

SECTION III

Critical Infrastructure

The SAFETY Act— A Practitioner’s Guide to the Homeland Security Technology Catalyst

by Mark J. Robertson and Jeffrey Kaliei

The following chapter aims to familiarize counsel with the liability protections available under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act, passed by Congress as a part of the Homeland Security Act of 2002). The chapter addresses the background of the SAFETY Act, provides a detailed discussion of the system of risk and litigation management provided under the act, and summarizes the responsibilities of companies offering SAFETY Act–approved technologies. The chapter also aims to put the SAFETY Act in context with other liability protection devices and addresses practicalities involved in obtaining SAFETY Act approvals.

The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) was passed by Congress as part of the Homeland Security Act of 2002 (Subtitle G of Title VIII), which created the U.S. Department of Homeland Security (DHS).¹ Congress designed the SAFETY Act to encourage the rapid development and fielding of anti-terror technologies. The SAFETY Act removes a recognized hindrance

1. 6 U.S.C. §§ 441–444

to companies that wish to invest in and deploy technologies helpful in homeland security: the potentially catastrophic liability that could result if their technology were to become the subject of litigation following a terror attack. The SAFETY Act largely eliminates this concern. A firm with DHS approval under the SAFETY Act would have protections against liability if, in the event of a terror attack, its product or service failed to perform as intended. The SAFETY Act provides important liability protections not only for a selling company and its shareholders, but also for those who purchase and deploy protected technologies, and sharply limits the possibility of costly liability for both.

The SAFETY Act is a tool that should be considered by every provider of an anti-terrorism “technology” as that term is expansively defined by the SAFETY Act and its implementing regulations.² Those who procure and utilize homeland security technologies are increasingly insisting that technology providers obtain SAFETY Act coverage. Although delays in promulgating regulatory guidance and a somewhat convoluted initial application process adversely affected early implementation efforts, DHS has since taken action that has engendered greater confidence in, and paved the way for, more robust implementation of the SAFETY Act. DHS has to date granted SAFETY Act coverage to approximately 250 different anti-terrorism technologies. Whatever the history of the SAFETY Act and its implementation, companies today should recognize that the act essentially offers them a relatively inexpensive insurance policy against catastrophic risk. Moreover, the SAFETY Act’s limit of potential liability in itself can allow firms to offer technologies at a more competitive price, and it can free companies to design products that provide at least some meaningful level of protection while shielding them from the specter of overzealous plaintiffs and juries.

There is also a growing sense that SAFETY Act approval is seen in industry as a *de facto* seal of approval affording advantages in marketing a product or service, as it indicates a substantial level of government

2. *See Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act)*, 71 Fed. Reg. 33,147–68 (June 8, 2006); “The term ‘Technology’ means any product, equipment, service (including support services), device, or technology (including information technology) or any combination of the foregoing. Design services, consulting services, engineering services, software development services, software integration services, threat assessments, vulnerability studies, and other analyses relevant to homeland security may be deemed a Technology under this part.” 6 C.F.R. § 25.2.

review and assessment of a technology and its safety and effectiveness. Further, recent changes to the Federal Acquisition Regulations (FAR) integrate the SAFETY Act into the federal acquisition process, effectively extending advantages to SAFETY Act–approved technologies. Some also argue that corporate officers have a duty to their shareholders to seek SAFETY Act liability protection when fielding homeland security technologies. In sum, there are a host of reasons for companies to obtain SAFETY Act protections.

This article aims to familiarize in-house and outside counsel with the protections available under the SAFETY Act, so that they might in turn advise clients in the broader homeland security community. We will discuss the background of the SAFETY Act, then discuss in detail the protections offered and responsibilities of companies that offer SAFETY Act–approved technologies. We will also put the SAFETY Act in context with other liability protection devices, such as the Public Readiness and Emergency Preparedness Act (PREP Act) and the Government Contractor Defense. Finally, we will address practicalities involved in advancing a SAFETY Act application.

THE SAFETY ACT'S PROTECTIONS

The SAFETY Act, it should be emphasized, offers its liability protections well beyond the actual vendors who sell their technologies to the federal government. The benefits of the SAFETY Act's liability protection flow up and down the supply chain, in both government and private markets. Both users and suppliers of anti-terror technologies are covered by SAFETY Act protections if the technology they are fielding has been "Designated" or "Certified" by DHS. Excluding government indemnification for unusually hazardous risks pursuant to P.L. 85-804, before the SAFETY Act was enacted, the great majority of technologies could access liability protections only when they were sold to the U.S. military and when their designers complied with strict government requirements (the Government Contractor Defense is discussed below). These protections, limited as they were, led to incentives for the defense industry to aggressively and creatively work to meet some of the Department of Defense's technological requirements. One could argue that a large part of the American defense industry's success in developing new defense technologies can be traced back to its liability protections, which allowed for greater risk-taking.

After September 11, 2001, Congress recognized that similar incentives did not exist for technologies that could protect civilian populations in the homeland, and the industrial base for those technologies remained small. Even technologies designed for the Department of Defense (DoD) with potential crossover applications could not be brought to the civilian market without losing critical liability protections.

