Protecting Your Investment: SAFETY Act Protection as a Risk-Management Tool

By Lorelie S. Masters, Kevin W. Jones and Charlotte Leszinske

After years of researching and developing a security product, your company's management is understandably concerned about protecting its investment. The SAFETY Act is a powerful risk management tool that helps organizations protect themselves from exposure to liability arising from the use of their technology: products, services, and systems. Recognition by the federal government under the SAFETY Act that a technology is safe and effective can also provide companies additional value, including reputational benefits and potentially lower insurance premiums. This article provides an overview of the SAFETY Act and how your company can take to obtain this protection.

To help navigate what can be a complex process and obtain the most favorable terms for your technology, your company should work with counsel experienced with the process of applying for and obtaining SAFETY Act protection. Importantly, working with counsel may also cloak in privilege sensitive information regarding the technology and improvements to it.

WHAT IS THE SAFETY ACT?

The Supporting Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act was passed in 2002. The purpose of the SAFETY Act is to encourage the development of technology that prevents or reduces harm caused by acts of terrorism causing mass injury or loss. SAFETY Act-certified or designated technologies enjoy certain protections from legal liability.

The SAFETY Act created a program to promote the development of "qualified anti-terrorism technologies" meant to safeguard against "acts of terrorism." Both of these terms are defined broadly in the relevant regulations. "Technology," for example, can be a product, service, or system. The Department of Homeland Security, through its Office of SAFETY Act Implementation (OSAI), determines whether technology meets the SAFETY Act's requirements of a "qualified anti-terrorism technology." OSAI will expect that designated technologies show "proven effectiveness (with confidence of repeatability)" and certified technologies demonstrate a higher standard of "consistently proven effectiveness (with high confidence of enduring effectiveness)." An "act of terrorism" includes unlawful acts that cause harm in the U.S. resulting in mass injury or loss.

Both cyber and physical attacks may constitute an "act of terrorism," though the Secretary of Homeland Security must declare an attack to be an "act of terrorism" in order for statutory protections to attach. Nevertheless, even if an act of terrorism is not formally declared, a SAFETY Act certification can still prove valuable in the event of an incident.

Some recent recipients of SAFETY Act protection are:

- *Chicago Park District and ASM Global Convention Center Management, LLC*: Designation for system for stadium security management to deter and defend against terrorist attacks at sports stadiums;
- *AeroDefense*: Designation for an alert system to detect drones in protected airspace;
- *Delta Scientific Corporation*: Certification for vehicle barriers;
- *ASIS International, Inc.*: Designation for a certification and re-certification program for security professionals based on examinations; and
- *American Petroleum Institute*: Certification for its standard providing requirements and guidance for managing cyber risk for the oil and natural gas pipeline industry.

The authors, attorneys with Hunton Andrews Kurth LLP, may be contacted at lmasters@hunton.com, kjones@hunton.com and cleszinske@hunton.com, respectively.

Designated technologies will have their third-party liability capped to a pre-determined amount equal to required insurance coverage, while also receiving other benefits such as exclusive federal jurisdiction and prohibition of punitive damages. Certified technologies are immune from such claims under the government contractor defense.

Even in the absence of a declared act of terrorism, SAFETY Act protection provides meaningful reputational and risk-management benefits. Technologies awarded SAFETY Act protection can be placed on OSAI's Approved Technologies list, and the technology may be marketed using a DHS seal. SAFETY Act protection is a mark of credibility and effectiveness in the security technology marketplace. It signifies that a company's products or services have been rigorously evaluated by DHS for their ability to mitigate terrorism risks. This "stamp of approval" can differentiate a company from competitors and increase its attractiveness to potential customers, partners, and government agencies seeking reliable security solutions.

For companies involved in supplying security technologies to government agencies, obtaining SAFETY Act protections can streamline the procurement process. Government entities may give preference to SAFETY Act-designated products and services due to the reduced liability and proven efficacy, expediting contract awards and enhancing business opportunities. Indeed, SAFETY Act recognition is often required for both public and private security-related contracts.

