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

The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure

April 15, 2011 (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 "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure":

"As you know, cybersecurity is an area of mutual interest, and I share the concerns of the Chairman and Ranking Member that this is one of our greatest national vulnerabilities.

I am concerned about the consequences of failures of our national critical infrastructures.

A cyber attack is one way that those infrastructures, such as our electric grids, our telecommunications system, and our financial services sector, could be disrupted.

These sectors, and many others remain vulnerable to attack.

We know that they are constantly being attacked, and that many of those attacks are successful.

I would like to echo remarks made by the Ranking Member at earlier hearings on this topic: We are already under attack. The enemy has already penetrated our infrastructures.

We know that foreigners and criminal organizations have infiltrated the computer systems that control our electric grids and have stolen huge amounts of our data for a variety of reasons, such as corporate espionage and identity theft.

But what happens when our enemies decide not just to steal from us but to actually disrupt or even destroy some of those critical infrastructures?

What happens when a virus disrupts, modifies, or destroys our financial data? How do we conduct our economic activities?

What happens when our telecommunications systems are taken down? How do we communicate?

We know that there are at least two threats: the aurora vulnerability and the stuxnet virus that can destroy components of our electric grid.

We faced a very limited government shutdown this week, and it caused a lot of concern.

But what if a widespread, sophisticated cyber attack takes our government networks down and bars us from cyber space?

All of these terrible scenarios, and countless others, could await us at any time.

We have been breached, and we are merely lucky that our critical systems have not yet been destroyed.

But make no mistake: that could happen at any time.

I have introduced a bill, H.R. 174, that would address these issues.

It grants DHS the authority to require government networks and networks in critical infrastructure sectors to meet security performance requirements.

I hope that action on the bill will commence soon.

Hopefully, our witnesses today will tell us that DHS has made some progress in working with critical infrastructures, but more work remains to be done.

This problem has been lingering for too long.

We need to move forward. Legislation, executive orders, and public-private partnerships will all play a role, but I am tired of hearing report after report about our networks being penetrated.

I thank the witnesses and look forward to your testimony. But if you tell me that we have the situation handled or that we are making great progress, I am going to be skeptical.

I want to hear where the breakdowns are and what needs to be done to fix them.

And then I want you to go do it, and if it takes legislation, I want this Committee and this Congress to act."

# # #

FOR MORE INFORMATION: Please contact Dena Graziano or 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