As such, one potential major effect of the SAFETY Act is to allow the movement of existing defense and homeland security technologies from mere federal agency use to the broader civilian homeland security marketplace—to all those transportation hubs, stadiums, office towers, shopping malls, and manufacturing and chemical facilities that have real and immediate security needs. Toward this end, SAFETY Act protections are available to both newly developed and existing technologies, whether they have been specifically developed for anti-terror purposes or not.³ This is no small accomplishment, as the homeland security community has increasingly recognized that the government alone cannot fully defend the nation from a terror attack. The involvement of the private sector is crucial, especially in light of the fact that as much as 85 percent of the nation's critical infrastructure is privately held. Still, after verdicts like the one that held the Port Authority of New York and New Jersey more than two-thirds responsible for the 1993 World Trade Center bombing, many in the security and technologies industries faced a high barrier to entering the civilian homeland security market.⁴

Under the SAFETY Act, the “seller”⁵ of an anti-terror technology may apply to DHS for protection from civil liability following a terrorist attack. To date, SAFETY Act approval has been awarded to technologies ranging from video surveillance systems to explosive detection technol-

3. 6 U.S.C. § 444 allows for SAFETY Act designation of technology that is “designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm” caused by acts of terrorism.

4. *See* *Nash v. Port Auth. of N.Y. & N.J.*, #129074/93, 2008 N.Y. App. Div. LEXIS 374, 2008 N.Y. slip op. 03991 (1st Dept.). Victims of the 1993 World Trade Center bombings sued the Port Authority of New York and New Jersey for damages. A New York appellate panel affirmed the jury verdict that the Port Authority was more than two-thirds responsible for the 1993 terrorist bombing of the World Trade Center.

5. *See* 6 C.F.R. § 25.2. For purposes of the SAFETY Act, the term “seller” means any person, firm, or other entity that sells or otherwise provides Qualified Anti-Terrorism Technology to any customer(s) and to whom or to which (as appropriate) a designation and/or certification has been issued.

ogy, from software and IT applications to radiological detection equipment.⁶ Protection, in short, is available for virtually any product or service that can effectively deter, mitigate, or help respond to a terrorist attack. The definition of technology for purposes of the SAFETY Act and its implementing regulations is expansive and includes “any product, equipment, service (including support services), device, or technology (including information technology) or any combination of the foregoing.”⁷ Further, the regulatory definition specifies that “[d]esign services, consulting services, engineering services, software development services, software integration services, threat assessments, vulnerability studies, and other analyses relevant to homeland security may be deemed a Technology . . .” under the SAFETY Act.⁸

DESIGNATION AS A QUALIFIED ANTI-TERRORISM TECHNOLOGY

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 evaluating whether a technology should be designated as a QATT, DHS must consider the following factors:

1. Prior U.S. government use or demonstrated substantial utility and effectiveness.
2. Availability of the technology for immediate deployment in public and private settings.
3. Existence of extraordinarily large or extraordinarily unquantifiable potential third-party liability risk exposure to the seller or other provider of such anti-terrorism technology.

6. Recently designated technologies include: cargo and vehicle inspection systems, criminal information sharing services, Smarttech Chem system, protective services, rail transportation security services, Sulf-N[®] 26 fertilizer process and product, multi-threat risk analysis and physical perimeter protection system for the federal secure border initiative network program, and explosive trace detection inspection services. A full list of certified technologies is available on the Web site of the Office of SAFETY Act Implementation at www.safetyact.gov.

7. See note 2 above.

8. *Id.*

4. Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under [the SAFETY Act] are extended.
5. Magnitude of risk exposure to the public if such anti-terrorism technology is not deployed.
6. Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.
7. Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.
8. A determination made by federal, state, or local officials that the technology is appropriate for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause.
9. Any other factor that the Under Secretary [of DHS's Science and Technology Directorate] may consider to be relevant to the determination or to the homeland security of the United States.⁹

The SAFETY Act's implementing regulations provide for broad discretion in determining whether to designate a particular technology as a QATT. Further, in conducting his analysis, the DHS Under Secretary for Science and Technology has discretion to give greater weight to certain factors over others, and he may determine that failure to meet one or more of the criteria does not necessary disqualify a technology from being designated as a QATT.¹⁰

Upon designation by DHS, 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 Qualified Anti-Terrorism Technologies to an amount of liability insurance coverage specified for each Qualified Anti-Terrorism Technology, pro-

9. *See* 6 C.F.R. § 25.4(b)(1).

10. *See* 6 C.F.R. § 25.3; all of the responsibilities, powers, and functions of the Secretary of Homeland Security under the SAFETY Act, except the authority to declare that an act is an act of terrorism for purposes of the SAFETY Act have been delegated to the DHS Under Secretary for Science & Technology.

vided that sellers cannot be required to obtain any more liability insurance coverage than is reasonably available “at prices and terms that will not unreasonably distort the sales price” of the technology;¹¹

2. A prohibition on joint and several liability such that sellers can only be liable for the percentage of noneconomic damages that is proportionate to their responsibility;¹²
3. A complete bar on punitive damages and prejudgment interest;¹³
4. The reduction of a plaintiff’s recovery by the amount of collateral source compensation, such as insurance benefits or government benefits, such plaintiff receives or is eligible to receive;¹⁴
5. Exclusive jurisdiction in federal court for suits against the sellers of Qualified Anti-Terrorism Technologies;¹⁵ and
6. A rebuttable presumption that sellers are entitled to the Government Contractor Defense.¹⁶

The designation of a technology as a QATT confers each of the aforementioned liability protections except for the rebuttable presumption in favor of the Government Contractor Defense, or GCD. That specific liability protection is conferred only upon an additional certification by the secretary, as discussed below.

