VENABLE LLP

white paper

APRIL 2014

The SAFETY Act:

Providing Critical Liability Protections for Cyber and Physical Security Efforts

VENABLE LLP ON CYBERSECURITY LAW

VENABLE LLP

white paper

APRIL 2014

AUTHORS

Dismas N. Locaria
dlocaria@Venable.com
202.344.8013

Brian M. Zimmet
bmzimmet@Venable.com
202.344.4510

Jason R. Wool
jrwool@Venable.com
202.344.4511

The SAFETY Act: Providing Critical Liability Protections for Cyber and Physical Security Efforts

VENABLE LLP ON CYBERSECURITY LAW

Since September 11, 2001, Americans have been keenly aware of the need to better protect both the people and assets of the United States from those who may be intent on doing us harm. We have seen, and largely accepted, increased physical security measures at airports, government facilities, and even sporting event venues. Requirements that once would have seemed a gross invasion of privacy are now commonplace. Some of these requirements were federally mandated; however, because the private sector owns and operates the vast majority of critical infrastructure, the government has been reluctant (or perhaps unable) to impose sweeping security measures across all swaths of life. Nevertheless, despite the cost of some of these measures, we have seen the private sector increase physical security efforts in an effort to better protect the public and manage the risk of liability that could arise from an attack. In some instances, these measures were also implemented to obtain a little-known government "carrot," namely liability protection under a federal statute referred to as the SAFETY Act (or "Act").

We have been recently bombarded with both fact and fiction about the vulnerabilities of our critical infrastructure to cyber intrusion and attack. Some in Congress have sought to adopt comprehensive cybersecurity regulation, but legislative efforts to adopt such regulation have fallen short. In lieu of mandatory regulation, the federal government has sought to encourage owners and operators of critical infrastructure to adopt baseline cybersecurity measures to protect their assets, primarily through the adoption of a new Cybersecurity Framework by the National Institute of Standards and Technology ("NIST"). In its promotion of the NIST Cybersecurity Framework, the government has sought to identify incentives for owners and operators of critical infrastructure to adopt the framework. The SAFETY Act is one of the few tools in the government's toolbox that can provide concrete, achievable benefits for owners and operators of critical infrastructure. In this context, the SAFETY Act may also serve not only to incentivize the improvement of an organization's

cybersecurity, thereby better protecting its assets, but may also benefit the organization at-large, in non-terror contexts.

The SAFETY Act

In the wake of 9/11, Congress passed the Homeland Security Act of 2002 with a little known section called the "Support Anti-Terrorism by Fostering Effective Technologies Act of 2002," or the "SAFETY Act."[1] The purpose of the SAFETY Act was to encourage the development and deployment of anti-terrorism products and services (collectively referred to by the statute and herein as "technologies") by granting various risk management protections.

The SAFETY Act, when enacted, held tremendous promise for protecting sellers of new, as well as established, technologies that were needed to combat terrorism and remove impediments to bringing such technologies to and/or maintaining their place in the market. It did so by establishing two levels of protection from third-party liability – Designation and Certification – that may arise from injury, loss of life, or damage to property or businesses arising out of an act of terrorism where the technology was deployed in defense against, response to or recovery from such an act.

Importantly, in the final rule, the Department of Homeland Security ("DHS") recognized that to encourage industry to make new technologies would likely mean that some would require additional development, testing and evaluation before being available for deployment.[2] As a result the final regulation implements a process whereby technologies in development may be afforded SAFETY Act Designation.[3] This type of Designation is referred to as Developmental Testing and Evaluation ("DT&E") Designation. This is particularly significant to potential sellers of technologies that may be reluctant to enter the marketplace, or cannot find affordable insurance, for fear of massive liability. This process sees to it that promising technologies are not killed at the drawing board due to the enormity of liability arising from acts they are designed to prevent.

The Benefits of the SAFETY Act

The SAFETY Act offers substantial protections for sellers of technologies that receive Designation, or the higher-tiered protection, Certification. Designation (including DT&E Designation) most notably caps third-party liability at an approved level of insurance. The Act, however, also includes a myriad of additional risk management benefits along with Designation, such as exclusive jurisdiction in federal court for suits against sellers of a technology arising from acts of terrorism; a bar against punitive damages and prejudgment interest; a limitation on non-economic damages; and liability only in proportion to the responsibility of the seller.

