SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
ATTORNEYS AT LAW

DECEMBER 2003

Liability Limitations For Anti-Terrorist Technologies Under The SAFETY Act

By Douglas E. Perry and David S. Gallacher

Following the September 11th terrorist attacks, Congress passed a new law known as the Support Anti-Terrorism by Fostering Effective Technologies ("SAFETY") Act of 2002 to encourage the development of anti-terrorism technologies and devices. The premise of the Act is straightforward - sellers of anti-terrorist technologies are encouraged to submit their technologies for review and evaluation to the Department of Homeland Security (the "Department" or "DHS"). If the Department designates or certifies the technology as a "qualified anti-terrorist technology," the seller's liability in the event of a terrorist attack is capped.

On October 16, 2003, DHS issued interim rules implementing the SAFETY Act. These interim rules outline the procedures for applying for and receiving SAFETY Act protections; they also provide additional details concerning (i) the scope of the SAFETY Act, (ii) the definition of "anti-terrorist technologies," and (iii) the levels of liability limitation available to sellers of designated or certified anti-terrorist technologies.

1. *Scope of the SAFETY Act*

As a preliminary matter, sellers of anti-terrorist technologies should recognize that the SAFETY Act only limits liability if the underlying damage results from an act of terror. Under the interim rules, an "act of terrorism" may include an act in the United States or overseas "if it causes harm to a person, property, or an entity in the United States." If the underlying damage is caused by acts or omissions not related to terrorism, the sellers of technologies that are otherwise "qualified" or "certified" do not receive the benefits of the SAFETY Act.

For purposes of the SAFETY Act, a "seller" is defined as the entity that receives the Designation for a qualified anti-terrorism technology. A "Seller" is the only entity required to obtain the required liability insurance coverage.

2. *Definition of Anti-Terrorist Technologies*

The interim rules indicate that the Department intends to cover a broad range of anti-terrorism

technologies under the SAFETY Act. In general, "any qualifying product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or prepared for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause" are intended to be within the scope of the SAFETY Act.

The interim rules clarify that multiple use technologies may satisfy the definition of a qualified anti-terrorist technology. Thus, technologies not designed exclusively to meet terrorist threats may nonetheless receive the liability limitation benefits of the SAFETY Act provided they serve the purpose of preventing, detecting, identifying, or deterring acts of terrorism.

Ultimately, the Department is afforded broad discretion (and flexibility) in evaluating the technology and considering whether technology qualifies under the SAFETY Act. Moreover, the Department's determinations are not subject to judicial review. Sellers wishing to avail themselves of the liability protections of the SAFETY Act should therefore submit comprehensive application materials and address all DHS concerns or questions.

3. *Levels Of Liability Limitation Protections*

The interim rules establish two levels of limited liability protections.

The first level of protection is provided to technologies that are "designated" as qualified anti-terrorism technologies. Sellers of "designated" technologies receive the following liability limitation benefits in the event of a terrorist attack:

1. They are not liable for punitive damages and pre-judgment interest penalties.

2. Joint and several liability for "non-economic damages" is limited to an amount directly proportional to the seller's responsibility for losses due to the terrorist act.

3. Damages are reduced in amounts equal to compensation received from collateral sources, such as private insurance and other government benefits.

4. Liability is capped in an amount equal to the amount of insurance the Department determines the seller will be required to obtain and maintain. (This cap, in turn, will likely be a function of the first three limitations set forth above.)

The second level of protection is provided to technologies that are "certified" as approved products for DHS. "Certified" technologies receive the liability protections of "designated" technologies as well as a presumption that a doctrine known as the "Government contractor defense" applies. In essence, this defense shields the seller of "certified" anti-terrorist technologies from tort liability, provided the seller did not receive the certification approval on the basis of fraud or willful misconduct.

Sellers of anti-terrorist technologies would prefer to receive the increased protection afforded to

"certified" technologies. The process for "designating" and then "certifying" anti-terrorist technologies is discussed below.

4. *"Designation" of Anti-Terrorism Technologies*

The Department is afforded broad discretion and flexibility to "designate" anti-terrorist technologies, with the burden falling on the seller to justify the designation. The Department has emphasized that "[a]n application for a Designation or a Certification is a positive assertion on that applicant's part that the technology in question deserves special protections under the law in order to promote a public good. It is the applicant's responsibility to make a persuasive and defensible case."

In designating qualified technology, the Department considers three general categories: Technical, Business, and Insurance.

