Testimony before the Subcommittee on Space
Committee on Science, Space, and Technology

United States House of Representatives

For Release on Delivery
expected at 10:00 a.m.
on June 20, 2014

NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information

Statement of
Gail A. Robinson
Deputy Inspector General
National Aeronautics and Space Administration

Mr. Chairmen, Ranking Members, and Members of the Subcommittees on Space and Oversight:

The Office of Inspector General (OIG) is committed to providing independent, aggressive, and objective oversight of NASA programs and personnel, and we thank you for inviting us to discuss our work relating to the Agency's management of foreign national access to its information and Centers, compliance with export control laws, and related security issues.

In January of each year, the OIG submits to the House of Representatives and Senate Appropriations Committees a letter describing the audits and investigations we conducted the preceding year that shed light on the extent to which NASA is complying with Federal export control laws.

In our most recent letter we summarized

- four audits examining security controls for NASA's information technology (IT) assets, many of which contain data subject to export control laws; and
- a special review examining a Chinese national's access to the Langley Research Center (Langley) in Hampton, Virginia.

Before highlighting two of the audits and describing the Langley investigation and another special review involving foreign nationals and export issues at the Ames Research Center (Ames) in Mountain View, California, I will highlight several themes from our oversight work that echo findings made by the Government Accountability Office (GAO) and the National Academy of Public Administration (NAPA) in their recent examinations of export control practices and management of foreign national access at NASA.[1]

First, our audit and investigative work lead us to conclude that NASA needs to take a more standardized and systematic approach to both foreign national access and export control management. In the Langley matter, we were struck by the highly bureaucratic nature of NASA's process for reviewing foreign visit requests. For example, we noted that the many individuals involved in the process appeared to view their roles in isolation, with little consideration or understanding of the role played by others. Similarly, in the Ames review, we encountered a lack of early coordination between project and export control personnel, as well as deep disagreement between these two groups regarding whether work performed by foreign nationals involved technology subject to the International Traffic in Arms Regulations (ITAR) that control the transfer of military and space-related technology. Indeed, the issue only surfaced when the Ames scientists sought to publish a paper many months after work on the project had begun. In addition, it appeared that NASA lacked an efficient mechanism to resolve the dispute between the two groups, which dragged on for months. We believe that NASA needs to work toward a model that

[1] GAO, "Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the risk of Unauthorized Access to its Technologies" (GAO-14-315, April 2014); and NAPA, "An Independent Review of Foreign National Access Management" (January 2014).

encourages Agency scientists and engineers to consult with export professionals when projects involving foreign nationals are initiated and develop a mechanism for resolving disputes in a timely manner.

Second, we believe export control professionals at the various NASA Centers could improve their understanding of the type and location of export-controlled technology and information at their Centers and other facilities under their Center's control. For example, over the course of a recent investigation, we learned that a Center Export Control Administrator was not aware that an off-site lab under his responsibility contained export-controlled equipment and data. Center export control personnel need this type of information to ensure that foreign nationals do not have access to these areas.

Third, we encourage NASA to study the best practices noted in the GAO and NAPA reports and adopt them at all its field Centers. As we have learned through our oversight work in other areas, NASA Centers often work independently from one another and do not consistently learn about or benefit from successful practices developed at other locations. We are particularly intrigued by discussion in the GAO report about the Jet Propulsion Laboratory's (JPL) success with using engineers and scientists as export control representatives to work with the JPL's export control staff – a model that could help address the lack of early interaction between project managers and export control staff we observed at Ames as well as provide a mechanism for dispute resolution.

Finally, we agree that NASA needs to improve and expand training to provide its scientists and engineers with a deeper understanding of the importance of complying with rules and regulations governing export control and foreign national access.

As noted above, NASA stores export-controlled information in various Agency databases. We have repeatedly reported that ensuring the security of its information and IT systems remains one of NASA's top management challenges. On the one hand, the Agency's mission to widely disseminate and publicly share its information helps push the boundaries of science and space exploration; however, at the same time, the Agency must ensure the security of its IT assets and comply with an array of complex export control laws and regulations. Below, I summarize several of our recent audit and investigative work products that involve IT security, foreign national access, and export control issues.

In a June 2013 audit report, we examined whether NASA's IT governance structure – its process for designing, procuring, and protecting IT resources – appropriately aligns authority and responsibility to support the Agency's overall mission.[2] We found that the decentralized nature of NASA's operations and the Agency's longstanding culture of autonomy hinder its ability to implement effective IT governance. NASA's Chief Information Officer (CIO) has limited visibility and control over a majority of the Agency's IT investments, operates in an organizational structure that marginalizes the authority of the position, and cannot enforce security measures

[2] NASA OIG, "NASA's Information Technology Governance" (IG-13-015, June 5, 2013).

across NASA's computer networks. Specifically, although the CIO is responsible for developing IT security policies and implementing an Agency-wide IT security program, the position lacks authority and control over the majority of NASA's networks and therefore the CIO is unable to enforce implementation of IT security programs across all Agency IT assets.

We made eight recommendations to the CIO to overcome the barriers that have resulted in inefficient and ineffective management of the Agency's IT assets and security. Effective implementation of these recommendations will require a cultural shift and significant changes to the Agency's IT management decision-making regime, including the realignment of authority and responsibilities. To date, NASA is taking appropriate steps to meet our recommendations.