Those who deploy QATTs are protected from liability for punitive damages if the technology allegedly fails to perform as intended in a terror attack. Liability is restricted to noneconomic damages in direct proportion to the seller’s percentage of responsibility.¹⁷ Noneconomic damages under the SAFETY Act are defined as “damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.”¹⁸

Further, compensatory damages may not exceed a predetermined amount of liability insurance coverage that the seller is obligated to main-

11. *See* 6 U.S.C. § 443 (c); 6 U.S.C. § 443(a)(2).

12. *See* 6 U.S.C. § 442 (b)(2).

13. *See* 6 U.S.C. § 442(b)(1).

14. *See* 6 U.S.C. § 442(c).

15. *See* 6 U.S.C. § 442(a)(2).

16. 6 U.S.C. § 442(d).

17. 6 U.S.C. § 442(b)(2)(A).

18. 6 U.S.C. § 442(b)(2)(B).

tain. The SAFETY Act provides that in connection with designation of a QATT, the seller is obligated to obtain liability insurance of such types and amounts that DHS has determined is appropriate “to satisfy otherwise compensable third-party 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.”¹⁹ The SAFETY Act provides that “[n]otwithstanding any other provision of law, liability for all claims against a Seller arising out of, relating to, or resulting from an act of terrorism when [QATTs] 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 . . .” shall not be in an amount greater than the limits of liability insurance that the seller is obligated to maintain.²⁰ Further, any recovery by a plaintiff in this context shall be offset by the amount of plaintiff’s collateral source compensation.²¹ The SAFETY Act’s insurance requirement and how the appropriate amount of insurance is calculated is discussed below.

In addition, exclusive jurisdiction in federal court is granted for all suits against the sellers of Qualified Anti-Terrorism Technologies.²² This is an especially important provision, as DHS interprets it to mean that in any suit arising out of a terrorism incident, not only can the seller be sued exclusively in federal court (itself an important protection against inflated damages awarded by some state jurisdictions), but further that it is *only* against the *seller* of a QATT that any suit can be upheld. As DHS states in the preamble to the SAFETY Act final rule, “[I]t is clear that the Seller is the only appropriate defendant in this exclusive Federal cause of action.”²³ That is, no lawsuit shall proceed against any user, vendor, or subcontractor employing a QATT, according to DHS interpretation. As DHS explains in the preamble to the final rule implementing the SAFETY Act, “[I]f the Seller of the Qualified Anti-Terrorism Technology at issue were not the only defendant, would-be plaintiffs could, in an effort to circumvent the statute, bring claims (arising out of or relating to the performance or non-performance of the Seller’s Qualified Anti-Terrorism Technology) against arguably less culpable persons or entities, including but not limited to contractors, subcontractors, suppliers, vendors, and customers of the Seller of the technology. Because the claims in the

19. 6 U.S.C. § 443(a).

20. 6 U.S.C. § 443(c).

21. 6 U.S.C. §§ 442(c).

22. 6 U.S.C. § 442(a).

23. 6 C.F.R. § 25 at 33150.

cause of action would be predicated on the performance or nonperformance of the Seller's Qualified Anti-Terrorism Technology, those persons or entities, in turn, would file a third-party action against the Seller."²⁴ It is for this reason that DHS interprets the SAFETY Act to bar claims against entities other than the seller.

CERTIFICATION OF A QATT

Following designation, the second class of protection is SAFETY Act *certification*.²⁵ Certification provides all the benefits of the systems of risk and liability management of designation, plus an additional layer of liability protection. DHS has interpreted this bi-level scheme to mean that a designation must be granted in order for a certification to be granted, but both may be granted simultaneously, if warranted. A seller of a Certified QATT is entitled to assert the Government Contractor Defense (GCD) in product liability or other litigation involving its SAFETY Act-certified technology resulting from an act of terrorism.²⁶ SAFETY Act certification of a QATT creates the rebuttable presumption that the GCD applies, which can only be overcome if a plaintiff proves that the seller acted "fraudulently" or "with willful misconduct" in applying for SAFETY Act protections.²⁷

The GCD, which exists in no statute but has been created in case law by the federal judiciary, essentially immunizes contractors that supply goods to the government provided they have met certain conditions. It has been used primarily by military contractors in cases involving allegations of defective military equipment. We will discuss the GCD in more detail below, but for now it is important to bear in mind that certification under the SAFETY Act entitles the seller to assert the affirmative GCD and thus serves as important protection against potential liability.

