U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Space
Subcommittee on Oversight

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

CHARTER

Friday, June 20, 2014
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

The Subcommittees on Space and Oversight will hold a joint hearing, *NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information*, at 10:00 a.m. on Friday, June 20, 2014. The Government Accountability Office (GAO), the National Academy of Public Administration (NAPA), and the NASA Office of Inspector General (OIG) have all released reports within the past several months addressing how NASA manages access of NASA facilities and sensitive information to foreign nationals. This hearing will review these practices and procedures, as well as recommendations for improvement identified in these reports.

Witnesses

- **Mr. Richard Keegan**, Associate Deputy Administrator, National Aeronautics and Space Administration;
- **Ms. Belva Martin,** Director, Acquisition and Sourcing Management, Government Accountability Office;
- **Ms. Gail A. Robinson,** Deputy Inspector General, National Aeronautics and Space Administration;
- **Mr. Douglas Webster,** Fellow, National Academy of Public Administration and Principal, Cambio Consulting Group.

Background

The National Aeronautics and Space Act of 1957 directs that NASA "provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."[1] Conversely, the Act also directs NASA to protect classified, trade secret, and confidential information.[2] Additionally, NASA—like other federal agencies—is subject to the requirements of the Arms Export Control Act and the Export Administration Act.[3]

[1] 51 U.S.C. §20112(a)(3)
[2] 51 U.S.C. §20131 and 20132
[3] 22 U.S.C. §2751-2799aa-2 and 50 U.S.C. app. §2401-2420

Two high-profile events highlighted this tension:

- On March 16, 2013, agents from the Department of Homeland Security conducted a search of a former NASA contractor as part of an investigation of potential export control violations. Six weeks later, the individual pleaded guilty in Federal court to a misdemeanor offense of violating Agency security rules. On August 22, 2013, NASA's Office of Inspector General (OIG) issued a report of investigation titled "Bo Jiang's Access to NASA's Langley Research Center." This report was released to the public (with redactions) on October 22, 2013.[4]
- In a separate case, Federal law enforcement agencies received complaints dating back to 2009 that foreign nationals working as contractors at NASA's Ames Research Center were given improper access to facilities and sensitive information. These complaints led to a 4-year criminal investigation by the Federal Bureau of Investigation, the Department of Homeland Security, and the NASA Office of Inspector General, culminating in the forwarding of the case for prosecution to the U.S. Attorney for the Northern District of California. The criminal matter was not pursued; however the NASA IG continued the investigation as an administrative matter. On February 12, 2014, NASA's OIG issued a report titled "Review of International Traffic in Arms Regulations and Foreign National Access Issues at Ames Research Center." A brief summary of this report was released to the public on February 26, 2014.[5]

The issues highlighted in these reports were also corroborated by two separate, independent reviews:

- In January 2014, the National Academy of Public Administration issued a report titled "An Independent Review of Foreign National Access Management," which was requested by Rep. Frank Wolf. NASA has publicly released the executive summary of this report.[6]
- Last month, the Government Accountability Office released a report titled "Export Controls: NASA Management Action and improved Oversight Needed to Reduce the Risk of Unauthorized Access to its Technologies."[7] This report was requested by Oversight Subcommittee Chairman Paul Broun on October 25, 2012.[8]

[4] Accessed at http://oig.nasa.gov/Special-Review/OIG_Investigative_Summary.pdf
[5] Accessed at http://oig.nasa.gov/Special-Review/Ames_ITAR.pdf
[6] Accessed at http://www.nasa.gov/sites/default/files/files/NAPA_Executive_Summary_FNAM_Review_2014_Outlined-TAGGED-Final.pdf
[7] Accessed at http://www.gao.gov/products/GAO-14-315
[8] Accessed at http://science.house.gov/letter/broun-letter-gao-comptroller-general-dodaro-nasa-export-controls

Findings

The NASA OIG issued the following noteworthy findings in their two reports:[9]

- "We found that Langley's process for requesting access for foreign nationals was structured pursuant to NASA regulations. However, we also found the process overly complex, required input from numerous Centers and headquarters employees, and not sufficiently integrated to ensure that responsible personnel had access to all relevant information."
- "…we determined that several employees who have 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 and the appropriateness of Jiang taking his NASA-provided laptop to China."
- "…we were struck by the highly bureaucratic nature of Langley's process for reviewing foreign visit requests. Each of the many actors in the process appeared to view their role in isolation, with little consideration or understanding of the role others played in the process. In many instances, individuals seemed more focused on moving requests into the next person's in-box than ensuring that their actions made sense in the context of the request they have been asked to review."
- "In some instances, employees seemed to realize that they did not fully understand what they were doing or why they were doing it but proceeded anyway, assuming that someone else down the road would figure it out."
- "…NIA appeared to lack sufficient procedures to ensure that appropriate officials in its organization were informed of the restrictions NASA placed on Jiang's access to the Center [LaRC]."
- "From an individual perspective, the preponderance of evidence available to us suggests that one of Jiang's sponsors inappropriately authorized Jiang to take the laptop to China."
- "…we believe Jiang's sponsor erred in not consulting Center export personnel before providing Jiang access to Rahman's [NASA employee] hard drive or informing export officials they had done so in a timely manner."
- "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."
- "…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."
- "We also found that a foreign national working at Ames inappropriately traveled overseas with a NASA-issued laptop containing ITAR-restricted information."
- "…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."
- "…we found that security rules designed to protect NASA property and data were not consistently followed in a rush to bring two foreign nationals on board at Ames. For example, contrary to NASA rules a foreign national improperly received unescorted

