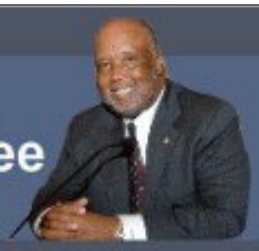
NEWS ALERT

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 Cybersecurity Act of 2015: Industry Perspectives

June 15, 2016 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the Emergency Preparedness, Response and Communications subcommittee and Cybersecurity, Infrastructure Protection, and Security Technologies subcommittee hearing entitled "The Cybersecurity Act of 2015: Industry Perspectives":

"Today, the Subcommittee turns its attention to another pressing issue: securing our cyber networks. Cyber threats are constantly evolving. While a few years ago, critical infrastructure operators were primarily concerned about spear-phishing and DDOS attacks, today, the threat of ransomware attacks are front-of-mind. Over the past year, the proliferation of ransomware attacks, where networks of a hospital system, government agency, or utility are held hostage for electronic payments, has reached epidemic proportions.

In March, DHS reported that over the past year, there have been 321 incidents of "ransomware-related activity" affecting 29 Federal networks. The FBI Internet Crime Complaint Center, for its part, has acknowledged that over the last decade, of the $58 million in financial damage attributable to such attacks, attacks in just the last year account for $24 million in damage.

With more Americans coming to embrace the Internet of Things, the disruptive and damaging effects of ransomware and other innovative modes of deployed by hackers have the potential to inflict significant damage to our nation.

To counter this threat, we must redouble our efforts to promote cyber hygiene practices, encryption, and information sharing. The enactment of the "Cybersecurity Act" in December provides for the sharing of information on cybersecurity threats and defensive measures between the government and the private sector and within the private sector.

Privacy, liability, and anti-trust provisions that are universally understood as essential to the timely sharing of cyber threat information are part of this law. Under the Act, the epicenter for such activity is, of course, the National Cybersecurity and Communications Integration Center.

I am interested in exploring two key mandates in the Act. First, I want to hear from industry stakeholders how they see the launch of the "Automated Indicator Sharing" capability, as required under the Act, impacting information sharing.

Second, I would like to hear the witnesses' perspective on how well DHS is carrying out the requirement to periodically share, through publication and targeted outreach, cybersecurity best practices in a manner that gives "attention to accessibility and implementation challenges faced by small businesses."

Before I close, I would like to note that, this past week, I was heartened to see how the United States stacks up to other nations when it comes to vulnerability to hacking.

The U.S. was ranked fourteenth on the "National Exposure Index," a world-wide comparative analysis of vulnerability to cyber attacks and cyber crime that is based on the scanning of millions of internet channels for vulnerabilities such as unencrypted and plain text services.

While it is good to see that the United States is less vulnerable than Brussels, Australia, France, and China-- countries on the list found to have weak authentication and encryption practices-- now is not the time to rest on our laurels.

# # #

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