Today's
GENERAL COUNSEL

SAFETY Act Decreases Private Sector Risk and Liability

By Joseph I. Lieberman, Clarine Nardi Riddle and Mark J. Robertson

Litigation stemming from the October 2017 Las Vegas mass shooting incident has brought renewed attention to the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, the 2002 federal legislation that was intended to encourage the development and deployment of technologies to counter terrorist threats and to make organizations more resilient against a terror attack. However, recent media coverage has not adequately described the SAFETY Act or explained the important role it plays in the United States' overall homeland security efforts.

In-house counsel and risk managers should consider securing SAFETY Act approval (which provides for protection against civil liability for companies deploying approved anti-terrorism technology) in the face of evolving terrorist threats, particularly cyber threats. This is the case especially

among critical infrastructure owners and operators, including energy, industrial manufacturing, real estate, healthcare and financial services firms. Given the complexity of the SAFETY Act and confidentiality concerns related to applying for SAFETY Act protection, companies should consult a practitioner with experience in SAFETY Act applications.

The following provides an overview of the SAFETY Act and serves as a reference to those considering whether to seek SAFETY Act approval.

Origins of the Safety Act

The SAFETY Act of 2002 was passed by Congress as part of the Homeland Security Act, the legislation that created the Department of Homeland Security (DHS). The SAFETY Act removes a major obstacle for companies to develop and deploy technologies helpful to homeland security: the potentially catastrophic liability that could result if their technology becomes the subject of litigation following a terror attack. A firm with DHS approval under the SAFETY Act would have protections against civil liability if, in the event of a terror attack, its product or service failed to perform as intended.

A SAFETY Act approval of technology provides important liability protections not only for a company manufacturing and selling the approved technology but also for a company that purchases and deploys the approved technology if it fails to perform as intended following a terror attack. DHS has to date issued over 1,000 SAFETY Act approvals, encouraging the deployment of security technologies that protect Americans and make United States institutions more resilient. There is evidence that the SAFETY Act's risk management and litigation management provisions are encouraging greater investment in innovative technologies that increase our collective homeland security.

Commercially, SAFETY Act approval may aid in marketing a security product or service by indicating a substantial level of government review and assessment of a technology's safety and effectiveness. Changes to the Federal Acquisition Regulations (FAR) integrate the SAFETY Act into the Federal acquisition process, effectively extending advantages to SAFETY Act-approved technologies. Entities that procure and utilize homeland security technologies are increasingly insisting that technology providers obtain SAFETY Act coverage. Approval under the SAFETY Act thus provides a relatively inexpensive insurance policy against catastrophic risk.

Protections

The SAFETY Act offers liability protections up and down the supply chain, in both government and private markets. Users and suppliers of anti-terrorism technologies are covered by SAFETY Act protections if the technology they are fielding has been "Designated" or "Certified" by DHS.

Before the SAFETY Act — excluding government indemnification for unusually hazardous risks pursuant to Public Law 85-804 — the majority of technologies could access liability protections only when sold to the United States military and when their designers complied with strict government requirements. These protections led to incentives for the defense industry to meet the Department of Defense's (DOD's) technological requirements. After September 11, 2001, Congress recognized that similar incentives did not exist for technologies that could protect United States civilian populations. Technologies designed for DOD use could not be brought to the civilian market without losing critical liability protections.

The homeland security community has recognized that the government alone cannot fully defend the nation from a terror attack. The role of the private sector in homeland security is crucial, especially in light of the fact that as much as 85 percent of the nation's critical infrastructure is privately held. The SAFETY Act allows the movement of existing defense and homeland security technologies from federal agency use to the broader civilian marketplace — transportation hubs, stadiums, office towers, shopping malls, and manufacturing and chemical facilities — that have immediate security needs. SAFETY Act protections are available to both newly developed and existing technologies, regardless of whether they have been specifically developed for anti-terrorist purposes.

Under the SAFETY Act, the "Seller" of an "anti-terrorism technology" (which includes any person, firm, or other entity that sells or otherwise provides anti-terrorism or homeland security-related technology to any customer) may apply to DHS for protection from civil liability alleged after a terrorist attack. SAFETY Act approval has been awarded to an array of technologies ranging from video surveillance systems to explosive detection technology, from software and cyber security applications to infrastructure protection and physical security programs.

Protection is available to virtually any product or service that can effectively deter, mitigate or help respond to a terrorist attack. The definition of anti-terrorism technology for SAFETY Act purposes is expansive and includes "any product, equipment, service (including support services), device, or technology (including information technology) or any combination of the foregoing." Furthermore, the definition specifies that a variety of services relevant to homeland security may be deemed a technology under the SAFETY Act.

The SAFETY Act provides two potential classes of protection for approved anti-terrorism technologies. First, products or services may be designated as a Qualified Anti-Terrorism Technology (QATT). In its evaluation, DHS considers a number

of factors to determine whether the technology is safe and effective at countering terrorist threats.

DHS has broad discretion in determining whether to designate a particular technology as a QATT. The DHS Under Secretary for Science & Technology has discretion to give greater weight to certain factors over others. Upon such designation, the seller and all users of the approved QATT enjoy the benefits of the system of risk management and litigation management established by the SAFETY Act. Together, the risk and litigation management provisions provide the following protections:

(1) A limitation on the liability of sellers of QATTs to a pre-determined amount;
(2) A prohibition on joint and several liability such that sellers can only be liable for a percentage of non-economic damages proportionate to their responsibility;
(3) A complete bar on punitive damages and prejudgment interest;
(4) The reduction of a plaintiff's recovery by the amount of collateral source compensation, such as insurance benefits or government benefits the plaintiff receives; and
(5) Exclusive jurisdiction in federal court for suits against the sellers of "Qualified Anti-Terrorism Technologies."

