public, collaborate with research partners, and provide Agency civil servant and contractor employees with remote access to NASA networks. Hundreds of these web applications are part of IT systems NASA characterizes as high- or moderate-impact, meaning that a security breach could result in the loss of sensitive data (including export-controlled information) or seriously impair Agency operations. NASA's publicly accessible web applications consist mainly of websites, but also include web-based login portals and administrative systems that provide authorized personnel remote access to Agency IT resources.

NASA is a regular target of cyber attacks both because of the large size of Agency networks and because those networks contain technical and other sensitive information highly sought after by criminals. The frequency and sophistication of attacks directed at NASA's publicly accessible web applications has increased dramatically over the past several years. For example, between fiscal years 2012 and 2013, NASA experienced an 850 percent increase (from 42 to 359) in structured query language (SQL) injection attacks that attempted to compromise Agency web applications in order to steal data or gain a foothold into its networks for future exploitations.[6] Reducing the Agency's extensive web "footprint" is one of the more effective ways NASA can counter the threat of cyber attacks on its publicly accessible web applications.

We found that NASA's ongoing efforts to reduce its web presence and to identify and scan for vulnerabilities on its publicly accessible web applications have improved Agency IT security. However, NASA needs to close remaining security gaps, strengthen program oversight, and further reduce the number of publicly accessible web applications. Specifically, despite a reduction from about 1,500 to 1,200 publicly accessible web applications in a 15-month period, we found deficiencies in the design and implementation of NASA's Web Application Security Program (WASP) that leaves the Agency's publicly accessible web applications at risk of compromise. These deficiencies occurred because WASP did not prioritize identification of security vulnerabilities by seriousness of potential impact, identify the underlying cause of vulnerabilities, identify weaknesses associated with unsound IT security practices, or implement an effective process to ensure timely mitigation of identified vulnerabilities.

To improve the effectiveness of WASP, we made five recommendations to NASA's Chief Information Officer. The Chief Information Officer concurred with our recommendations and proposed appropriate corrective actions.

To view the full report, visit http://oig.nasa.gov/audits/reports/FY14/IG-14-023.pdf.

Audit of the Space Network's Physical and Information Technology Security Risks (IG-14-026, July 22, 2014)

During our audit of NASA's Space Network Project, we identified IT security, IT resource, and physical security issues associated with the Space Network and the White Sands Complex that required NASA management's attention. Specifically, we found that NASA has not ensured physical and IT security controls are in place on elements of its wide area network infrastructure, needs to clarify waiver requirements for IT security controls and mitigations, and should take additional steps to ensure that long-standing physical security risks are addressed. We also found that the Space Network is not using NASA's ACES contract to obtain administrative computers and associated end-user services and therefore may be spending more than necessary for equipment and services without realizing the operational and security benefits of systems provided through ACES.

To address these issues, we made four recommendations to which the Agency generally agreed and proposed appropriate corrective actions.

To view a summary of this report, visit http://oig.nasa.gov/audits/reports/FY14/IG-14-026.pdf.

[6] SQL is an industry standard computer language used to query, operate, and administer many databases, including Microsoft and Oracle databases. In a SQL injection attack, the attacker appends (injects) instructions onto the end of a valid SQL statement in an attempt to gain unauthorized access to the system and its data.

Federal Information Security Management Act: Fiscal Year 2014 Evaluation (IG-15-004, November 13, 2014)

This annual report, submitted as a memorandum from the Inspector General to the NASA Administrator, provides the OIG's independent assessment of NASA's IT security posture. For fiscal year 2014, the OIG adopted a risk-based approach under which we reviewed a sample of 24 Agency and contractor IT systems. We also relied on findings from our past and ongoing audit work.

Overall, we found that NASA has established a program to address the challenges in each of the 11 areas designated by the Office of Management and Budget for review: (1) continuous monitoring management, (2) configuration management, (3) identity and access management, (4) incident response and reporting, (5) risk management, (6) security training, (7) plan of action and milestones, (8) remote access management, (9) contingency planning, (10) contractor systems, and (11) security capital planning. However, consistent with last year's report, we also found that the Agency needs to enhance its efforts with regard to configuration management, risk management, and contractor systems.

To view a summary of this report, visit http://oig.nasa.gov/audits/reports/FY15/IG-15-004.pdf.

