COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
CHAIRMAN LAMAR SMITH

For Immediate Release
January 27, 2015

Media Contacts: Zachary Kurz, Laura Crist
(202) 225-6371

Statement of Research and Technology Subcommittee Chairwoman Barbara Comstock (R-Va.)
The Expanding Cyber Threat

Chairwoman Comstock: I want to begin by thanking everyone for attending the first hearing of the Research and Technology Subcommittee in the 114th Congress. I look forward to working with the Members of the Subcommittee on the many issues that fall under the jurisdiction of this Subcommittee.

The need to secure our information technology systems is a pervasive concern. Today's hearing marks the first of what will be several hearings to examine the topic of cybersecurity.

The Subcommittee has jurisdiction over the National Science Foundation, the National Institute of Standards and Technology and the Department of Homeland Security's Science and Technology Directorate. These organizations play a role in supporting basic research and development, establishing standards and best practices, and working with industry on cybersecurity concerns.

Advances in technology and the growing nature of every individual's online presence means cybersecurity needs to become an essential part of our vernacular.

Instances of harmful cyber-attacks are reported regularly and expose the very real threats growing in this area. Financial information, medical records, and personal data maintained on computer systems by individuals and organizations continue to be vulnerable. Cyber-attacks on companies like Sony or Target and the U.S. Central Command will not go away and we have to constantly adapt and intercept and stop these threats before they happen and understand where and how they are happening and stay ever vigilant.

Utilizing targeted emails, spam, malware, bots and other tools, cyber criminals, "hacktivists" and nation states are attempting to access information technology systems all the time. The defense of these systems relies on professionals who can react to threats and proactively prepare those systems for attack.

Our discussions about cybersecurity should examine the research that supports understanding how to defend and support our systems as well as how to better prepare our workforce by producing experts in these fields and learning of best practices in both the public and private sector. Well-trained professionals are essential to the implementation of security techniques. Institutions of higher education are working to create and improve cyber education and training programs focused on ensuring there are enough trained professionals to meet the needs of industry.

I look forward to hearing from our witnesses today as they provide an overview of the state of cybersecurity from the industry perspective and we learn how the federal government is playing a role in this important area.