Public Policy

July 28, 2014

House of Representatives Passes SAFETY Act Amendment

Clarifies that liability protections are available for cyber attacks

By Brian E. Finch

The U.S. House of Representatives took a major positive step towards increasing the nation's cyber security posture today when, on a voice vote, it passed H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act."

The NCCIP bill, co-sponsored by House Homeland Security Chairman Mike McCaul, Ranking Member Bennie G. Thompson, Subcommittee Chair Patrick Meehan, and Subcommittee Ranking Member Yvette Clarke, clarifies a number of roles and responsibilities of the Department of Homeland Security (DHS), and it also strengthens key public/private partnerships.

One of the most interesting and potentially helpful elements of the NCCIP bill is in Title II, Section 202. There, the House approved additional language to be inserted into the Support Anti-Terrorism by Fostering Technologies Act of 2002 (the SAFETY Act). The language would add the term "qualifying cyber incident" to the SAFETY Act, thereby making it perfectly clear that cyber attacks **unconnected to "acts of terrorism"** may trigger – at the discretion of the Secretary of Homeland Security – the liability protections offered by the SAFETY Act.

The specific language clarifying this position reads as follows:

> *"(7) QUALIFYING CYBER INCIDENT.—*
>
> *(A) IN GENERAL.—The term 'qualifying cyber incident' means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.*
>
> *'(B) REQUIREMENTS.—A qualifying cyber incident meets the requirements of this subparagraph if—*
>
> *(i) the incident is unlawful or otherwise exceeds authorized access authority;*

(ii) the incident disrupts or imminently jeopardizes the integrity, operation, confidentiality, or availability of programmable electronic devices, communication networks, including hardware, software and data that are essential to their reliable operation, electronic storage devices, or any other information system, or the information that system controls, processes, stores, or transmits;

(iii) the perpetrator of the incident gains access to an information system or a network of information systems resulting in—

(I) misappropriation or theft of data, assets, information, or intellectual property;

(II) corruption of data, assets, information, or intellectual property;

(III) operational disruption; or

(IV) an adverse effect on such system or network, or the data, assets, information, or intellectual property contained therein; and

(iv) the incident causes harm inside or outside the United States that results in material levels of damage, disruption, or casualties severely affecting the United States population, infrastructure, economy, or national morale, Federal, State, local, or tribal government functions.

(C) RULE OF CONSTRUCTION.—For purposes of clause (iv) of subparagraph (B), the term 'severely' includes any qualifying cyber incident, whether at a local, regional, state, national, international, or tribal level, that affects—

(i) the United States population, infrastructure, economy, or national morale, or

(ii) Federal, State, local or tribal government functions."

As the SAFETY Act is currently written, its protections apply when the Homeland Security Secretary declares that an "act of terrorism" has occurred. The definition of "act of terrorism" is extremely broad, and basically covers any unlawful attack intended to cause harm (including physical, property, or financial) in the U.S. with weapons or other instrumentalities intended to cause such harm. Under that current definition, the SAFETY Act should apply to cyber attacks unconnected to "terrorist" activity.

By adding the section referring to a "qualifying cyber incident", however, Congress has seen fit to make it perfectly clear inside and outside the federal government that the SAFETY Act offers liability protections for a whole range of cyber attacks. The amendment makes explicit that theft of information, disruption or destruction of data, and of course disruption or destruction of operations through cyber manipulation can trigger the liability protections offered by the SAFETY Act law.

Passage of this language will be extremely beneficial to the country as it will clear up lingering (but misplaced) concerns that the SAFETY Act does not apply to losses incurred as a result of cyber attacks. Now, companies public and private will have every reason to examine the protections offered by the SAFETY Act in case of a cyber attack and then make the appropriate determination as to whether they should take advantage of its liability limitations.

Passage of this bill is of course only one step on the SAFETY Act amendment becoming law. The U.S. Senate still must either pass similar language or agree to the House bill as part of legislative conference on

a bill to be ultimately sent to the President. Time will only tell whether this bill will actually become law. However, it is certain that its becoming law will be of great benefit as companies struggle to determine how they should best protect themselves from cyber attacks.

If there are any questions about the SAFETY Act amendment language or how companies can take advantage of the SAFETY Act as currently drafted, please feel free to contact Brian Finch at brian.finch@pillsburylaw.com or 202-663-8062.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Brian E. Finch **(bio)**
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com