Approval under the SAFETY Act provides a relatively inexpensive insurance policy against catastrophic risk.

The second class of protection is SAFETY Act "Certification," which entails a stricter level of review by DHS, provides all the benefits of QATT designation and adds one layer of liability protection. A "Seller" of a certified QATT is entitled to assert the Government Contractor Defense (GCD) in litigation arising from an act of terrorism involving SAFETY Act Certified technology. SAFETY Act certification of a QATT creates the rebuttable presumption that the GCD applies and can only be overcome if a plaintiff proves that the seller acted fraudulently or with willful misconduct in applying for SAFETY Act protections.

The GCD, which has been a judicial construct under the Supreme Court's Boyle line of cases, immunizes from liability contractors who supply goods to the government, provided they have met certain conditions. It has been relied on primarily by military contractors in cases involving allegations of defective military equipment. Certification under the SAFETY Act entitles the seller to assert the affirmative GCD, thus serving as important protection against potential liability.

Designation v. Certification

The SAFETY Act mandates that the stricter review culminating in a technology's certification must be "comprehensive," and must allow the Secretary [of Homeland Security] to determine "whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended."

The SAFETY Act codifies the GCD, and DHS has taken a firm stance as to the application of the GCD in the SAFETY Act context: "The Act does not permit judicial review of the Secretary's exercise of discretion in this context. When the Secretary determines that a Certification is appropriate, that decision creates a rebuttable presumption that the Government Contractor Defense applies. This presumption may only be rebutted by clear and convincing evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Department during the course of the consideration of such Technology."

In the SAFETY Act final rule, DHS offered its interpretation of how the courts would apply SAFETY Act protections in the event they are tested following a terrorist attack. DHS stated:

> *The best reading of [the SAFETY Act], and the reading the Department has adopted, is that (1) Only one cause of action exists for loss of property, personal injury, or death for performance or nonperformance of the Seller's QATT in relation to an Act of Terrorism, (2) Such cause of action may be brought only against the Seller of the QATT and may not be brought against the buyers, the buyers' contractors, downstream users of the QATT, the Seller's suppliers or contractors, or any other person or entity, and (3) Such cause of action must be brought in federal court.*

Importantly, the SAFETY Act is the first time that GCD protections have been expanded to non-military situations, and applies even where the government is not a party to any transaction involving the technology. The protections are available not only to federal government contractors but also to those who sell to state, local and tribal governments, as well as to the private sector.

To increase flexibility, DHS now also provides for Developmental Testing and Evaluation Designations (DT&E) for companies with unproven technologies. Their incorporation makes it possible to grant SAFETY Act protections to anti-terrorism technologies that are still in the development process, so that, for example, promising technologies that have yet to be field tested can qualify for the SAFETY Act's risk management and liability protections.

Following the SAFETY Act final

rule, the government amended the FAR to align SAFETY Act applications and the government procurement process. The FAR now require agencies across the federal government, not only in the homeland security arena, to determine whether the technology or service they are procuring may be eligible for SAFETY Act coverage.

Application Process

SAFETY Act applications require the submission of detailed data, some of which may be deemed proprietary if it includes confidential technical or business information. Such data can be extremely sensitive, both for commercial and security purposes. DHS has stated that information submitted, whether ultimately a part of a successful application or not, will be kept confidential to the fullest extent of the law.

Given these confidentiality concerns, applicants should consult a practitioner with experience in SAFETY Act applications, before applying for SAFETY Act protection. DHS information requests can be expansive, and applicants may confront various obstacles on the road to receiving designation or certification. Experienced counsel can help manage the exchange of information with DHS and limit potentially costly and time-consuming delays.

The SAFETY Act is a valuable tool for litigation and risk management for companies developing and fielding security technologies. By providing companies with the assurance they need to develop and deploy cost-effective homeland security technologies, the SAFETY Act has expanded the number of counter-terrorism technologies available. The SAFETY Act furthers private interests to the benefit of the common good by enhancing our nation's security and resilience against a terror attack. In-house and outside industry counsel can support these goals by promoting the use and understanding of the SAFETY Act. ■

Senator Joseph I. Lieberman, Senior Counsel at Kasowitz Benson Torres LLP, represents clients in independent and internal investigations and advises them on a wide range of public policy, strategic and regulatory issues. During his tenure as United States Senator, he helped shape legislation concerning national and homeland security, and served as Chairman of the Homeland Security and Government Affairs Committee.
jlieberman@kasowitz.com

The Hon. Clarine Nardi Riddle, Counsel at Kasowitz Benson Torres LLP and Chair of the firm's Government Affairs and Strategic Counsel Practice Group, provides legal, strategic and policy advice to clients on matters where law, business and public policy intersect. Formerly Attorney General of Connecticut, she also worked on homeland security policy issues as Senator Lieberman's Chief of Staff.
cnriddle@kasowitz.com

Mark J. Robertson, Special Counsel at Kasowitz Benson Torres LLP, represents clients in an array of government regulatory, enforcement and public policy matters, and advises clients with interests arising from national security and homeland security efforts. He played a central role in the development of the regulations implementing the SAFETY Act and served in several senior positions focusing on homeland security technology within the Department of Homeland Security.
mrobertson@kasowitz.com

KASOWITZ
BENSON TORRES