In a separate audit, we examined NASA's procedures related to its acquisition of IT security assessment and monitoring tools.[3] NASA spends more than $1.5 billion annually on its IT assets, including approximately 550 information systems the Agency uses to control spacecraft, collect and process scientific data, provide security for Agency IT infrastructure, and enable personnel to collaborate with colleagues around the world. However, the Agency's use of advanced technology, coupled with the large size of its internet-accessible networks, makes NASA an attractive target to cyber attacks. To thwart such attacks, NASA must ensure that Agency IT systems are regularly safeguarded, assessed, and monitored.

We found that the Agency has not fully implemented a process for identifying its IT security assets despite spending at least $58 million annually on IT security, a portion of which is used to acquire and manage security assessment and monitoring tools. Because NASA does not have a process that captures, consolidates, and assesses IT security tool requirements across the Agency, centralized purchases of such tools do not regularly occur. This inability limits NASA's efforts to reduce cost and improve program efficiencies on critical IT investments. To improve NASA's process for acquiring Agency-wide IT security assessment and monitoring tools, we made four recommendations to which Agency management concurred and proposed appropriate corrective actions.

In addition to our audit work, we also dedicate significant resources to investigating IT and other security-related issues. Of the 263 active cases currently being handled by our Office of Investigations, 56 involve cyber intrusions and misuse of NASA IT equipment and 15 involve allegations of export control violations. In one recently concluded investigation, we found that insufficient security practices at a facility located on the campus of one of NASA's university partners allowed unauthorized foreign nationals to enter a laboratory containing export-controlled equipment and data. Although the foreign nationals denied copying any data from the lab and a later search of their electronic media failed to uncover any controlled information, we were unable to definitively exclude that possibility. In addition, two of our most high-profile investigations

[3] NASA OIG, "NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools" (IG-13-006, March 18, 2013).

during the past year examined foreign national access and export control issues. I summarize each of these investigations below.

Chinese National's Access to Langley

In March 2013, Bo Jiang, a Chinese national working as a NASA contractor at Langley, was returning to China when Department of Homeland Security (DHS) agents searched him at Dulles International Airport as part of an investigation of potential export control violations. After questioning him about the electronic media in his possession, agents took Jiang into custody and charged him with making a false statement to Federal authorities because a search of his belongings revealed media he had not declared. After more than 6 weeks in detention, Jiang pleaded guilty to a misdemeanor security offense and left the country. Subsequent to the plea, the OIG opened an administrative investigation to examine the process by which Jiang came to work at Langley and the information and IT resources to which he had access.

Jiang originally came to the United States in 2007 as a Ph.D. student at Old Dominion University and began working at Langley in January 2011 under a contract with the National Institute of Aerospace. In November 2011 and again in November 2012, Jiang visited family in China and took with him a NASA-provided laptop computer. During the second visit, Langley export control officials raised concerns about Jiang's travel and access to NASA information.

We found that even though Langley's process for requesting access for foreign nationals was structured pursuant to NASA regulations, it was overly complex and not sufficiently integrated to ensure that responsible personnel had access to all relevant information. In addition, we determined that several employees who had roles in the screening process made errors that contributed to the confusion about the proper scope of Jiang's access to Langley facilities and IT resources. We made six recommendations to improve NASA's foreign visitor approval process, and NASA concurred with each.[4]

In the wake of the Jiang incident, Langley management has taken steps to strengthen its foreign national access process, including increased education and training for Langley employees, revising the form used to request access for foreign nationals, and ensuring the Center CIO's office is involved in the foreign visitor request process.

Ames ITAR investigation

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. These complaints led to a 4-year criminal investigation by the Federal Bureau of Investigation, Department of Homeland Security, and OIG. In February 2013, the U.S. Attorney for the Northern District of California closed the case without bringing criminal charges, and the OIG continued to

[4] NASA OIG, "Bo Jiang's Access to NASA's Langley Research Center" (October 22, 2013).

investigate the allegations as an administrative matter. In February 2014, we provided a 41-page report outlining our investigation and findings to the NASA Administrator. While the full report could not be released publicly because it contains information protected by the Privacy Act of 1974, we provided copies to several Congressional committees and posted a public summary on our website.[5]

Although we did not find intentional misconduct by any Ames civil servants, we believe several Ames managers exercised poor judgment in their dealings with foreign nationals. 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 as containing ITAR-restricted information by NASA export control personnel. However, we also found significant disagreement between scientists and engineers at Ames and export control personnel at the Center and NASA Headquarters as to whether the work performed by foreign nationals involved ITAR-controlled technology. Moreover, the foreign nationals subsequently applied for and received licenses permitting them to access the information. We concluded that these incidents resulted more from carelessness and a genuine disagreement about whether the information qualified for ITAR protection 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. Even though the foreign national had an ITAR license at the time, the regulations forbid taking export-controlled information out of the country. However, we were unable to substantiate concerns that the foreign national shared controlled information while overseas. Further, 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. For example, contrary to NASA rules a foreign national improperly received unescorted access privileges to Ames in 2006 prior to the completion of required background checks and worked at the Center for nearly 3 years without a required security plan.

Finally, we uncovered no evidence to support allegations that any foreign nationals at Ames were provided classified information during the period covered by our review. We encouraged NASA to consider the findings in our Ames report together with the NAPA review and previous OIG reports as it refines its foreign national and export control programs.

In closing, we are encouraged that NASA has embraced the recommendations made by our office, GAO, and NAPA and is taking action to improve Agency IT security and its management of export control and foreign national access. We will continue to provide aggressive oversight as NASA implements its Foreign National Access Management Program and works to improve its export control and IT security practices.

[5] NASA OIG, "Review of ITAR and Foreign National Access at Ames Research Center" (February 26, 2014).