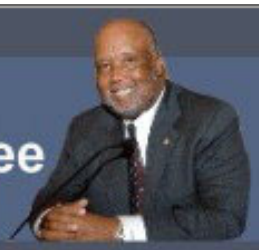
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



Statement of Ranking Member Bennie G. Thompson

"Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management"

October 30, 2013 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the Cybersecurity, Infrastructure Protection, & Security Technologies subcommittee and the Emergency Preparedness, Response, and Communications subcommittee joint hearing entitled "Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management":

"In 2010, former White House Counterterrorism Advisor Richard Clarke stated that this country's lack of preparation for a cyber attack could lead to a breakdown in our critical infrastructure system that would be like an "electronic Pearl Harbor." While some may consider his assessment a bit exaggerated, I think we would do well to remember it as we begin today's hearing.

We should also recall that in the 112th Congress, this Committee marked up cyber security legislation. Unfortunately, the Republican leadership of the House did not allow that legislation to come to the floor of the House. In January, the President issued an executive order requiring certain basic steps that will improve this nation's ability to protect and defend against cyber attacks.

While I applaud the President's efforts, I must point out that an Executive Order cannot expand existing legal authorities. In May of this year, the Department of Homeland Security testified before this committee that the "United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace." DHS also told us the Department processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure, and the Department's industry partners--- a 68 percent increase from 2011.

Mr. Chairman, I think that we should all have concern about cyber attacks on critical infrastructure—especially attacks that could disable the electric grid. For most of us, spending a day or two without electricity is an inconvenience. For others, it can be a matter of life or death. That is why I am pleased that Rep. Payne, Jr. introduced H.R. 2962, the SMART Grid Study Act. If enacted, the bill will require a comprehensive study to examine the construction, job creation, energy savings and environmental protections associated with fully upgrading to a SMART Grid System. The information gathered in the study may help us reduce the frequency and severity of outages during disaster events. I urge my colleagues to support this bill.

Still, there is more to be done. We cannot begin to address the current threats or anticipate future vulnerabilities if we have not invested in the kind of education and training necessary to develop the next generation of cyber professionals. Federal, state and local governments and the private sector are each vulnerable to cyber attacks. While the threats from and sophistication of hackers continues to grow, initiatives to address this mutual vulnerability must be comprehensive and coordinated. This country's history has repeatedly shown that a shared commitment to a common goal is necessary to achieve progress—from bringing electricity to the nation to walking on the moon. Today, the same kind of commitment and collaboration is necessary to address the cyber threat.

Like every previous movement that resulted in progress, this first step must be education.
That is why I am pleased that yesterday, this committee marked up Rep. Clarke's bill, H.R. 3107, the Homeland Security Cybersecurity Boots-on-the-Ground Act. This bill will help foster the development of a national security workforce capable of meeting current and future cybersecurity challenges, and it will outline how DHS can improve its recruitment and retention of cybersecurity professionals.

Mr. Chairman, I urge this committee to continue to put forward the kind of legislation that will help this nation resolve our known vulnerabilities. More than any other committee, we must be on the forefront of proposing innovations and pushing forward commonsense solutions.

# # #

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