NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Chairman

FOR IMMEDIATE RELEASE

Statement of Chairman Bennie G. Thompson

"The Cyber Initiative"

February 28, 2008 (Washington) – Today, Committee on Homeland Security Chairman Bennie G. Thompson (D-MS) delivered the following prepared remarks for the full Committee hearing entitled "The Cyber Initiative":

"Shielding the Nation's critical infrastructure from foreign and domestic terrorism is one of my chief goals in charting the course towards freedom from fear.

That is why we are meeting today to discuss the infiltration and exploitation of federal government networks and critical infrastructure networks – one of the most critical national security issues confronting our country today.

Public reports suggest that Federal networks have been under attack for years. These attacks have resulted in the loss of indeterminate amounts of information.

The purpose of today's hearing is to discuss the Administration's proposed "Cyber Initiative," a proposal that attempts to reduce the vulnerability of our Federal computer networks and critical infrastructure and the consequences of attacks against these networks.

We aim to discuss several things today, including:

The consolidation of Trusted Internet Centers – known as "TICKS" – which will reduce the number of Federal connections to the Internet and allow for easier monitoring of incoming and outgoing traffic;

The implementation of the Department of Homeland Security's cyber monitoring capability throughout Federal agencies, known as EINSTEIN;

The privacy implications of electronic data collection;

Efforts underway to conduct damage assessments of Federal systems; and

Efforts to secure our Federally and privately-owned critical infrastructure from cyber attack.

Thus far, I have been extremely disappointed in this Administration's efforts in cybersecurity.

The Administration drafted a high-level "National Strategy to Secure Cyberspace" in 2002 that presented problems and possible solutions to high level cybersecurity issues, but never mandated any changes required to improve security.

In 2003, the Administration eliminated its top advisor on cybersecurity – Richard Clarke – who was a key advisor to the President. Then, after Congress pushed for the creation of an Assistant Secretary for Cybersecurity, DHS waited over a year to fill the position, and buried it four levels down in the bureaucracy.

Despite the creation of a cross-agency intelligence Director, this Administration failed to educate Federal agency officials on the cyber threat.

For instance, in a 2007 hearing before this Committee, the Chief Information Officer at DHS –

Scott Charbo – told us that he never received any intelligence reports about nation-state hacking and that he was unfamiliar with this activity. To me, this suggests a failure on the part of the Director of National Intelligence, who is charged with connecting dots that would prevent cross-agency intelligence failures from occurring.

This Administration regularly requested inadequate budgets for DHS cybersecurity activities, both for the National Cyber Security Division, the US-CERT, the CIO security budgets, and the R&D activities undertaken at the Science and Technology Directorate.

And this Administration has vested responsibility for securing these networks in folks who don't understand the threat or the technical methods to deal with the threat. Secretary Chertoff's decision to promote Mr. Charbo to the position of Deputy Under Secretary for National Protection and Programs, places him in charge of DHS's efforts in the Cyber Initiative.

This decision was made in spite of the Committee's investigation into how he and his staff failed both to protect the Department's computers from intrusions and properly manage the contractor in charge of security.

In light of these and other issues, it's hard to believe that this Administration now believes it has the answers to secure our Federal networks and critical infrastructure.

I want to be clear – I believe that cybersecurity is a serious problem – maybe the most complicated national security issue in terms of threat and jurisdiction. This problem will be with us for decades to come.

I am pleased that this Administration recognizes the challenges we face in securing this arena.

As Chairman of this Committee, I continue to have numerous practical and theoretical questions about the Initiative and the possibility of its success:

Who is in charge?

What are the metrics for success?

Who is accountable?

How are privacy concerns being addressed?

How will future technologies be incorporated?

How will future threats be addressed?

What legal frameworks must be amended?

How will the Administration work with the private sector?

What will be done with critical infrastructure?

Simply put, securing our infrastructure and cyber networks from an attack advances my commitment to making clear that our government can provide the American people security, accountability, and most importantly, freedom from fear."

# # #

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