Revised Cyber Security Act 2012

By: Peter S. Bauman, Esq.

http://commercialcounselor.com/

Congress has been struggling with cyber security issues for several years, most recently in connection with the Cybersecurity Act of 2012 (CSA2012).

CSA2012 is an attempt to protect the nation's critical infrastructure from cybersecurity risks. The initial version of the bill attempted to do so by first identifying critical infrastructure, then requiring owners and operators of such assets to meet cybersecurity performance requirements.

But objections raised by privacy advocates led to a revised bill (S. 3414), which relies on voluntary private sector compliance with cybersecurity standards. [InsidePrivacy]

Specifically, CSA2012 establishes a National Cybersecurity Council tasked to:

- conduct sector-by-sector risk assessments;
- identify categories of critical cyber infrastructure;
- coordinate adoption of private-sector recommended voluntary outcome-based cybersecurity practices;
- establish an incentives-based voluntary cybersecurity program for critical infrastructure to encourage owners of critical infrastructure to adopt such practices;
- develop procedures to inform critical infrastructure owners and operators of cyber threats, vulnerabilities, and consequences;
- provide any technical guidance or assistance requested by owners and operators.

A designation of critical cyber infrastructure would apply only "if damage or unauthorized access could reasonably result in: (1) the interruption of life-sustaining services (including energy, water, transportation, emergency services, or food) sufficient to cause a mass casualty event or mass evacuations; (2) catastrophic economic damage to the United States, including financial markets, transportation systems, or other systemic, long-term damage; or (3) severe degradation of national security." [Bill Summary]

The revised Bill also imposes new limits on how information can be used and shared by private and Federal entities.

In the case of Federal entities, use of such information is generally limited to protecting an information system or information from cybersecurity threats. Federal entities may also share information with law enforcement, but only (i) to protect information systems from a cybersecurity threat or investigate, prosecute, or disrupt a cybersecurity crime; (ii) to protect individuals from an imminent threat of death or serious bodily harm; or (iii) to protect minors from any serious threat, including sexual exploitation and threats to physical safety. [Sec. 704(g)(2)(A)(ii)]

The revised CSA2012 may have been the product of discussion among various stakeholders but some argue that privacy groups "added so much baggage to the information sharing provisions that the new law is nearly useless to private sector companies who want to improve cybersecurity." http://bit.ly/N6h2cN

In addition, there are concerns that, among other things, the current version of S. 3414 will prevent private parties from publicly identifying hackers whose actions compromise cybersecurity.

For over 35 years small businesses, major corporations, public entities, individuals and insurance companies have depended on Tharpe & Howell, LLP, to deliver pragmatic, innovative, cost-effective civil litigation and transactional solutions. For more information, please contact us at (818) 473-5720 or email your request to cabusinesslawreport@tharpe-howell.com.