OPENING STATEMENT
The Honorable Ben Quayle (R-AZ), Chairman
Subcommittee on Technology and Innovation
Protecting Information in the Digital Age:
Federal Cybersecurity Research and Development Efforts

May 25, 2011

It is next to impossible to ignore the relevance of cybersecurity these days. News coverage has increasingly focused on cyber vulnerabilities covering stories such as a company losing personnel information or customers' financial data, or a government database being compromised by a malicious hacker. Perhaps most unsettling, is that most stakeholders agree that our national cybersecurity response has not kept pace with the threats.

In early 2008, the need to increase network security was brought to the forefront when President Bush formally established the Comprehensive National Cybersecurity Initiative (CNCI) to deal with widespread cyberattacks on Federal networks. Early in his administration, President Obama committed to continue this effort, and expanded it through the 2009 Cyberspace Policy Review, which identified a number of problems to be addressed through both near-term and mid-term actions. At that time, the Committee on Science, Space and Technology held a series of hearings evaluating the state of cybersecurity research and development and the recommendations contained within the Review.

Security efforts are often focused on the past, and designed to respond to the most recently faced attack. However, the technology sector is exceptionally dynamic, and where possible, we need to attempt to anticipate vulnerabilities and future threats. This is where research and development and proper coordination can make a contribution.

It has now been a number of years since the Review identified vulnerabilities across federal agencies. We are here today in part to evaluate what progress has been made.
Additionally, as new threats emerge, we must assess whether we are staying ahead with research and development. Finally, we must make sure that we are appropriately tracking federally funded research and development initiatives. Since multiple agencies have cybersecurity responsibilities, and federal efforts in this area are growing, I am concerned that agencies may compete with each other for cyber ownership. Congress must ensure that agencies are working collaboratively to prevent work from being duplicated at the cost of precious taxpayer funds.

Several agencies before us today have an important role in the development of cybersecurity standards. We should not underestimate the value of standards – whether they are minimum security measures for use by federal government agencies to protect information, or a framework to address cybersecurity risks for critical infrastructure. The lead responsibility for working closely with industry to develop successful standards has historically fallen to NIST.
We would like to ensure that any comprehensive cybersecurity legislation effectively leverages the expertise of all federal assets.

I should also note that today's hearing is focused on federal cybersecurity stakeholders. Notably absent are those who design, build, own, and operate the majority of the digital infrastructure in our nation. To that end, I intend to further the discussion of related cybersecurity issues through future hearings of the Technology and Innovation Subcommittee that will include voices from the private sector.

I would like to thank my co-chairman, Congressman Brooks, for sharing leadership on this important hearing. I also thank the witnesses for being here today and I look forward to a productive discussion.