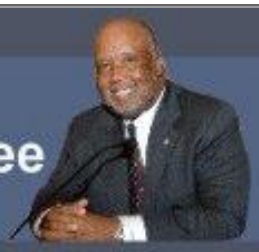
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Emerging Cyber Threats to the United States

February 25, 2016 (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 "Emerging Cyber Threats to the United States":

"Earlier this Congress, this Subcommittee heard from the federal government in detail the roles that the Department of Homeland Security takes in its mission to secure information networks and provide resilience, not only to government systems, but to assist private networks and data and protecting the nation's critical infrastructure.

On February 16, the Department of Homeland Security along with the Department of Justice issued guidelines and procedures required by the Cybersecurity Act of 2015. These guidelines provide both the federal government and the private sector with an understanding of how to share cyber threat indicators with the DHS National Cybersecurity and Communications Integration Center (NCCIC).

DHS and DOJ issued a separate guidance for the private sector. Today, I would like to hear from our witnesses, their take on the DHS and DOJ private sector guidance. Now that this Committee has written and passed useful legislation giving the DHS authorities to use and share its threat intelligence with private companies, and for companies to do the same with government in return, and DHS has published guidelines, it is our responsibility in Congress to oversee the realization of a mature risk management process for information security, and I hope we will hear some of the risk-based management approaches today.

Given the complexity of emerging threat capabilities, the link between physical and cyber domains and the diversity of cyber criminals, I would like to hear what challenges the private sector faces in working with the Department of Homeland Security.

For Congress to continue to make effective cybersecurity policy, whether it is related to cyber hygiene or infrastructure protection, it is our job to understand not only the scope of the problem, but also how our public and private sectors work together to enhance security.

Mr. Chairman, as an aside, for the past few weeks, cyberspace headlines have been littered with high profile cases. From the as-yet-to-be determined cyber-based electric grid problems in Ukraine, to a California hospital ransom-ware event…in which the hospital did not tell anyone about until after they had paid the ransom...to the encryption dilemma surrounding law enforcement access to some of the data on the mobile phone of a home-grown terrorist.

All of which need careful consideration, investigation, and deliberation. I would suggest that to make progress on all of these issues, we need to tone down the confrontational speech-making, rather than remaining on this argumentative, and adversarial highway."

# # #

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