

OPENING STATEMENT

Ranking Member Donna Edwards (D-MD)
Subcommittee on Space
Committee on Science, Space, and Technology

Joint Subcommittee Hearing
“NASA Security: Assessing the Agency’s Efforts to Protect Sensitive Information”

June 20, 2014

Good Morning, and welcome to our panel of witnesses. Mr. Chairman, thank you for calling this hearing on assessing NASA’s efforts to protect sensitive information.

The legislation establishing the National Aeronautics and Space Administration, the Space Act of 1958, recognizes the importance of NASA’s cooperation with other nations and groups of nations and directs NASA to *“provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof”*.

As a civil R&D agency that supports scientific research, NASA has a culture of openness, collaboration, and sharing of results. Last year, for instance, NASA approved more than 11,000 foreign national visits to its facilities and Centers and currently maintains an estimated 600 international agreements with more than 100 foreign countries, envisioning projects which may require an exchange of information to be successful.

However, the benefits of that culture of openness and sharing must be balanced with appropriate security limits and protections. Indeed, the Space Act also directs the NASA Administrator to *“establish such security requirements, restrictions, and safeguards as the Administrator deems necessary in the interest of the national security”*.

Mr. Chairman, I have often said that NASA is recognized across the world as a symbol of the United States’ greatness as a nation and its leadership in science and technology. Thus, it is no surprise that so many developed and emerging nations seek to follow suit in pursuing space exploration.

Nor should it be a surprise that some may seek to obtain NASA’s treasure trove of knowledge by all means possible in order to leapfrog the decades of research and billions of dollars of investment that the U.S. has made in acquiring its hard-earned capabilities.

That is why I appreciate the work completed by NASA's Office of the Inspector General, Government Accountability Office, and the National Academy of Public Administration, and their recommendations on how NASA can better protect controlled information, including export-controlled information, from unauthorized access—such as by foreign nationals.

The findings from the NASA OIG, GAO, and NAPA reports have areas of commonality. For example:

- GAO and NAPA raised concerns about the inconsistency in Center implementation of export controls, with NAPA urging NASA to take steps to reduce the decentralized authority given to Centers in implementing enterprise-wide processes. .
- The NASA OIG and NAPA found the Foreign National Access process to be overly complex and not sufficiently integrated to ensure that responsible security personnel have access to relevant information.
- Finally, GAO and NAPA both found that NASA lacks a comprehensive inventory of the types and locations of export-controlled technologies.

Corrective actions will likely be difficult for the agency to implement. We will need to be vigilant to ensure that these corrective actions do not destroy NASA's culture of openness which has proven to be a key ingredient in the agency's success.

Mr. Chairman, we have worked too hard and invested too many precious taxpayer dollars to let sensitive knowledge slip away as a result of inconsistent implementation of export controls, and so I am encouraged by the NASA Administrator's receptiveness to the recommendations made.

However, I also recognize that a sustained commitment on the part of all NASA employees and contractors will be needed for corrective actions to take hold.

I look forward to hearing from our distinguished panel, and in particular from NASA's witness, Mr. Keegan, on how NASA will address that challenge.

I yield back.