SAFETY Act recognition can also mitigate real-world liabilities outside of an act of terrorism. It can support assertions by the company that the technology satisfied standards of care, even in litigation not arising from a declared act of terrorism. It may also help the company reduce its insurance premiums, particularly for general liability, cyber, and D&O policies. Policyholders who demonstrate that they have taken proactive steps to reduce liability by obtaining review and certification of their technology may benefit from lower premiums and greater coverage.

HOW ARE SAFETY ACT PROTECTIONS OBTAINED?

The SAFETY Act application process has several steps. First, your management team should assess whether DHS is likely to consider your technology a good candidate for SAFETY Act certification or designation. In particular, before seeking SAFETY Act recognition, your team should prepare to explain:

(1) The exact specifications of the technology and economics of its production;

(2) How the technology will be used by consumers;

(3) Potential risks resulting from those uses; and

(4) How the technology fits into broader corporate strategy.

The company should also determine whether it maintains documentation to effectively describe the technology, particularly where it is offering a service. In addition, a company should identify documentation substantiating the effectiveness of the technology, preferably going back at least two to three years. Working with counsel to engage subject-matter experts and develop a central repository of information will help facilitate this process and cloak sensitive internal evaluations in privilege.

The next steps are to register with OSAI and complete a "pre-application." The pre-application is shorter than the full application and establishes contact with OSAI. Once the pre-application is submitted, applicants can request a consultation with OSAI, which will provide detailed feedback on the technology and guidance on where to focus efforts for the full application. OSAI will also provide feedback on the technology's likelihood of approval. This can save your company time and money on the full application and establish a good working relationship with OSAI. Before moving forward, your company should consult with counsel and key team members to determine whether implementing OSAI's suggestions are feasible and make business sense.

The next step is to complete a full application. Experienced advisors can help prepare what is often a complex and highly technical application in a manner that will describe the technology effectively to OSAI. Additional evidence of the technology or its effectiveness may be needed. For example, to obtain certification, applicants must complete safety and hazard analyses. Also at this time, your company must submit proof of its general liability insurance

program, which will factor into OSAI's determination of the liability cap for the technology. It is therefore important to work with your risk management team and insurers in advance to identify and address any gaps in coverage before applying for protection.

Once the application is complete, OSAI strives to complete its evaluation of the technology in 120 days. If OSAI determines that the technology satisfies SAFETY Act requirements, it will issue a decision letter. The letter will likely contain additional conditions (contours) that must be satisfied before the technology is put into use. Once those conditions are satisfied (in connection with advice of counsel), the technology will be protected under the SAFETY Act. Additionally, the company can use the SAFETY Act mark(s) in its marketing materials for the technology.

WHAT HAPPENS AFTER RECEIVING SAFETY ACT PROTECTIONS?

While designation or certification can last as long as eight years, OSAI normally limits the term to five years. Renewal is not automatic and requires submitting a renewal application, but doing so is less resource-intensive than the initial application. Applications for renewal should be submitted at least six months in advance of expiration.

During the period of designation or certification, your company may use the SAFETY Act mark in public relations and marketing materials and various stakeholder communications. You should also make your insurers aware that your technology has achieved protection, which may impact their underwriting for your policies and may help obtain reduced premiums or expanded coverage. Finally, it is important to communicate any changes to the technology to OSAI, which may require your company to submit additional documentation about those changes.

CONCLUSION

The SAFETY Act offers substantial advantages to companies that develop and deploy effective security technologies. From liability protection and enhanced marketability to streamlined procurement processes, improved investor confidence, engagement with regulators, and potentially lower insurance premiums, SAFETY Act protections provide valuable benefits. As threats evolve, obtaining SAFETY Act protections remains a prudent strategy for companies committed to safeguarding their assets, operations, and stakeholders against terrorism and other malicious activities.