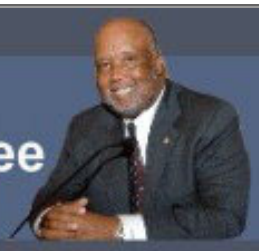
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Examining the President's Cybersecurity Information Sharing Proposal

February 25, 2015 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the full Committee hearing entitled "Examining the President's Cybersecurity Information Sharing Proposal":

"Over the past decade, we have witnessed an explosion of Internet use in all aspects of life. As a Nation, we do more business online than ever before -- trillions of dollars a year. For most Americans, smartphones, tablets, and other computers have become the platforms on which we live, work, and play.

Unfortunately, these devices and networks have also become targets for bad actors.

Last month's cyberattack on the Nation's second-largest health insurer, Anthem, resulted in tens of millions of Social Security numbers, birth dates, addresses and names being stolen from its database. Given that Anthem insures 7.5 million people in 14 States, the potential damage of this breach is expected to be extensive.

Last year's attack on Sony destroyed data, disabled thousands of computers, and exposed the personal information of Sony employees.

These attacks underscore that any network that is connected to the Internet is a potential victim.

The fact that our Nation's critical infrastructure – including the power grid, financial institutions, and health care systems – are all connected to the Internet make them particularly attractive targets for attack.

Cyber attackers are constantly probing for weaknesses in our critical infrastructure which powers much of our electric grid, financial institutions and health care systems.

The attention that cybersecurity has received in recent years by President Obama and Congress is reflective of the increasing awareness that the responsibility to address this homeland security threat is a collective one.
At its core, cybersecurity relies on effective information sharing among network operators about indicators, hacks, and cyber vulnerabilities.

This Committee has been central in efforts to foster better cyber information sharing by producing bipartisan cybersecurity legislation that President Obama signed into law at the end of last year.

The "National Cybersecurity Protection Act of 2014" authorizes the National Cybersecurity and Communications Integrity Center (NCCIC) within the Department of Homeland Security as an information sharing hub for cybersecurity risks and incidents, and directed the NCCIC to provide technical assistance, risk management support, and incident response capabilities to impacted network operators.

The legislative proposal that the President unveiled last month has, again, spurred debate.

Importantly, the Administration's proposal would require participating companies to comply with certain privacy restrictions such as removing unnecessary personal information and taking measures to protect any personal information to qualify for liability protection.

In my view, the President's proposal has some merit.

As we go forward, we should consider the following questions: First, what is being shared?—is it just computer code made up of "zeroes and ones" or does the information contain Americans' sensitive personal data? If it does contain personal data, I believe that "reasonable efforts" should be made by participating companies to remove "personally identifiable information" from information shared with the government. This will help to preserve Americans' privacy.

Second, who is doing the sharing?—is it a critical infrastructure operator?

Third, where is the sharing happening?—the answer to that question has privacy implications—particularly when the sharing is between the Federal government and the private sector, as opposed to sharing between private sector companies.

I look forward to hearing testimony from our witnesses on the potential risks and rewards of a cyber information sharing environment dominated by ISAOs, as the President envisions.

Certainly, I would like to hear how these proposed changes could impact the NCCIC. The success of the NCCIC is dependent on companies seeing the "value proposition" for sharing with the Department.

I look forward to hearing from the Department on how they intend to drive traffic to the NCCIC and how implementation of the new cyber law is progressing.

I would also like to hear more about the new education grant program that the President has proposed.

While I am pleased that the President seems to agree about the importance of making this investment in growing our cyber workforce, I am disappointed that the proposal calls for just $5 million a year to be spent over five years at thirteen Historically Black Colleges and Universities, and two national laboratories, is disappointing.

Given the billions of dollars spent on cybersecurity, much of which is spent on Federal contractors, I would have expected a more ambitious plan for developing cyber talent.

Before I close, I would like to acknowledge that the Committee just met with the President's cybersecurity advisor, Michael Daniel. I appreciate Mr. Daniel's willingness to lay out the Administration's vision for cybersecurity and to address our questions, particularly about the newly-announced cyber center that will be housed in the Intelligence Community.

On February 11th, together with the Chairman and the leadership of the Senate Homeland Security and Governmental Affairs Committee, we wrote to the President about this new "Cyber Threat Intelligence Integration Center". We look forward to a formal response to our questions, particularly as they relate to the NCCIC.

In conclusion, I look forward to hearing from our witnesses today and to working with the Chairman on forthcoming legislation to help ensure that the networks of our Nation's critical infrastructure are more secure.

# # #

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