

COMMITTEE ON  
**SCIENCE, SPACE, AND  
TECHNOLOGY**  
CHAIRMAN LAMAR SMITH



For Immediate Release  
June 20, 2014

Media Contacts: Zachary Kurz  
(202) 225-6371

**Statement of Oversight Subcommittee Chairman Paul Broun M.D. (R-Ga.)  
Hearing on NASA Security: Assessing the Agency's Efforts to Protect Sensitive Information**

**Chairman Broun:** Thank you Chairman Palazzo. I would like to add my welcome to all of our witnesses here today as well. I am looking forward to hearing from you all on this important matter of which I have been concerned for a number of years now.

This Committee and the Oversight Subcommittee, in particular, have held multiple hearings examining the state of information security at NASA. A hearing two years ago highlighted the unique cybersecurity challenges that NASA continues to face with constant and ever-changing threats and adversaries. Just last year, the Oversight Subcommittee held a hearing to focus on the broad intersection of two very important issues at stake here today - finding the appropriate balance between scientific openness, and protecting our national security.

We have learned that NASA should not only worry about sensitive information going out of the back door through cyber intrusions and lax protocols, but also out of the front door by its inability to protect sensitive technology and information from foreign nationals who may have unauthorized access to NASA's facilities.

In October of 2012, I wrote to the GAO regarding these front door concerns and requested a review of NASA's export control program. While I was glad to see the completed GAO report released last month, I was troubled by many of the report's findings. For example, it is very troubling to learn that although NASA's oversight tools have identified deficiencies, NASA headquarters has not addressed them. The GAO report states specifically that "at NASA's 2013 annual review, the Center Export Administrators presented NASA headquarters export control officials with a list of comments regarding the export control program...However, NASA headquarters' export control officials acknowledged that they have not fully addressed the CEA concerns from the most recent program review in March 2013 and have not developed specific plans to do so." This is intolerable. This is not because of any disagreement between NASA headquarters' staff and NASA centers' staff; in fact the GAO report explains that NASA headquarters export control officials agree with issues raised by the CEAs - yet, they have failed to develop an approach to address them.

This is wholly inadequate for protecting our valuable assets. NASA needs suitable accountability and oversight in order to, at the very least, make certain the agency's own audit findings and suggestions are implemented.

Further troubling, the report states that GAO "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."

NASA relies on new and sophisticated technology to accomplish its mission. Given the sensitivity of these technologies, many are subject to U.S. export controls, which restrict the transfer of military and dual-use technologies. In order to protect our leadership in technological innovations, we must ensure that there is adequate and consistent oversight and management of NASA's export control program. It is in our national interest. It must be done!

I look forward to hearing from our witnesses on their insight and recommendations on these matters, and I hope that NASA will do everything in its power to address all of the shortcomings discussed today to ensure our nation's space agency can securely support and appropriately protect cutting edge research and technology.

Thank you again Chairman Palazzo for holding this very important hearing, and I yield back the balance of my time.