NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member

FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure

March 20, 2013 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the Cybersecurity, Infrastructure Protection, and Security Technologies subcommittee hearing entitled "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure":

"The list of significant cyber intrusions against our critical infrastructure keeps growing.

Our top government officials are going on the record about state sponsors of aggressive cyber activities that have been stealing our trade secrets and intellectual property as well as targeting our most sensitive critical infrastructure networks.

National Security Advisor Tom Donilon and Director of National Intelligence James Clapper have spent recent weeks identifying state sponsors of aggressive cyber activities – including China, Iran, and Russia.

And just last week, President Obama raised the issue of cyber attacks with the Chinese President, instantly raising the importance of cybersecurity in the US-China relationship.

But even though we have made great strides in our response to state-sponsored cyber activities, we cannot expect the problem to go away overnight.

It would be prudent to expect the future to bring new, more sophisticated attacks.

Even the best, most secure critical infrastructure in our country is no match for a determined adversary backed by the resources of a government.

That is why it is so important for this Committee to pass comprehensive cybersecurity legislation.

We must act to provide a framework which will improve the partnership between the owners and operators of our critical infrastructure and the government to work together collaboratively to protect our networks.

I look forward to working with you, Chairman Meehan and Ranking Member Clarke, as well as Chairman McCaul, to ensure that this legislative necessity becomes a reality.

But while the threats we face are severe, it is important that we do not overstate them or call for a militarized response.

Not all attacks require a military response. The vast majority of attacks are against individual citizens and the private sector.

We need a measured civilian response that permits these threats to be addressed by DHS and the FBI working together to mitigate and respond to the attacks, investigate the perpetrators, and help prevent future attacks.

Just last week, NSA Director Keith Alexander testified before Congress that cyber attacks on U.S. soil required a civilian-led response.

The evolution or increase in threats is no justification for abandoning the traditional separation of foreign and domestic intelligence and law enforcement authorities.

We cannot allow cyber attacks to provide a reason to jettison the precious and hard-won American values of privacy and civil liberties.

I am convinced that any measure we put forth must embrace privacy and civil liberties as a bedrock principle.

As we move forward with cyber security legislation, with those values firmly embedded, we must take the time to fully investigate and understand the scope of the threats we face.

So, I am pleased that we are joined today by this panel of experts, who can speak to the diverse array of cyber threats to our critical infrastructure, and I look forward to their testimony."

# # #

FOR MORE INFORMATION: Please contact Adam Comis at (202) 225-9978

United States House of Representatives
Committee on Homeland Security
H2-117, Ford House Office Building, Washington, D.C. 20515
Phone: (202) 226-2616 | Fax: (202) 226-4499
http://chsdemocrats.house.gov