The second level of protection – Certification – confers all of the benefits of Designation as well as the marked addition of potential immunization from liability via the Government Contractor Defense.[4] The assertion of this defense, however, can be rebutted by proving with clear and convincing evidence that fraud or willful misconduct occurred by the seller in submitting

information to DHS. Certified technologies are also deemed "Approved Products for Homeland Security" by DHS.

Designation and Certification protections are awarded in five-year increments, which can be renewed in increments of five years thereafter. DT&E Designation limits the term of protection to 36 months (with no continuing survivorship for the life of the technology), and is terminable at will by DHS.

Perhaps the greatest benefit of either Designation or Certification, however, is that the Act itself provides that the only proper party defendant to a lawsuit arising out of an act of terrorism is the seller. Thus, customers, clients, subcontractors and vendors that either consume the technology or support the seller in deploying the technology are immune from liability. As one can imagine, providing customers and potential customers with the benefit of immunizing them from the potentially ruinous cost of terrorism liability is a tremendous market differentiator. Importantly, however, one does not have to provide the covered Technology to consumers to be considered a seller. Under the Act, an entity can provide a product or service to itself and still obtain Designation or Certification. In instances such as these, the entity would be a seller to itself.

An Act of Terrorism

The protections of the SAFETY Act are triggered by an "act of terrorism."[5] By statute, an "act of terrorism" is an act, determined by the Secretary of DHS, that:

i. [I]s unlawful;

ii. [C]auses 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

iii. [U]ses 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]

Importantly, the final rule to the SAFETY Act expands on the definition of "harm" to include "financial harm," either by nature or degree. This expansion of "harm" potentially broadens the applicability of the Act considerably by removing any need for physical damage.

Obtaining SAFETY Act Protections

SAFETY Act protections are sought through an application process. Designation must first be achieved to receive Certification, although applicants may seek both protections simultaneously as part of the same application submission. To receive Designation, applicants must demonstrate that a proposed technology meets various criteria, including:

- That the technology has utility and is effective;
- That the seller of the proposed technology has large or unquantifiable potential third-party liability risk exposure;
- That it is likely that without the SAFETY Act's protections, the liability associated with the technology would prevent or curtail the proposed technology's deployment;
- That there be a substantial potential risk exposure to the public should the technology not be deployed; and
- Any other factors DHS deems relevant to the security of the United States.

For Certification, applicants must satisfy all of the criteria of Designation, as well as provide information evidencing that the technology can meet three additional criteria, that the technology: 1) performs as intended; 2) conforms to specifications; and 3) is safe for use.

Ten Years and Counting

The SAFETY Act had a slow start following its inception in late 2002 as DHS established its Office of SAFETY Act Implementation ("OSAI") and finalized its internal procedures and operating policies. Following the statute's enactment, a proposed rule was issued in July 2003,[7] followed by an interim rule in October 2003.[8] Also in October 2003, DHS issued the first iteration of the SAFETY Act Application Kit. However, DHS took almost two years to issue a final regulation and revised Application Kit.[9]

The processing of applications for the SAFETY Act's protections was initially slow as well – from October 2003, when the initial SAFETY Act Application Kit was first published, until June 18, 2004 – a period of eight months – just three technologies received Certification status. It took another eight months to double that number to six Designations and Certifications. Today, while over 900 technologies have received SAFETY Act protections, this amounts to less than 100 per year. Thus, while the SAFETY Act holds tremendous benefits for corporations of all kinds, it remains something of a secret.

The SAFETY Act Today

While the event that led to the creation of the SAFETY Act was an act of physical terror, there is no question that cyber-attacks can also have enormously destructive effects, especially in the context of critical infrastructure. Moreover, current and former officials of the FBI and DHS, as well as numerous members of Congress, agree that cyber-terrorism is a significant security concern.

The potential liability from a successful cyber-terrorist attack is substantial. Disruption to a company's operations alone can result in lost business, negative customer reaction, financial harm, government investigations, contract breaches, shareholder lawsuits, and more. In some instances, a cyber-attack could also

result in physical destruction and harm, which could expose the victim to tort liability. For owners and operators of information technology systems, the ramifications of a cyber-attack can extend to large swaths of third parties (think of a major power outage, lack of telecommunications, or broken ATMs).