DESIGNATION VS. CERTIFICATION UNDER THE SAFETY ACT

As discussed above, the SAFETY Act creates two classes of protections. The broader classification is the designation of QATTs. The stricter classi-

24. *Id.*

25. 6 U.S.C. § 442(d).

26. *Id.*

27. 6 U.S.C. § 442(d)(1).

fication is certification, which serves to establish “[a] rebuttable presumption that the Seller is entitled to the ‘government contractor defense.’” The SAFETY Act mandates that the review culminating in a technology’s Certification must be “comprehensive,” and it must allow the DHS Secretary to determine “whether it will perform as intended, conforms to the Seller’s specifications, and is safe for use as intended.”²⁸ The Seller is also required to conduct “safety and hazard analyses on such technology, and . . . supply the Secretary with all such information.”²⁹

Just as the requirements for QATT certification are more rigorous than those for designation, the benefits attendant SAFETY Act certification are comparatively sweeping. In short, the SAFETY Act has, for the first time, codified the GCD—something that until now had been entirely a judicial construct.

Government Contractor Defense

Much has been written about the GCD, and while we will not attempt to provide exhaustive analysis, it is important, for purposes of understanding the SAFETY Act, to know the reach and limitations of the GCD. The leading case for the GCD is *Boyle v. United Technologies Corp.*, 487 U.S. 500 (1988). In that case, a U.S. Marine was killed in a crash of a helicopter manufactured by United Technologies. The Supreme Court held that the government contractor may invoke the GCD “when (1) the United States approved reasonably precise specifications; (2) the equipment conformed to those specifications; and (3) the supplier warned the United States about the dangers in the use of the equipment that were known to the supplier but not to the United States.”³⁰

The first prong is satisfied when the contractor shows that the government provided the technical requirements for the equipment or service, and that the government had exclusive control over the design, use, and application of the product. The second prong is a question of fact. The third prong ensures that the government knew about the dangers of a product before use. Many courts, like the U.S. Court of Appeals for the Ninth Circuit, have interpreted *Boyle* to apply only in the context of military procurement.³¹ Other courts have broadened the scope slightly.

28. 6 U.S.C. § 442(d)(2).

29. *Id.*

30. 487 U.S. 500, 512 (1988).

31. *Nielsen v. George Diamond Vogel Paint Co.*, 892 F.2d 1450, 1454–55 (9th Cir. 1990).

Whether the defense can be invoked against, for example, manufacturing defects is also controversial. On this and other issues, there has been an uneven and sometime unpredictable application of the GCD in our courts. What is clear is that where the GCD applies, state tort law is displaced: the Supreme Court in *Boyle* held that “state law which holds Government contractors liable for design defects” can present a conflict with federal policy and therefore “must be displaced.”³²

The decision clearly stated some important protections for defense contractors, but the doctrine was painstakingly limited by the Court. As one commentator has noted, “[w]hile the *Boyle* decision recognized the need to provide some litigation protections to private entities that help reduce public risk, the decision was quite limited in its application: it related only to contracts entered into directly with the federal government to provide goods that furthered the military’s conducting of the national defense. Yet, in light of recent developments in the war on terrorism and the threat posed by a potential avian flu pandemic, it becomes clear that the general policy justification for the government contractor defense in *Boyle* is compelling in contexts well beyond those presented in *Boyle*.”³³

Public Readiness and Emergency Preparedness Act

The SAFETY Act is not the only legislation that provides broad liability protections. Congress adopted a similar approach of shielding companies from liability when it passed the Public Readiness and Emergency Preparedness Act (PREP Act) enacted as Division C of the Defense Appropriations Act for fiscal year 2006, Pub. L. No. 109-148.³⁴ The PREP Act grants makers of drugs, vaccines, and devices immunity from civil liability for anything related to the development and production of drugs, vaccines, or devices. Just as Congress was concerned that not enough anti-terror technologies would make it to market without liability protections, so too was it concerned that vital protections against bioterrorism like vaccines and drugs would not become available absent protections against potential liability.

32. 487 U.S. 500, 512 (1988)

33. Paul Taylor, *We're All in This Together: Extending Sovereign Immunity to Encourage Private Parties to Reduce Public Risk*, 75 U. CIN. L. REV. 1595.

34. The PREP Act may be found in sections 319F-3 and 319F-4 of the Public Health Service Act and is codified at 42 U.S.C. §§ 247d-6d, 247d-6e.

