West Texas Cyber Security Consortium

Latest cyber security bill riddled with Net neutrality loopholes

Critics attack CISA's vague wording for providing a backdoor route for mounting attacks on Net neutrality and privacy

By **Serdar Yegulalp** | **InfoWorld**

The latest cyber security information sharing bill being considered in the Senate strikes many as overly broad and in need of revision. In fact, say some it's worded vaguely enough that it could be used by ISPs to sidestep Net neutrality provisions in the name of public safety.

The **Cybersecurity Information Sharing Act (CISA)** has already been **roundly criticized** for having troubling implications for privacy. Ostensibly devised to allow the private sector to share with the government information about cyber security threats, it's been attacked for potentially allowing companies to share any personal information they please with the government under the guise of being a security issue. Worse, the few anonymization provisions present in the bill can be **easily dodged**.

The wording of the bill -- like with so many of its predecessors that went down to defeat -- is being carefully scrutinized for possible side effects, including being used as a backdoor way for ISPs to undermine Net neutrality. **Motherboard** argues that the "countermeasures" provision in the bill allows for a broad range of responses and could be used by an ISP to take actions to protect itself from anything it chooses to brand as a threat. For example, throttling Netflix could be classified as a countermeasure as long as a good excuse could be found. Previously, ISPs used **jeopardized back-end peerage deals** to justify throttling; the pervasiveness of security threats could make such actions easier.

A **letter jointly authored by a number of civil liberties groups** and sent to the bill's sponsors, Senators Dianne Feinstein (D-Calif.) and Saxby Chambliss (R.-Ga.), outlines a number of ways the bill could be abused. In addition to worries that CISA could lead to a militarization of the cyber security program, the letter also expresses concerns

about how provisions in the bill "could be construed to modify or alter any Open Internet rules adopted by the Federal Communications Commission. Net neutrality is a complex topic and policy on this matter should not be set by cyber security legislation."

It's hard to argue with the idea of a robust system for sharing information about cyber threats. Microsoft has unveiled its own **Interflow** system for such sharing, which uses open standards (good) on top of Microsoft's proprietary cloud platform (not so good).

But so far, Congress's proposed plans for sharing threat data have all illustrated how legal language wielded by nontechnical people can create more problems than they solve and need to be more carefully constructed to avoid opportunistic abuse.

http://www.infoworld.com/t/net-neutrality/latest-cyber-security-bill-riddled-net-neutrality-loopholes-245510?source=IFWNLE_nlt_sec_2014-07-03