Owners of such systems should explore the possibility of seeking SAFETY Act coverage as a way to complement cybersecurity insurance policies and other risk-mitigation tools. Such consideration would include:

- Reviewing your cyber-attack risks and potential liabilities to determine whether obtaining SAFETY Act coverage would benefit your business;

- Examining whether any of your security systems, business continuity, physical and cyber-related defense/mitigation plans, or other products and services qualify for coverage under the SAFETY Act;

- To the extent possible, procuring SAFETY Act-approved products and services to take advantage of the liability flow downs, or working with your business partners to encourage them to obtain SAFETY Act coverage; and

- Including SAFETY Act requirements in all of your security product and service procurements.

Any entity that sells cybersecurity solutions to owners of information technology systems should consider applying for SAFETY Act protection for such products or services. First, such sellers should review or seek advice on whether your products and services are likely to qualify for coverage under the SAFETY Act. If your products or services do not currently qualify for coverage, keep the SAFETY Act in mind, because it may be a significant way to differentiate your future products and services from those of your competitors.

Put simply, the SAFETY Act represents a win/win for both the government and private industry. By taking advantage of the program, private industry can help protect the country from cyber-attack while also lowering insurance costs and mitigating liability risks. Even in the absence of a terrorist attack, SAFETY Act coverage serves as a stamp of approval from the federal government that a Technology – which, again, includes security services that a company provides to itself – is an effective tool for preventing, detecting, or responding to cyber-attacks. Coverage is therefore not only a market differentiator, but also significant evidence of commercial reasonableness in legal proceedings not associated with an act of terrorism. As a result, any company facing cyber-risk should carefully consider how a SAFETY Act Designation or Certification could protect its interests and elevate its standing in the marketplace.

Venable office locations

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21201
t 410.244.7400
f 410.244.7742

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE
AMERICAS
25TH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

ROCKVILLE, MD
ONE CHURCH STREET
FIFTH FLOOR
ROCKVILLE, MD 20850
t 301.217.5600
f 301.217.5617

SAN FRANCISCO, CA
SPEAR TOWER, 40TH FLOOR
ONE MARKET PLAZA
1 MARKET STREET
SAN FRANCISCO, CA 94105
t 415.653.3750
f 415.653.3755

TOWSON, MD
210 W. PENNSYLVANIA AVE.
SUITE 500
TOWSON, MD 21204
t 410.494.6200
f 410.821.0147

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949

WASHINGTON, DC
575 7TH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

WILMINGTON, DE
1201 NORTH MARKET STREET
SUITE 1400
WILMINGTON, DE 19801
t 302.298.3535
f 302.298.3550

© VENABLE 2014

[1] Homeland Security Act of 2002, Pub. L. No. 107-246, §§ 861-865, 116 Stat. 2135 (2002) (Title VII, Subtitle G) (codified at 6 U.S.C. §§ 441-444). The Department of Homeland Security issued the final rule, implementing the SAFETY Act on June 8, 2006 (71 Fed. Reg. 33,147 *et seq.* (June 8, 2006, Final Rule), which codified the Act's implementing regulations at 6 C.F.R. Part 25.
[2] 71 Fed. Reg. 33,147, 33,156 (June 8, 2006, Final Rule).
[3] 6 C.F.R. § 25.4(f).
[4] The Government Contractor Defense arose out of a landmark case, *Boyle v. United Technologies Corporation*, 487 U.S. 500 (1988), whereby the U.S. Supreme Court determined that a defense contractor manufacturing a military product in accordance with precise government specifications may not be held liable for claims resulting from use of the manufactured product. With respect to the SAFETY Act, DHS limits the defense to that which existed on the day of the SAFETY Act's enactment (November 25, 2002), meaning that future judicial developments in the government contractor defense would not apply. Hence, the considerable body of law growing out of *Boyle*, and its progeny up to the enactment of the SAFETY Act (November 25, 2002), are essentially frozen in time.
[5] 6 U.S.C. § 444(2).
[6] *Id.*
[7] 68 Fed. Reg. 41,420 *et seq.* (July 11, 2003, Proposed Rule).
[8] 68 Fed. Reg. 59,684 *et seq.* (October 16, 2003, Interim Rule).
[9] 71 Fed. Reg. 33,147 *et seq.* (June 8, 2006, Final Rule).