Companies covered under the PREP Act are granted even broader protection from liability than the coverage available under the SAFETY Act. Under the PREP Act, so-called “covered entities” are “immune from suit and liability under Federal and State law with respect to all claims for loss caused by, arising out of, relating to, or resulting from the administration to or the use by an individual of a covered countermeasure.”³⁵ The process by which a countermeasure becomes “covered” is quite different from that under the SAFETY Act, however. Under the PREP Act, a countermeasure is covered if the secretary of HHS “makes a determination that a disease or other health condition or other threat to health constitutes a public health emergency, or that there is a credible risk that the disease, condition, or threat may in the future constitute such an emergency” and makes a declaration, through publication in the *Federal Register*, recommending, under such conditions as the secretary may specify, the manufacture, testing, development, distribution, administration, or use of one or more covered countermeasures.³⁶

Such government interventions in the private marketplace are rare and not without controversy. To a certain extent, such actions build upon the much less controversial, and long-established, common law principle of sovereign immunity, which provides that a government is immune from lawsuits unless it consents. The theory is that the government must be able to perform its essential functions, using the judgment of its elected officials and their subordinates, free from the prospect of litigation that would necessarily second-guess governmental decisions. Though the *Boyle* Court made clear that the government contractor defense is not based on sovereign immunity and expressly declined to decide whether such contractors enjoy such immunity, it reasoned that “it makes little sense to insulate the Government against financial liability for the judgment that a particular feature of military equipment is necessary when the Government produces the equipment itself, but not when it contracts for the production.”³⁷ The Court explained that “[t]he financial burden of judgments against the contractors would ultimately be passed through, substantially if not totally, to the United States itself, since defense contractors will predictably raise their prices to cover, or to insure against, contingent liability for the Government-ordered designs.”³⁸ Generally, the idea

35. 42 U.S.C. § 247d-6d.

36. *Id.*

37. *See Boyle*, 487 U.S. 512 (1988).

38. *See id.* at 511–12.

is that the government should be able to accomplish its most pressing national defense goals with the help of private companies, if it so chooses, without sacrificing its sovereign immunity. Until the SAFETY Act and the PREP Act, however, this line of reasoning had only rarely been extended to non-military functions.

The final rule implementing the SAFETY Act attempts to clarify the relationship between the SAFETY Act and the GCD: "The Department believes with the SAFETY Act that Congress incorporated government contractor defense protections outlined in the Supreme Court's *Boyle* line of cases as it existed on the date of enactment of the SAFETY Act, rather than incorporating future developments of the government contractor defense in the courts."³⁹ This interpretation begs several questions, especially since the GCD is not evenly applied across courts. Further, 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."⁴⁰

In the same way the GCD has been the subject of varying judicial interpretation, there will likely be no uniform national application of SAFETY Act protections in the event they are tested following a terrorist attack. Any SAFETY Act protections will be raised as an affirmative defense before a court, and it will ultimately be the courts that determine whether DHS's interpretation of its authority is valid. For example, DHS's interpretation in the final rule is that lawsuits may only be brought for claims for injuries that are proximately caused by sellers that provide qualified antiterrorism technology:

The best reading of § 863(a), 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 non-performance of the Seller's Qualified Anti-Terrorism Technology in relation to an Act of Terrorism, (2) Such cause of action may be brought only against the Seller of the Qualified Anti-

39. 6 C.F.R. § 25.

40. 6 C.F.R. § 25.8(b).

Terrorism Technology and may not be brought against the buyers, the buyers' contractors, downstream users of the Qualified Anti-Terrorism Technology, the Seller's suppliers or contractors, or any other person or entity, and (3) Such cause of action must be brought in Federal court. The exclusive Federal nature of this cause of action is evidenced in large part by the exclusive jurisdiction provision in § 863(a)(2).⁴¹

That said, what is beyond doubt is that the SAFETY Act is the first time the GCD has been expanded to non-military situations. In fact, the act applies even where the government is not a party at all 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—or to the private sector. With the SAFETY Act, the “government contractor defense” becomes the “seller of qualified anti-terror technology defense.”

Another way the SAFETY Act diverges significantly from the GCD is in the area of product design. Sellers of QATTs need not have designed their technologies to government specifications in order to obtain SAFETY Act protections. In fact, it works in the opposite manner, where a fully designed and potentially market-ready product is submitted to DHS for review.

One way the SAFETY Act's protections are more restrictive than the GCD is that the SAFETY Act's liability protections are effective only in the event of an act of terrorism. Under the GCD, contractors can use the shield whether or not there has been an act of terrorism or war or any other national security crisis. Accordingly, for the purposes of the SAFETY Act, the definition of an “Act of Terrorism” is crucial.⁴²

41. 6 C.F.R. § 25.

42. Relying upon the statute, DHS defined “Act of Terrorism” in the SAFETY Act Final Rule as follows: “any act determined to have met the following requirements or such other requirements as defined and specified by the Secretary: (1) Is 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.” See 6 C.F.R. § 25.2.

SAFETY ACT RESPONSIBILITIES

In addition to the benefits that SAFETY Act protection affords, there are also responsibilities for the sellers of the anti-terrorism technologies who receive SAFETY Act protection. Chief among these are the requirements to inform DHS of material modifications to QATTs and to maintain specified insurance. Section 443 of the SAFETY Act requires persons who “sell or otherwise provide a qualified anti-terrorism technology to Federal and non-Federal Government customers . . . [to] obtain liability insurance . . . in such amounts as shall be required.”⁴³ DHS has clarified that such insurance need not protect the seller’s contractors, subcontractors, suppliers, vendors, and customers.⁴⁴ The seller of the anti-terrorism technology may not be required to obtain insurance that is not “available on the world market [or] that would unreasonably distort the sales price of the Seller’s anti-terrorism Technology.”⁴⁵

The SAFETY Act final rule sets forth the following factors that should be considered in determining the requisite amount of liability insurance sellers are obligated to maintain in connection with their QATT:

1. The particular technology at issue;
2. The amount of liability insurance the seller maintained prior to application;
3. The amount of liability insurance maintained by the seller for other technologies or for the seller’s business as a whole;
4. The amount of liability insurance typically maintained by sellers of comparable technologies;
5. Information regarding the amount of liability insurance offered on the world market;
6. Data and history regarding mass casualty losses;
7. The intended use of the technology; and

43. 6 U.S.C. § 443(a)(1).