INVESTIGATIONS

Chinese National Sentenced to 15 Months for Scheme to Fraudulently Obtain Technology Products

In October 2014, a Federal judge in Maryland sentenced a Chinese national and naturalized U.S. citizen to 15 months in prison followed by 3 years of supervised release for false personation of a Federal employee and obstruction of justice in connection with a scheme to fraudulently obtain technology products from U.S. companies for export to China.

Zhenchun Huang worked as a contract scientist at NASA's Goddard Space Flight Center (Goddard) from February 1995 to June 2001. Thereafter, he consulted on a limited basis until October 2003 to provide assistance on a specific Goddard project. In April 2001, he established a company using his Maryland residence as the stated principle place of business to form joint ventures with Chinese governmental and private entities to research, develop, and distribute telecommunication and information technology products.

During the latter part of 2003 and into early 2004, Huang falsely represented to three U.S. companies that he was employed by NASA and was working on a joint project with the Agency in an effort to obtain technological components for use by his company, whose actual base of operations was located in China. To make it look like NASA was purchasing these components, Huang directed that purchased items be shipped to an associate employed at Goddard, used a Goddard e-mail account to communicate with the companies before redirecting the e-mails to his personal account, faxed (or had faxed) a purchase order from a number associated with Goddard, and presented his former business card that identified him as a NASA contract employee.

The components Huang was attempting to obtain and export could have been used to fabricate an infrared detector suitable for military applications, such as night vision and missile detection, that would have been controlled for export to China. He also purchased and in May 2006 attempted to travel to China with export-controlled ultraviolet light emitting diodes that could have been used in a non-line-of-sight communications system. U.S. Immigration and Customs Enforcement officials at O'Hare International Airport in Chicago inspected his luggage and found the diodes prior to his outbound flight. After making false statements in regard to the diodes, he instructed his wife to destroy files related to his company and later fled the country until his arrest in London in December 2013.

This investigation was conducted by the FBI, U.S. Immigration and Customs Enforcement's Homeland Security Investigations, and U.S. Department of Commerce's Bureau of Industry and Security Office of Export Enforcement. NASA OIG assisted in subsequent debarment actions regarding Huang and his company.

Chinese Researchers Accessed Restricted Areas of a University Research Center Supporting NASA

In April 2014, the OIG closed an investigation and issued a memorandum to NASA management regarding two Chinese nationals that improperly obtained access to a restricted NASA laboratory that housed export-restricted materials and data. The laboratory, located in the National Space Science Technology Center at the University of Alabama in Huntsville, contains an export-restricted gamma ray detection device. Both Chinese nationals were employed by the University but neither was authorized access to the laboratory. In response to the OIG investigation and recommendations, the University and NASA management instituted additional controls to ensure compliance with all relevant export control regulations and terminated the Chinese nationals' employment.

Estonian Extradited to New York City for Fraud Scheme Infecting 4 Million Computers with Malware

In October 2014, an Estonian national was arraigned in U.S. District Court for the Southern District of New York on multiple counts of criminal conspiracy, computer intrusion, fraud, and money laundering. The charges relate to the operation of a sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries. The malware secretly altered the settings on infected computers, enabling the accused and six other defendants to digitally hijack Internet searches and reroute computers to certain websites and advertisements. As a result, the defendants and their coconspirators illicitly collected at least $14 million through "click hijacking" and advertisement replacement fraud, and then laundered these proceeds through numerous companies. The OIG is working this case jointly with the FBI.

If you or your staff would like to meet to discuss any of the reports or investigations discussed in this letter, please contact me or Renee Juhans, OIG Executive Officer, at 202-358-1220.

Sincerely,

Paul K. Martin
Inspector General

cc: Charles F. Bolden, Jr.
NASA Administrator

Robert Lightfoot
Associate Administrator

Michael French
Chief of Staff

Larry Sweet
Chief Information Officer

Michael F. O'Brien
Associate Administrator, International and Interagency Relations

Richard Keegan
Associate Administrator, Mission Support Directorate

Sumara Thompson-King
General Counsel

Enclosure – 1

ENCLOSURE I: CONGRESSIONAL RECIPIENTS

United States Senate

The Honorable John Thune
The Honorable Bill Nelson
The Honorable Ted Cruz
The Honorable Ron Johnson
The Honorable Thomas R. Carper

U.S. House of Representatives

The Honorable John Culberson
The Honorable Chaka Fattah
The Honorable Jason Chaffetz
The Honorable Elijah Cummings
The Honorable Mark Meadows
The Honorable Gerry Connolly
The Honorable Lamar Smith
The Honorable Eddie Bernice Johnson