Embargoed Until Delivered
November 20, 2014

Contact: Allison Getty
202-225-7690
allison.getty@mail.house.gov

Ranking Member Opening Statement
HPSCI Open Hearing on Advanced Cyber Threats Facing the U.S.

Thank you, Admiral Rogers, for appearing before us today.

This Committee has been sounding the alarm on the cyber threat for years, and has twice led the House passage of critical cyber legislation. But the threat has not waited on the full Congress to act.

In 2012, we warned of the coming danger as a huge Saudi oil company, Saudi Aramco, suffered a devastating cyber attack. The virus—or malware—erased data on 30,000 of the companies' computers, replacing it with a picture of a burning American flag.

Then the threat hit our shores. We continued to warn as cyber attacks hit U.S. Government computers, including at the Department of Defense, the U.S. Sentencing Commission, and the U.S. Treasury. But, still, the full Congress did not act.

The threat then spread further, now to our private networks. Target was struck. Then our banks: J.P. Morgan was hit, as well as VISA, and Bank of America.

In FY2012, DHS responded to 198 cyber incidents across all critical infrastructure sectors. Of these, 40% were in the energy sector. The energy sector continues to bear the brunt of our country's cyber attacks because hackers recognize that the energy sector is our country's Achilles Heel.

The effects of an attack would send a shock wave through our economy. Remember how a single fallen tree in Ohio back in 2003 triggered a black-out for nearly 50 million people? Just think about what a cyber attack could do. It could be catastrophic.

We are watching the threat grow and spread. Attacks have hit the State Department and the White House. The danger is not waiting. So what's the full Congress waiting for?

Thank you to Chairman Rogers' leadership, and this bi-partisan Committee, the House passed its cyber legislation. This legislation would fix a dangerous gap in our nation's cyber armor—the inability to share threat information between the public and private sectors.

The private sector owns about 80% of the internet, which makes it difficult for the government to help protect our networks.

Right now, if your house is broken into, you call 911 and the cops come. But, if a company gets cyber attacked, and billions of dollars are stolen, they can't call a cyber 911 line in the same way.

On the other hand, the government may have cyber threat information but currently, there is no legislative framework in place to share it with the private sector.

It's like being able to see Hurricane Sandy heading up the coast, but not being able to warn anyone in its path. That's what our cyber legislation does. It enables this crucial two-way information sharing of cyber threat information.

It's the description of the burglar. It's the trajectory of the coming storm. That's what's being shared. Not private information.

The Senate has its own cyber legislation, which is very similar to ours, but which has not passed the full Senate. We need to move quickly to reconcile the two and pass the legislation. The threat is not going to wait.

So, thank you, Admiral Rogers, for talking to us today about the cyber threat, and thank you, Chairman Rogers, for holding this important hearing.

###