Government Contracts

Congress Considering SAFETY Act Amendment to Provide Liability Protection for Cyber Attacks

By Kevin P. Mullen, Mary Ellen Callahan and James A. Tucker

Sophisticated cyber-attacks are becoming more prevalent against critical public and private computer assets in the United States, putting the nation's infrastructure at greater risk. In addition to the Executive Branch response to the 2013 Executive Order on Cybersecurity, Congress currently is debating a significant response to this threat in H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2013 ("NCCIP Act"). Among its provisions is an expansion of the powerful liability protections afforded by the SAFETY Act. If the bill passes, cybersecurity providers soon may be eligible for the same protections currently extended to providers of anti-terrorism technologies.

I. The SAFETY Act

Following the September 11, 2001 terrorist attacks, Congress passed the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 ("SAFETY Act"), as part of the Homeland Security Act of 2002. The SAFETY Act was designed to prevent the risk of liability from deterring the development, deployment, and commercializing of technologies that could save lives in the event of another act of terrorism.

Broadly speaking, the SAFETY Act limits liability for "claims arising out of, relating to, or resulting from an act of terrorism," where a qualified anti-terrorism technology has been deployed and the seller has maintained the prescribed level of insurance coverage. As used in the Act, "anti-terrorism technology" applies to a wide range of new and existing technologies, procedures, software, and services that have been "designed, developed, modified, procured, or sold for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, for which a Designation has been issued pursuant to this part." *See* 6 C.F.R. § 25.2.

The Department of Homeland Security, which administers the Act, grants two classes of qualification for anti-terrorism technologies: Designation and Certification. Both classes provide the following protections, limiting a seller's exposure to tort claims of third-party plaintiffs harmed in a terrorist attack:

- Exclusive Federal jurisdiction for claims for property loss, personal injury, or death against providers of qualified anti-terrorism technologies that are deployed in defense against or recovery from acts of terrorism;
- Liability capped at the provider's liability insurance coverage, as specified in the provider's Designation or Certification;
- Elimination of joint and several liability, with a provider liable only for the percentage of noneconomic damage that it caused;
- Elimination of punitive damages and prejudgment interest; and
- Further reduction of liability by the amount of other compensation a plaintiff is eligible to receive (*e.g.*, from insurance or Government benefits).

In addition, a Certification creates a rebuttable presumption that the provider enjoys the government contractor defense – complete immunity against certain claims "arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies . . . have been deployed in defense against or response or

recovery from such act and such claims result or may result in loss to the Seller," whether the technology was sold to the Government or to the private sector.

II. Acts of Terrorism and Cyber-Attacks

The liability protections of the SAFETY Act currently are triggered only by an "act of terrorism." The Act's implementing regulations define "act of terrorism" as an act determined by the Secretary of Homeland Security to meet the following three criteria:

1. [The act] [i]s unlawful;
2. Causes harm, including financial harm, to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and
3. Uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

6 C.F.R. § 25.2.

Many cybersecurity technologies defend against or mitigate the harm of such acts and already may be eligible for SAFETY Act Designation or Certification. The definition of "act of terrorism" is worded broadly enough for protection to be triggered by illegal cyber attacks that are designed to cause "mass destruction, injury, or other loss" to U.S. citizens or institutions, and that do cause such harm. Other cyber attacks, however, may not fall so neatly into the regulatory definition of "act of terrorism," and, therefore, would not trigger the statute's liability protection.

III. NCCIP Act and "Qualifying Cyber Incidents"

Among other improvements to the nation's defense against cyber-attacks, Section 202 of the NCCIP Act would amend the SAFETY Act to extend its liability protection beyond "acts of terrorism" to also cover "qualifying cyber incidents." This would broaden the pool of technologies eligible for Designation and Certification, and expand the potential events that could trigger the SAFETY Act's powerful liability coverage.

Under the proposed amendment, a "qualifying cyber incident" would exist and trigger SAFETY Act protection, if the DHS Secretary determines that the incident —

1. is unlawful or otherwise exceeds authorized access authority;
2. 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;
3. gains access to an information system or a network of information systems resulting in—
    - misappropriation or theft of data, assets, information, or intellectual property;
    - corruption of data, assets, information, or intellectual property;
    - operational disruption; or
    - an adverse effect on such system or network, or the data, assets, information, or intellectual property contained therein; and
4. 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, national morale, or Federal, State, local, or tribal government functions.

As a practical matter, the amendment would allow for Designation and Certification of some cybersecurity products, procedures, and services (including a firm's internal cybersecurity procedures) that may not meet the current definition of "anti-terrorism technology." The bill also would provide SAFETY Act protection in the event of a "qualifying cyber incident," even if that incident does not meet all of the requirements for an "act of terrorism."

Cybersecurity providers should keep an eye on the NCCIP Act. Although it is too early to predict when or in what form the bill may pass, it enjoys bipartisan support and already has garnered praise from stakeholders as diverse as the Secretary of Homeland Security and the American Civil Liberties Union. Although a cybersecurity provider's technology already may be eligible for SAFETY Act coverage under the existing

statute, the NCCIP Act addresses cybersecurity head-on and, if passed either as part of NCCIP or through other legislative vehicles, could make SAFETY Act Designation and Certification even more attractive.

CONTACT US

Kevin P. Mullen, Partner, Jenner & Block

Phone: 202 639-6024 Email: kmullen@jenner.com Download V-Card

Practice Groups: Government Contracts

Mary Ellen Callahan, Partner, Jenner & Block

Phone: 202 639-6064 Email: mecallahan@jenner.com Download V-Card

Practices: Privacy and Information Governance

James A. Tucker, Associate, Jenner & Block

Phone: 202 637-6335 Email: jtucker@jenner.com Download V-Card

Practice Groups: Government Contracts