BE PREPARED FOR CYBERSECURITY WEEK

From: The Committee on Homeland Security - Minority Staff
Bill: H.R. 3523
Date: 4/20/2012

Be Prepared For "Cybersecurity Week"

Three Things to Know About CISPA (H.R. 3523)

April 20, 2012

Dear Colleague:

Information sharing is vital to promoting to preventing, containing, and mitigating devastating cyber attacks. As someone committed to improving our Nation's cybersecurity posture, I have an interest in promoting the voluntary sharing of information about hacks, incursions, and other cyber threats between and among the Federal government and the private sector. The main rule bill to be considered next week, in what is being touted as "Cybersecurity Week," is H.R. 3523 – The "Cyber Intelligence Sharing and Protection Act" (CISPA). Here are three things you need to know about CISPA, to understand the steady drumbeat of criticism that has been building against this bill.

(1) CISPA would create a "Wild West" of cyber information sharing, where any certified private entity can share information with any government agency. Not only does this raise privacy concerns with a framework running counter to the traditional foreign focus for military and intelligence agencies, it would create a more ambiguous and diffuse structure for Federal cybersecurity efforts, with no one agency having the whole picture, instead of clarifying and streamlining those efforts.

(2) CISPA allows companies to broadly share sensitive and private information about Americans' Internet use with the government. It allows the sharing of Internet use records or the content of emails for "cybersecurity purposes" and unlike proposals drafted by Sens. Joe Lieberman and Dianne Feinstein or the Obama Administration, CISPA does not require companies to remove personally-identifiable information (PII) that could be tied to a specific individual.

(3) CISPA lets the government use the private information it collects about Americans for <u>any purpose</u> it deems fit (outside of regulation). Under CISPA, the information that companies choose to share to foster greater cybersecurity can be used by the government for "any lawful purpose" so long as a "significant purpose" of its use is a cybersecurity or national security one. While the "significant purpose" limitation may sounds like a measure of protection, in practice such language—when inserted in foreign intelligence surveillance laws—has been virtually meaningless.

In light of these concerns, the following not-so-veiled criticism of CISPA from an Obama Administration spokesperson comes into focus: *"while information sharing legislation is an essential component of comprehensive legislation to address critical infrastructure risks, information sharing provisions must include robust safeguards to preserve the privacy and civil liberties of our citizens. Legislation without new authorities to address our nation's critical infrastructure vulnerabilities, or legislation that would sacrifice the privacy of our citizens in the name of security, will not meet our nation's urgent needs."*

Next week, I intend to offer an amendment to strike the right balance between security and privacy. It can be done, and with your support, it will be done.

Sincerely,

Bennie G. Thompson (D-MS)
Ranking Member, Committee on Homeland Security