OPENING STATEMENT

Ranking Member Dan Maffei (D-NY)
Subcommittee on Oversight
Committee on Science, Space, and Technology

Joint Subcommittee Hearing
"NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information"

June 20, 2014

Thank you Chairman Palazzo and Chairman Broun for holding this hearing today.

Ensuring that America's sensitive technical designs and security related research is not intentionally pilfered or inappropriately exported is important to this nation's economic and national security. Each year the U.S. loses billions of dollars' worth of advanced technologies, innovative scientific research, and other sensitive data due to economic espionage and data theft. This impacts U.S. businesses as well as U.S. government laboratories and research centers. NASA is no exception. The National Aeronautics and Space Administration (NASA), like other federal agencies, is a prime target of foreign agents and global cyber criminals.

The agency has a lot to offer. NASA leads the world in space exploration, aeronautics research, and other key scientific areas. Controlling the inadvertent release of sensitive information or intentional theft of export controlled technologies has always been a difficult task. This is particularly true when that sort of data resides in an environment that depends upon international collaborations and access to foreign scientists and facilities. Over its history NASA has had more than 3,000 international cooperative agreements and currently maintains an estimated 600 international agreements with more than 100 foreign countries. Last year NASA approved more than 11,000 foreign national visits to its facilities. At a time of constrained federal budgets and reductions in investments in science and technology, NASA is dependent upon these global interactions to ensure its continued success.

Unfortunately, NASA has suffered from several security incidents in recent years that sparked reviews of its security policies and practices. These reviews by the Government Accountability Office (GAO), NASA's Office of Inspector General and the National Academy of Public Administration (NAPA) have all identified poor practices in protecting sensitive NASA technologies, organizational issues that may undermine NASA's security protocols, and financial constraints that may contribute to the inadvertent release of export restricted data. NASA was fortunate, however, that the incidents themselves do not appear to have resulted in major losses of sensitive data.

In one of the most high profile cases involving Chinese national Bo Jiang, who was accused of attempting to take a NASA laptop to China without proper authorization while working at NASA's Langley Research Center in Virginia, federal prosecutors found that, "none of the computer media that Jiang attempted to bring to [China] on March 16, 2013, contained classified

information, export-controlled information, or NASA proprietary information." In a separate incident involving two foreign nationals working at NASA's Ames Research Center in California a NASA Inspector General report released in February, "uncovered no evidence to support allegations that any foreign nationals at Ames were provided classified information during the period covered by our review."

NASA was lucky it did not sustain a serious loss of critical data or technology, but the space agency has unique national assets, innovative technologies, and valuable scientific data that must be properly protected from global economic competitors, foreign adversaries, or individual theft by those seeking to cash in on the agency's valuable research and innovative discoveries.

Being able to detect and deter these security threats while at the same time supporting important international scientific collaborations is a delicate and often difficult balance to achieve. I look forward to our witnesses helping us to better understand these issues, evaluating these often conflicting objectives, and recommending ways to maintain an appropriate balance.