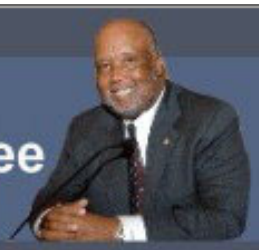
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Oversight of Executive Order 13636 and Development of the Cybersecurity Framework

July 18, 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 "Oversight of Executive Order 13636 and Development of the Cybersecurity Framework":

"Several years ago, this Committee passed the legislation that became the DHS' Chemical Facility Anti-Terrorism Standards (CFATS) program. CFATS was one of this Committee's first attempts to proactively explore how to make this country safer by engaging the private sector. We knew that no private facility wanted to become the target of terrorists. But we also knew that the private sector does not often view the government as a partner.

We needed to create a structure that permitted government and the private sector to work together without fear of penalty or reprisal. I believe we created such a system. Today, we are here to discuss another instance in which the private sector is being asked to cooperate with the government to safeguard the American people. While the potential danger posed by a terrorist attack on a chemical facility is easy to understand, the threat posed by an attack on the cyber network of a facility is difficult to envision.

But let's be clear-- cyber attacks that cause large scale system failures among the businesses and organizations that we use every day would not only cause inconvenience, for some people, such system failures could be life-threatening.

While something in our history and culture may not allow us to admit it easily, we need to acknowledge that we rely on the everyday presence of power plants, hospitals, manufacturing plants, mass transit and subway systems, airports, and the system of electronic commerce.

And in our current world, none of these systems can exist without a computer network that is linked to many other computer networks. Our national and individual interests depend upon the protection of these networks and the security of the information in them.

Government and the private sector must work together to assure that the owners and operators of these facilities are able to safeguard their operations and assets from the risk of cyber attack. Also, we must be sure that if attacked by a cyber terrorist, these facilities are able to quickly determine the damage, recover from the injury and move forward.

The cyber security executive order attempts to achieve these goals. Needless to say, I would prefer that this Congress take up legislation to address the many cyber security threats facing the critical infrastructure of this nation. However, this Congress seems to have a difficult time engaging in the legislative process.

Thus, I look forward to the implementation of Executive Order 13636, which directs Federal agencies to coordinate the development and implementation of risk-based standards. I look forward to hearing about the progress being made on the implementation of this order."

# # #

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