COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
CHAIRMAN LAMAR SMITH

For Immediate Release
March 6, 2014

Media Contacts: Zachary Kurz
(202) 225-6371

Statement of Oversight Subcommittee Chairman Paul Broun (R-Ga.)
Hearing on Can Technology Protect Americans from International Cybercriminals?

Chairman Broun: Good morning. Let me begin by extending a warm welcome to our witnesses and thank you all for appearing. I especially appreciate everyone's patience and flexibility - witnesses and Members alike - in making themselves available today given the weather interruption earlier this week.

Today's hearing is titled "Can Technology Protect Americans from International Cybercriminals?" I hope you can all help us more fully answer that question and explore what specifically is being done to secure U.S. IT infrastructure.

On the one hand, we are here this morning to review what appears to be a rash of recent attacks and successful breaches of American IT infrastructure and computer networks: Target; Neiman Marcus; Easton Sports; Michaels Stores; the University of Maryland; Blue Cross Blue Shield in New Jersey; and now maybe even Sears! A reported 823 million exposed records made 2013 a record year for data breaches. The majority of these data breaches hit businesses and health-care, followed by government, academic, and financial institutions, in that order. In fact, the Identity Theft Center, a non-profit organization that tracks data theft, reported that health-care insurance providers and organizations suffered 267 breaches, or 43 percent of all attacks in 2013. That's significantly higher than the business sector, comprised of retailers, tech companies and others. It seems like an epidemic, and the clear implications of people's privacy being violated concerns me greatly.

On the other hand, fraud and breaches within the retail credit card and debit card industry only amount to five-hundredths of 1% of sales, or 5 cents on the dollar. And that loss has been declining. In other words, more records are being exposed, but the financial damage may be less. Is this a growing problem justifying more attention and effort, or an example of the ongoing, successful efforts of the private sector, with the help of the government's experience, knowledge, and cooperation to counter these attacks? I take pride in noting that financial technology companies in my home state of Georgia handle over 60 percent of all payment card transactions in America. These Georgia companies are industry leaders in consumer protection and data security, as documented in a February 23rd piece in the Peach Pundit by the CEO of the Electronic Transactions Association.

Today, among other things, we will hear what the private sector is doing in response to the market forces of risk, cost, liability, and reward. I would suggest those free market incentives and disincentives and the right of free association and cooperation are sufficient and the most effective at addressing the evolving, quick-moving threat of sophisticated hacking organizations and cybercriminals. The fact that the payment industry and retailers have been actively working together to make the necessary investments to tighten credit card and debit card security next year by transitioning to "smart or chip card" technology is proof of that.

Nevertheless, the organized, international nature of the new IT threat to intellectual property, trade secrets and other proprietary data, personally identifiable information, medical and insurance records, financial resources, and even top secret material, makes this a critical danger to our economic and national security. We will hear today that China and Russia are actively and aggressively waging economic war on us with massive hacking espionage campaigns. This is very disconcerting, and I look forward to the discussion about the role of law enforcement and intelligence capabilities to deter, detect, and punish global cybercrime syndicates, and whether they need more technological tools and resources.

After all, before former FBI Director Robert Mueller stepped down, he declared that "in the not too-distant-future we anticipate that the cyber threat will pose the greatest threat to our country." Well, it will be interesting to hear what the former FBI Deputy Assistant Director for Cyber, who served under Director Mueller, has to say in his testimony.

###