44. “The Department recognizes that an action for recovery of damages proximately caused by a QATT that arises out of an Act of Terrorism may only be properly brought against a Seller. Accordingly, the Department has specified, and will continue to specify in particular Designations, that the liability insurance required to be obtained by the Seller shall not be required to provide coverage for the Seller’s contractors, subcontractors, suppliers, vendors or customers.” 6 C.F.R. § 25 at 33154.

45. 6 C.F.R. § 25.5.

8. The possible effects of the cost of insurance on the price of the product, and the possible consequences thereof for development, production, or deployment of the technology.

If the seller fails to maintain coverage at the requisite level, a designation may be terminated.⁴⁶

Clearly, there are challenges inherent in a process to determine an appropriate level of insurance to be maintained by a seller of a particular QATT. The insurance component of the SAFETY Act has proven among the most difficult in the program's implementation. DHS has made recent progress through its utilization of a risk-based methodology and maintaining a high degree of flexibility in working with applicants to address the insurance component.

CHANGES TO DHS REGULATIONS IN 2007— STREAMLINING AND EXPANSION

DHS had been operating under an interim SAFETY Act regulation until 2007. In the SAFETY Act final rule, DHS applied industry and public comments and lessons learned from the first years of the SAFETY Act program. In the preamble to the final rule, DHS explained that the Final Rule:

1. further clarifies the liability protections available under the SAFETY Act;
2. states with greater specificity those products and services that are eligible for Designation as a Qualified Anti-Terrorism Technology;
3. clarifies the Department's efforts to protect the confidential information, intellectual property, and trade secrets of SAFETY Act applicants;
4. articulates the Department's intention to extend SAFETY Act liability protections to well-defined categories of anti-terrorism technologies by issuing "Block Designations" and "Block Certifications;"
5. discusses appropriate coordination of SAFETY Act consideration of anti-terrorism technologies with government procurement processes; and

46. 6 C.F.R. § 25.5(h).

6. takes other actions necessary to streamline processes, add flexibility for applicants, and clarify protections afforded by the SAFETY Act.⁴⁷

To increase flexibility, DHS provided for Developmental Testing and Evaluation Designations, as well as Block Designations and Block Certifications, which provide more flexible options for both companies with unproven technologies and those with proven technologies, respectively.

The incorporation of Developmental Testing and Evaluation (DT&E) Designations makes it possible to grant SAFETY Act protections to anti-terrorism technologies that are still in the development process. For example, promising technologies—including those developed by DHS's own Science and Technology Directorate researchers in cooperation with the private sector—that have yet to be field-tested could qualify for a DT&E Designation.⁴⁸ The litigation and risk management protections of the SAFETY Act could be made available, though with some limitations. DT&E Designations would have limitations on the use and deployment of the subject technology, remain terminable at-will by the department should any concerns regarding the safety of technology come to light, and have a limited term not to exceed a reasonable period for testing or evaluating the technology. Such a provision could also allow for rapid fielding of technologies in exigent circumstances, where there simply was not enough time to fully test certain technologies. As DHS has said, "The Department may issue a DT&E Designation for anti-terrorism technologies that show promise but that may not yet meet the requirements for Designation as a QATT."⁴⁹

Where DT&E Designations can help provide protection for unproven technologies, the use of Block Designations or Block Certifications can provide easy access to protections for sellers of technologies that have an

47. 6 C.F.R. § 25 at 33148.

48. About half of S&T's research and development budget goes toward identifying and developing technologies that have been specifically requested by field agents. To accomplish this, the S&T Directorate created "customer-led" Capstone Integrated Product Teams (IPTs) charged with identifying technological capability requirements across the department. This model is intended to ensure that investments meet up with actual homeland security requirements.

49. SAFETY Act Application Kit, July 2006, p.8.

established record of success. Such designations and certifications recognize technologies that meet technical criteria and established performance standards. When DHS issues such Block Designations or Certifications, it signals to sellers of covered technologies that the particular QATT already satisfies all relevant technical criteria—and no further technical analysis will be necessary before approval.⁵⁰ As DHS has stated, “[A]pplications from sellers of a QATT that is the subject of a Block Designation or Block Certification will receive expedited review and will not require submission of information concerning the technical merits of the underlying technology.”⁵¹ In short, entire classes of technology makers can receive the valuable protections of the SAFETY Act with minimum effort in this streamlined process. It should be noted that such Block Designations or Certifications can be issued either in response to an application to DHS or on DHS’s own initiative. Trade associations and industry groups would be well-advised to consider a relevant request to DHS. Similarly, an aggressive use of this provision by DHS could give a boost to the SAFETY Act program.