[9] See *Supra* 4 and 5

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."
- "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."

The GAO made the following findings of note in their report last month:[10]

- "Weaknesses in implementation of NASA export control, foreign national access, and scientific and technical information procedures at some Centers creates export control vulnerabilities."
- "Management decisions on Center Export Administrator authority, organizational placement, and resources affect export control implementation at Centers."
- "We identified instances where NASA security procedures for foreign national access were not followed, which **were significant given the potential impact on national security** or foreign policy from unauthorized access to NASA technologies" [emphasis added].
- "…at one center, export control officials' statements and our review of documentation showed that, in seven instances between March and July of 2013, foreign nationals fulfilled the role of sponsors – typically NASA project managers or other NASA officials who establish and endorse the need for a relationship between the foreign national and NASA and request their access to NASA facilities and information technology systems – by identifying the access rights to NASA technology for themselves and other foreign nationals for one NASA program."
- "CEAs [Center Export Administrators] and Security officials from three centers cited instances where sponsors, escorts and personnel working at the facility being visited by foreign nationals are not aware of their roles and responsibilities of the provisos that detailed the level of physical and virtual access for the foreign national visitor."
- "Based on our review of NASA's most recent STI [Scientific and Technical Information] compliance audits, most centers continue to release STI that has not been reviewed for export control purposes."
- "We did not assess STI documents that were not reviewed or information that was posted on NASA websites without export control review to determine if their release violated export controls, but without the completion of these reviews, **NASA is at increased risk of inadvertently releasing controlled technologies.**" [emphasis added]
- "NASA lacks a comprehensive inventory of export-controlled technologies and NASA Headquarters is not fully utilizing oversight tools"
- "…it is important to have clear export control policies that have strong management support and effective oversight to ensure consistent adherence across NASA Centers. **NASA's program is lacking in both areas.**" [emphasis added]
- "When dealing with export controlled information, every instance of unapproved foreign national access or unapproved release of scientific information increases the risk of harm to national security."

[10] See *Supra* 7

The NAPA review issued the following notable findings:[11]

- "The Academy found that there is little accountability for non-compliance when identified through specific incidents or periodic assessments. This validates the identified perception among NASA personnel that 'mandatory compliance' means little, as there are few, if any, consequences for deliberate or inadvertent violations of the mandates."
- "Due to the fact that the NASA systems lack the necessary controls to protect information, allow foreign nationals access to the networks, and allow remote access, **the Panel concludes that the NASA networks are compromised.** Publicly available reports on systemic data breaches across the country, NASA's own internal reports, and briefings given to Academy staff leave little doubt that information contained on the NASA IT systems is compromised." [emphasis added]
- "NASA Headquarters (HQ) Officials and Center Directors have not adequately communicated that strict compliance was and is required for foreign national hosting, sponsoring, and escort policy and procedures."
- "Directives, and orders, can be seen more as 'guidance' as opposed to mandatory policy and procedural requirements that must be adhered to. This can lead to communications breakdowns and negative outcomes."
- "After fixing a problem, the Agency has a tendency to lapse back into old habits once the spotlight is off the area under review;"
- "A number of NASA leaders also noted that **the Agency tends not to hold individuals accountable even when they make serious, preventable errors.** Whenever an example of such an error was mentioned during the interviews, Academy staff would follow-up with: *what happened to those responsible for the error?* In almost every instance, the answer was either 'nothing' or 'I don't know'" [emphasis added]
- "Others [NASA centers] take a more *laissez-faire* approach with training either being optional or, if mandatory, provides no sanctions against those who fail to take the training"
- "In summary, the Panel found export control training requirements are inconsistent; the training is confusing and inadequate; and the rationale for such training is often poorly understood.
- "The Export Control program needs a more standardized and systematic approach in furtherance of its export compliance objectives, as well as better audit and review mechanisms. NASA senior leaders also need to more strongly endorse the critical importance of such controls."
- "Specific intelligence regarding threats posed by foreign nationals and insiders to specific NASA assets is available from IC agencies, but has been inconsistently utilized to educate NASA personnel."
- "NASA facilities, personnel, technologies, and information are highly regarded and of great interest to the world. That interest extends to some countries, governments, organizations, and individuals whose intent is to compromise those facilities, co-opt the personnel, and steal those technologies and information."

