OPENING STATEMENT
The Honorable Paul Broun (R-GA), Chairman
Subcommittee on Investigations & Oversight
Committee on Science, Space, and Technology
NASA Cybersecurity: An Examination of the Agency's Information Security

February 29, 2012

The topic of cybersecurity is certainly hot these days. As Washington debates the government's appropriate role in private-sector cybersecurity activities, we should remember that the government is already responsible for securing its own networks and information – a task that it has executed with mixed success.

While the defense and intelligence communities take great steps to protect data and operations from theft and corruption, often times civil agencies are not as vigilant. In many instances, this is for good reason. Transparency, coordination, and collaboration are core values of an effective government, particularly as it involves scientific agencies.

Openness, however, does not come without risk. Many of the technologies developed and utilized by NASA are just as useful for military purposes as they are for civil space applications. While our nation's defense and intelligence communities guard the "front door" and prevent network intrusions that could steal or corrupt sensitive information, NASA could essentially become an unlocked "back door" without persistent vigilance.

Information security concerns at NASA are not limited to non-proliferation. There is a serious economic competitiveness aspect as well. The loss or theft of NASA technologies could compromise U.S. innovation and curtail significant future commercial activities that bolster our economy. In order to ensure that NASA does not become the weak underbelly that allows enemies and competitors to access sensitive technologies, we have to make sure that NASA has the necessary authorities to protect that information.

The NASA Office of the Inspector General has monitored the Agency's cyber security for over a decade, issuing dozens of reports and recommendations. To NASA's credit, they have taken action to address those recommendations in a timely fashion by clarifying the role of the Headquarters Chief Information Officer, realigning the Agency's other CIOs under that office, setting up the Security Operations Center (SOC), and improving integration and visibility. Despite this progress, the threat to NASA's information security is persistent, and ever changing. Unless NASA is able to continuously innovate and adapt, their data, systems, and operations will continue to be endangered.

These are not simply bureaucratic matters that have no real-world impact, or theoretical possibilities with little chance of occurring. As the Inspector General points out in his testimony, NASA experienced 5,408 computer security incidents in 2010 and 2011. These intrusions resulted in the installation of malicious software or unauthorized access which caused significant disruptions to mission operations, the theft of export-controlled data and technologies, and cost the Agency more than $7 million.

Just last year, the theft of an unencrypted NASA laptop resulted in the loss of algorithms used to command and control the International Space Station. Similarly, the U.S. China Economic and Security Review Commission recently noted in its annual report to Congress that the Terra and Landsat-7 satellites "have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems."

The fact that NASA is a high profile target should come as no surprise. What is astonishing, however, is the fact that they are such a big target. NASA manages approximately 3,400 individual websites. For context, there are approximately 4000 websites throughout the rest of the government. Simply surveying this attack profile is a challenge, but defending it presents even more difficulties.

Adding to this complexity are differing security profiles for NASA's Centers, Mission Directorates and institutional capabilities. Despite the challenge, it is still imperative that NASA conduct a thorough Agency-wide risk assessment and develop a corresponding mitigation strategy in a timely fashion as recommended by the NASA IG last March.

I look forward to our witnesses' testimony, and hope that we can all work together to ensure that our nation's space agency can securely support and appropriately protect cutting edge research, collaborative science, and mission operations.

###