NEW DEVELOPMENTS—FAR AMENDMENT AND COORDINATION OF PROCUREMENTS

With an important addition to the Federal Acquisition Regulation (FAR), the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (the councils) have enhanced the significance of the SAFETY Act across the range of government procurements. In so doing, the councils built upon and expanded tools provided by the SAFETY Act final rule. In that rule, DHS had promised that it “recognize[d] the need to align consideration of SAFETY Act applications and the government procurement process more closely. Accordingly, the final rule incorporates provisions that establish a flexible approach for such coordination.”⁵²

In November 2007, the councils issued an Interim Rule that incorporated the SAFETY Act into the FAR.⁵³ To start, the rule ensures that SAFETY Act considerations are made an integral part of each agency’s acquisition planning procedures, and that contracting officers give ad-

50. 6 C.F.R. § 25.6(h); 6 C.F.R. § 25.9(j).

51. *Id.*

52. 6 C.F.R. § 25, preamble, at 33156.

53. 72 Fed. Reg. 63,027.

equate lead time in their acquisition plans to account for DHS's review process of SAFETY Act applications.⁵⁴ The Interim Rule emphasizes two other points: 1) it streamlines SAFETY Act approval in some cases, and 2) it gives government contracting officers the authority to allow companies to submit proposals that they can make *contingent* on SAFETY Act approval. Therefore, it is possible for a contractor to limit its financial exposure of proposing an otherwise risky technology to be fielded for the government.⁵⁵

The rule creates a new section in the FAR that requires 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.⁵⁶ In most cases, this will require that the contracting officer consult with DHS's Office of SAFETY Act Implementation. If DHS decides that SAFETY Act protection is not appropriate, a clause must be included in the Request for Proposal (RFP) or Solicitation stating that SAFETY Act coverage is not applicable. The procurement then proceeds as every other procurement does.⁵⁷

But if DHS determines that the technology or service is appropriate for SAFETY Act coverage, and it does not already fall under a Block Designation or a Block Certification approval for similar technologies, all potential offerors would have to stand up and take note. The procuring agency would get a “pre-qualification decision” from DHS—essentially a preview of what DHS will do with a certain technology once it receives a full SAFETY Act application. The pre-qualification decision, transmitted to the contracting officer, can be in one of two forms, both of which offer important benefits for offerors: first, DHS could say the particular product or service will be awarded SAFETY Act coverage once an application is received; second, DHS could give a presumptive

54. FAR 50.205-2.

55. The rule permits offerors to submit offers contingent on DHS issuing a SAFETY Act Designation or Certification. Under this first alternative, contracting officers may permit such contingent offers only if DHS has issued, for offers contingent upon SAFETY Act Designation, a prequalification Designation Notice or a Block Designation, or for offers contingent upon SAFETY Act Certification, a Block Certification.

56. FAR Part 50.204.

57. Contracting officers are required to insert FAR 52.250-2, SAFETY Act Coverage Not Applicable, if, after consultation with DHS, the agency has determined that SAFETY Act protection is not applicable for the acquisition, or DHS denies approval of a prequalification Designation Notice.

determination that the technology or service could qualify for SAFETY Act coverage, but it needs more data to be sure. In both cases, all offerors on that particular RFP would be eligible for streamlined SAFETY Act approval process. DHS has successfully used this process prior to the promulgation of the interim rule.

As discussed above, contracting officers can now issue awards on the presumption that the contractor will receive SAFETY Act coverage after the contract is awarded. Based on a clause required in this instance, an eventual decision by DHS to deny SAFETY Act coverage would be a ground for the contractor to seek an equitable adjustment, and to demand that the procuring agency compensate the vendor for its increased financial risk.⁵⁸ As further evidence of the federal focus on the SAFETY Act, the Interim Rule further requires agencies to encourage offerors to apply for SAFETY Act protections, even before a solicitation. In addition, it encourages industry outreach on SAFETY Act issues, such as in Requests for Information (RFIs), draft RFPs, and industry conferences.

Notably, the Interim Rule in the FAR builds upon an important development in the SAFETY Act Final Rule discussed above. Section 50.205-1(a) includes coverage for Block Designations and Block Certifications, requiring that the procuring agency verify with DHS whether one exists. If one does, then the requiring activity must inform the contracting officer, who must then incorporate the Block Designations and Block Certifications in any solicitation or advanced public notice to inform potential offerors of this important preexisting benefit.⁵⁹

The FAR addition expands further the intent of the SAFETY Act to encourage development of anti-terror technologies. If the goal of the SAFETY Act in general is to promote the use of the private sector for public homeland security concerns, and if the FAR regulation in particu-

58. If DHS does not issue a SAFETY Act Designation or SAFETY Act Certification to the successful offeror by the time of contract award, the contracting officer is then permitted to award the contract with the clause at 52.250-5, SAFETY Act-Equitable Adjustment, which allows for an equitable adjustment in the event DHS denies the contractor's SAFETY Act application.