[11] See *Supra* 6

Recommendations

The NASA OIG made six recommendations to improve NASA's foreign visitor approval process[12]:

1. "Examine the roles of the different offices that have input into the foreign visitor approval process and ensure that all appropriate offices are represented and that responsibilities are appropriately assigned.
2. Improve training for sponsors of foreign nationals to ensure they understand how the foreign national visit approval process works and their responsibilities as sponsors. This training should be required prior to an individual becoming a sponsor and be repeated at least annually as long as they continue to serve in this capacity.
3. Revise the Security Technology Transfer Control Plan (STTCP) to include NASA policy regarding taking information technology (IT) equipment out of the United States and ensure that employees are trained regarding this policy.
4. Consider the following improvements to IdMax [electronic database used to process foreign national access]:
    a. Require individuals who will be acting as sponsors to acknowledge receipt of the plan and their understanding of all conditions placed on the visits of foreign nationals they are sponsoring; and
    b. Prevent the system from generating final approval until all key documents, including the STTCP, are loaded into the system.
5. Ensure that the National Institute of Aerospace (NIA) and other similar organizations have a process in place so that appropriate organizational officials are aware of the many conditions NASA places on foreign nationals associated with their organizations who are working with NASA.
6. Consider whether discipline and/or performance-based counseling are appropriate for any of the NASA civil servants discussed in this report [related to Bo Jiang's access]."

The GAO issued the following recommendations:[13]

To ensure consistent implementation of NASA's export control program, GAO recommended that NASA:

1. "Establish guidance of defining the appropriate level and organizational placement of the CEA function.
2. Assess CEA workload and other factors to determine appropriate resources needed to support the CEA function at each Center."

GAO made five additional recommendations to improve NASA's oversight and address identified deficiencies in the export control program:

[12] See *Supra* 4

[13] See *Supra* 7

1. "Implement a risk-based approach to the export control program by using existing information sources, such as counterintelligence assessments, to identify targeted technologies that are identified and managed by CEAs within each Center.
2. Direct Center Directors to oversee implementation of export-related audit findings which could involve collaboration among several Center offices.
3. Develop a plan, including timeframes for addressing CEA issues and suggestions for improvement provided during the annual export control conference, and share the plan with CEAs.
4. Re-emphasize to CEAs the requirements on how and when to notify the Headquarters Export Administrator about potential voluntary disclosures to ensure more consistent reporting of potential export control violations at NASA Centers.
5. Develop plans with specific time frames to monitor correction actions related to management of foreign national access to NASA facilities and assess their effectiveness."

NAPA made a total of 27 recommendations in their full report, which are summarized by the following topics:[14]

1. **"Manage FNAM as a Program.** The Panel proposed a number of steps for NASA to take which would begin to coordinate efforts and secure better results including realignment of both field and Headquarters organizational elements, strengthening the oversight capabilities of headquarters, and, improving training by developing comprehensive, integrated curriculums and lesson plans.
2. **Reduce the flexibility given to Centers to interpret FNAM requirements.** The Panel recommended that NASA Headquarters write a comprehensive and detailed FNAM operating manual covering all functional aspects of the program. Currently, FNAM directives can be found in several different publications, each with their own Headquarters and field constituencies. Headquarters staff should work in consultation with knowledgeable field staff to create this manual.
3. **Determine critical assets and build mechanisms to protect them.** The Panel envisions the creation of an Asset Protection Oversight Board which would use the results of the Independent Review Teams assessments of individual program compliance metrics as well as overall performance and outcomes of FNAM and the adequacy of the comprehensive threat/risk assessment at each Center.
4. **Correct longstanding information technology security issues.** The Panel believes NASA needs to identify and protect sensitive, proprietary information in a manner that does not prevent system owners from meeting their mission needs. Among the specific recommendations in this area are for NASA to establish clear, specific, and mandatory requirements for all Centers to follow regarding remote access of their information technology systems and that the NASA Chief Information Officer be given more control over IT operations in field Centers.
5. **Work to change several aspects of NASA culture.** Included in this are the recommendations to reduce unnecessary competition between field centers, ensure that accountability for conforming to FNAM requirements is established, and finally, to guard against the organizational tendency to revert back to prior lax habits once a problem area has been addressed.

[14] See *Supra* 6

6. **Communicate the importance of these FNAM changes clearly, firmly and consistently.** The importance of security, the existence of "real world" threats to NASA assets, and the need for improvements in handling foreign national issues have not been clearly and consistently communicated throughout NASA. Senior leaders must firmly establish and communicate their total commitment to an effective Foreign National Access Management program that enhances cooperation while safeguarding information."