

In A Dangerous World Energy Cos. Should Look To SAFETY

Law360, New York (September 10, 2014, 10:35 AM ET) --

As we approach the anniversary of the horrific attacks of Sept. 11, 2001, news reports about the threat of terrorism on U.S. soil are again in the headlines. There is no question that an act of terrorism targeting our energy sector could have devastating effects on both industry and national security. A terrorist attack on a refinery, pipeline or substation could result in significant destruction of property, loss of life, long-term injuries and disrupted operations for the targeted facility and its customers. In addition, the facility owners and operators could be forced to contend with a flood of third-party liability claims, the magnitude of which is difficult, if not impossible, to predict.

Investments in security, such as regular threat and vulnerability assessments, access control measures, video and electronic surveillance, security personnel, visitor and delivery screening, cybersecurity measures, background checks, training, emergency drills and contingency planning, help mitigate the risk of an act of terrorism occurring at a particular facility. Although a substantial commitment of resources and a well-calibrated insurance portfolio are important tools for risk mitigation in a post-9/11 world, businesses of all sizes, including many in the energy sector, too often overlook the Support Anti-terrorism by Fostering Effective Technologies Act as an additional layer of protection against the persistent threat of terrorism.



Scott A. Freling

SAFETY Act Protection

Enacted in 2002, the SAFETY Act is designed to promote the creation and use of anti-terrorism technologies by, among other things, capping — and, in some cases, eliminating — liability for providers and users of such technologies. Specifically, the SAFETY Act caps third-party liability arising from an act of terrorism when an approved anti-terrorism technology has been deployed in defense or response. The liability cap is set by the U.S. Department of Homeland Security in the form of a predetermined amount of terrorism insurance that must be maintained by the entity holding the SAFETY Act protection. In other words, damages from tort claims against a SAFETY Act-protected technology following an act of terrorism may not exceed the required insurance coverage. The SAFETY Act also bars claims for punitive damages, precludes state court litigation and prohibits pain and suffering claims without proof of physical harm. And where an applicant can demonstrate that its anti-terrorism technology performs as

intended and is safe for its intended use, the SAFETY Act can offer immunity from liability for certain claims.

Any technology, or system of technologies, that detects, prevents or deters acts of terrorism may be eligible for SAFETY Act coverage. The SAFETY Act's protections have been granted to a wide range of products and services, including the collection of security measures protecting several high-profile facilities throughout the country. For example, the operators of LaGuardia Airport and Cincinnati/Northern Kentucky Airport have received SAFETY Act protection for their security operations. The operators of Yankee Stadium, Citi Field and MetLife Stadium have likewise obtained SAFETY Act protection for the protective measures at their venues. Other facilities with SAFETY Act protection include the New York Stock Exchange, World Financial Center in New York, Willis Tower in Chicago (formerly known as the Sears Tower), and George W. Bush Presidential Center in Dallas.

Notably absent from the list of facilities with SAFETY Act protection are any of the critical infrastructure components of our domestic energy sector. This absence is particularly striking given that the protective measures already in place at many energy production or distribution facilities in the U.S. are a natural fit for SAFETY Act protection. Yet, without completing the formal application and review process administered by the DHS, operators of energy facilities risk leaving themselves exposed to nearly limitless third-party liability claims in the event of a terrorist attack. Given the stakes, facility operators in the energy sector should take a cue from their forward-looking counterparts in the transportation, real estate and entertainment industries and examine whether the SAFETY Act might offer an additional layer of financial protection.

Applying for Protection

Applications for SAFETY Act protection are submitted to the Office of SAFETY Act Implementation at DHS through its website. OSAI, which is responsible for coordinating a technical review of each application, has promulgated regulations to administer the SAFETY Act program. It has also published helpful commentary in the Federal Register as well as an Application Kit to guide prospective applicants in their preparation of an application.

An application must, among other things, adequately describe the technology or technologies at issue and demonstrate its utility and effectiveness with supporting documentation, data and analysis. The technology description defines the legal boundaries of an applicant's approved SAFETY Act protection. It is one of the most important, and often the most difficult, parts of the application process. This is particularly true for a complex system of technologies, like the security program deployed to protect a piece of critical infrastructure, as there are many layers of protective measures that must come together to deter, defend against and respond to acts of terror and other manmade threats. Prospective applicants are well-advised to begin the application process with a careful study of the technology or technologies that may be eligible for SAFETY Act protection. This initial analysis is likely to reveal additional areas by which an eventual application may be broadened. At bottom, a more expansive technology description should offer stronger liability protection following an act of terrorism.

The DHS requires an applicant to submit sufficient documentation to show — on paper — the utility and effectiveness of the technology or technologies at issue. Thankfully, most SAFETY Act applicants cannot point to a past instance where their technology helped thwart an act of terrorism. Recognizing that direct evidence like this is often not available, DHS expects an applicant to think creatively for indicia of utility and effectiveness. There is no set method for demonstrating that a technology works; it will depend in large measure on the nature of the technology. For a facility-based security program, this

might include operational records, such as shift reports and incident logs; after action reports from an actual incident or a drill; internal assessments; third-party reviews; and written testimony.

Conclusion

The process for securing SAFETY Act protection can be detailed and time consuming. It generally requires a substantial commitment of internal resources. But the potential benefit of SAFETY Act protection can be quite valuable, and may well outweigh the cost associated with preparing the application. Facility operators in the energy sector should at a minimum ensure that the SAFETY Act becomes part of the risk mitigation calculus and make an informed decision about whether an application for protection could further safeguard against the terrorist threat.

—By Scott A. Freling, Covington & Burling LLP

Scott Freling is an associate in Covington & Burling's Washington, D.C., office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2014, Portfolio Media, Inc.