59. Contracting officers are required to insert 52.250-3, SAFETY Act Block Designation/Certification, or 52.250-4, SAFETY Act Pre-qualification Designation Notice, in solicitations when DHS has issued a block designation/certification or a prequalification designation notice, respectively, for the solicited technologies. These provisions do not permit submission of offers contingent upon SAFETY Act Designation or Certification of the proposed product(s) or service(s).

lar aims to promote the use of the SAFETY Act in the procurement process, we are seeing progress on both fronts. One good example is TSA's Screening Partnership Program (SPP), which allows an airport operator to have screening services performed by a private screening company. The contractor must perform under federal oversight, and the contracted screeners must perform to equal or higher performance levels than federal screeners. TSA has established a SAFETY Act certification process for SPP contractors to help them limit their liability and offer a competitive price to the airport operators procuring their services.⁶⁰

THE OFFICE OF SAFETY ACT IMPLEMENTATION— HOW THE PROCESS WORKS IN PRACTICE

After the SAFETY Act Final Rule went into effect in July 2006, the DHS Office of SAFETY Act Implementation (OSAI) issued a new SAFETY Act Application Kit. The updated application kit contains the required forms for a submission, which request a good amount of detailed technical and financial information. The application requires the disclosure of a nonproprietary description of the technology, the technology's procurement status, the technological and essential elements of the technology (including proprietary information), and the type of terrorist attack the technology is intended to counter.

60. As TSA has publicly stated:

TSA also seeks to address the liability issue through clarification on the applicability of the Support of Anti-terrorism by Fostering Effective Technologies Act of 2002 . . . The Department of Homeland Security (DHS) Office of Science and Technology (OST) makes determinations concerning the applicability of the SAFETY Act. Application of the SAFETY Act does not provide blanket indemnification but limits third-party tort suits in the event of a terrorist incident. Significantly, liability protection pursuant to the SAFETY Act for services 'designated' as a qualified anti-terrorism technology will result in limited liability risks for the private screening company and its contractors, subcontractors, suppliers, vendors,s and customers as well as the contractors, subcontractors, suppliers, and vendors of the customer. TSA, OST, and the Office of General Counsel have been working closely on SAFETY Act determinations. The Department is still reviewing the applicability of the SAFETY Act.

Frequently Asked Questions, http://www.tsa.gov/what_we_do/optout/spp_faqs.shtml, last visited Oct. 7, 2008.

Once an application is received, the DHS under secretary of the S&T Directorate has 30 days to notify an applicant that receipt of the application is complete, 90 days to review a complete application, and the ability to extend without reason the review period for another 45 days.⁶¹ In short, DHS has up to 165 days to complete its review of a SAFETY Act application.

DHS also suggests that applicants submit a preapplication form. Such a form allows for a pre-application consultation, which is “a voluntary means through which OSAI provides helpful guidance to potential applicants without requiring the completion and submission of a full SAFETY Act Application.”⁶² Such a consultation allows a potential applicant to gauge its likelihood of ultimate approval and is an important safeguard against wasted time and effort.

Applicants should understand that SAFETY Act applications request a fair amount of detailed data, some of which applicants may view as proprietary either due to its technical nature or because it represents sensitive business information. Such data, while necessary for a proper evaluation of the technology, can be extremely sensitive for both business and security purposes. DHS has stated that such submitted information, whether ultimately a part of a successful application or not, will be safeguarded to the fullest extent of the law. “DHS is committed to taking all appropriate steps to protect the proprietary information of applicants consistent with applicable FOIA exemptions and the Trade Secrets Act (18 U.S.C. 1905). As an example of this commitment, those engaged in evaluating applications are required to enter into appropriate nondisclosure agreements. . . . Underlying this commitment to protect an applicant’s information are various Federal civil and criminal laws that potentially apply to unauthorized disclosure of SAFETY Act confidential materials, including the Trade Secrets Act and 18 U.S.C. Chapter 90.”⁶³

With these concerns in mind, applicants should consider consulting a practitioner with experience in SAFETY Act applications ahead of tendering such sensitive information. Moreover, DHS often will ask applicants for additional installments of information following an initial submission, and sometimes these information requests are overly aggressive. Counsel can play an important role in managing the exchange of

61. 6 C.F.R. § 25.6.

62. Safety Act Application Kit, July 2006, p.14.

63. 6 C.F.R. § 25.10.

information with DHS and navigating the overall application process. While the discussion above points to real improvement in the SAFETY Act procedures, applicants regularly confront obstacles on the road to receiving designation or certification. For example, disagreements over the appropriate type and amount of insurance coverage is a perennial issue. Experienced SAFETY Act practitioners can help applicants with the overall application process and limit potentially costly and time-consuming delays.

SUMMARY

The SAFETY Act is a valuable tool for litigation and risk management for companies developing and fielding anti-terrorism technologies. By giving companies the assurance they need to develop and deploy cost-effective homeland security technologies, the act has the potential to expand both the number of technologies available and the homeland uses of existing technologies. As discussed above, the SAFETY Act furthers private interests to the benefit of the greater common good by enhancing our nation's security. In-house and outside industry counsel can support both goals by promoting the use and understanding of the SAFETY Act.

