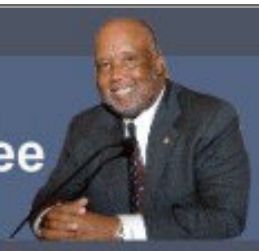
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Markup - the National Cybersecurity Protection Advancement Act

April 14, 2015 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the full Committee markup of the *National Cybersecurity Protection Advancement Act (H.R. 1731)*:

"At the outset, I would like to acknowledge the collaborative and inclusive approach that was taken to develop this legislation. Today's markup is an opportunity for this Committee to continue to show leadership on cybersecurity.

Last December, we succeeded in enacting bipartisan legislation to provide new authorities to the Department of Homeland Security as the lead Federal agency responsible for working with the private sector to make cyberspace more secure.

As we began our work this Congress, high-profile attacks on Sony, Anthem healthcare, Target, and Home Depot, have brought into sharp focus the fact that cybersecurity is a shared responsibility. Cybersecurity is one of those place where the old adage "knowledge is power" applies. When companies come forward and share their knowledge about imminent cyber threats, timely actions can be taken to mitigate or even prevent damage to vital IT networks.

These days, it seems like every month, Americans read about some wide-scale cyber incident that leaves them exposed to identity fraud and other harms.

What does not make news is when a company avoids a major cyber attack by taking simple and timely actions, like patching software and installing firewalls, to protect their data and their customers. However, companies take such actions daily. As such, information sharing can be a powerful cybersecurity tool.

That is why I am pleased that the legislation we are considering today authorizes private companies to voluntarily share malware, suspicious signatures, and other cyber threat indicators with DHS or another impacted company.

I am also pleased that the bill authorizes companies to monitor their own IT networks to identify penetrations and take steps to protect their networks from cyber threats. Importantly, the bill requires any participating company to make reasonable efforts to scrub the data it shares to remove information that could identify a person, when that person is not believed to be related to the threat.

It also directs DHS to scrub the data it receives, as an added layer of privacy protection. Additionally, the bill requires the National Cybersecurity and Communications Integration Center (NCCIC) to have strong procedures for protecting privacy and calls for robust oversight of the NCCIC by the Department's Chief Privacy Officer, its Chief Civil Rights and Civil Liberties Officer and Inspector General, and the Privacy and Civil Liberties Oversight Board.

Much of the bill is the product of months of bipartisan stakeholder engagement where this Committee sought the best ideas from a broad array of stakeholders on how to effectively foster

better information sharing while protecting privacy.

However, unfortunately, at the direction of the House Republican Leadership, language on liability protection was dropped into this bill with no regard for the complexity of this issue and no possibility to negotiate.

As written, it would put an unduly complicated structure in place that runs the risk of directly or inadvertently providing liability relief to a company that acts negligently. It only allows lawsuits where a plaintiff can prove 'willful misconduct.' Bizarrely, on page 35, line 22, it actually incentivizes companies not to act on cyber threat information by explicitly protecting inaction.

This provision runs counter to the fundamental goal of this legislation which is to get cyber threat information to companies to empower them to take action to protect their networks.

We can do better. I support President Obama's tailored, straightforward approach to providing liability protection. Later today, Mr. Richmond, our leader on the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee, will be offering amendments to ensure that companies are provided the liability protection they need but that negligence and inaction are not rewarded.

I hope that Members will support his efforts to make this right. The irony here is that even as we meet and wrestle with the language, the White House is negotiating with a different House Committee to change this provision.

That said there are a number of amendments that Democrats will be offering today to make improvements to the bill that I hope will be accepted. I look forward to a robust debate on this timely homeland security issue."

# # #

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