In the "Technical" area, the Department assesses the effectiveness, suitability, and safety of the technology. The Department has established a "voluntary consensus process" involving users, manufacturers, and private and public sector technical communities in "all phases" of the development of technical standards to evaluate technologies. If applicable standards do not exist or are incomplete, the Department will evaluate technologies based on best practices or existing laboratory or field testing. The Department also has indicated that it is establishing a network of certified laboratories to conduct this testing.

In the "Business" area, the Department assesses the seller's ability to produce and deploy the technology, as well as the potential risks that could keep the technology from market.

In the "Insurance" area, the Department conducts a comprehensive evaluation of the insurance needs associated with the technology.

As a practical matter, applicants would be well advised to provide as much information as possible concerning

1. The broad range of successful applications and effectiveness of the technology.

2. Test results, scientific studies, and past experience with the technology.

3. The current availability of the technology.

4. The risks of the technology (balanced with its benefits).

5. The availability of insurance coverage for the technology.

6. The likelihood of deployment in the absence of SAFETY Act coverage.

The interim rules indicate that the Department will reach a decision on an application within approximately 150 days from its submittal. Given the Department's goal of deploying anti-terrorist technologies as soon as possible, industry believes that the Department will make every effort to reach a decision within that time frame. If the Department "designates" a technology under the SAFETY Act,

the designation will be valid for a period of 5-8 years. The designation is renewable, it is transferable to licensees, and it will contain a certification of the required liability insurance the seller is expected to carry.

Sellers whose technology receives the "designation" label should note that the designation will be canceled automatically if the technology is significantly modified. Under the interim rules, modifications that reduce the safety or effectiveness of the technology are considered a "significant modification." In other words, if the effect of a modification to the design, material or manufacturing process is to reduce the safety or effectiveness of the technology, the seller will be required to submit an "Application for Modification of Designation"; on the other hand, if the modification does not affect the safety effectiveness of the technology, sellers will not be required to submit a modification application to continue to receive the SAFETY Act protections.

As a practical matter, sellers should seek a designation that is broad and flexible to account for product modifications, while carefully monitoring any changes to ensure that the effectiveness of the technology is not compromised. Sellers should also seek, as appropriate, new designations for the technologies as they change over time.

5. *Insurance Requirements*

The Department will not "designate" an anti-terrorist technology unless and until the seller obtains and maintains liability insurance for a single terrorist act that is appropriate to satisfy third-party claims from the act. The interim rules indicate that the certified amount (which may include self-insurance, as approved by the Department) need not exceed an amount reasonably available on world markets at prices and terms that will not unreasonably distort the price of the technology. The Department, thus, has broad discretion in setting (and certifying to) the required insurance limits.

In light of these rules, sellers seeking to qualify their technologies as "designated" technologies should provide a comprehensive explanation of the availability of the insurance and the basis for the proposed insurance coverage in their application to the Department. Obviously, determining an appropriate amount of insurance could be very difficult given the lack of comprehensive actuarial data for new technologies. However, sellers must attempt to identify fair and reasonable numbers to justify their insurance position before the Department.

Sellers are also required to provide to the Department annual certifications of insurance coverage regarding the approved technologies. Sellers must also notify the Department of any change in type or amount of insurance coverage.

6. *"Certification" of Anti-Terrorist Technologies*

The seller of anti-terrorist technologies receives additional product liability limitation protections if the Department "certifies" that the technology is an "approved product" of DHS. Once a technology is "certified," the seller is granted the rebuttable

presumption of the "government contractor defense." Under this doctrine, sellers receive immunity from liability for claims brought in a product liability or other lawsuit arising out of, relating to, or resulting from a terrorist act.

To receive the certification, the seller must (i) follow the procedures outlined above for "designating" the technology and (ii) then submit "safety and hazard analyses and other relevant data and information regarding such technology" to the Department. Before the technology is certified, the Department is required to conduct a comprehensive review of the design to determine that the technology works as intended, conforms to the seller's specifications, and is safe for its intended use. As part of this review process, sellers should seek to meet with Department officials to explain and demonstrate their technologies.

Sellers whose technologies are "certified" may transfer the certification to licensees. Moreover, as is the case with "designated" technologies, sellers should review the certification carefully to make sure that any product modifications fall within the scope of the certification.

7. *Application Procedures*

Applicants may sign up for automatic email notifications and avoid filing delays by submitting an application online at :
www.safetyact.gov/DHS/SActHome.nsf.

If an applicant chooses to submit an application via "hard-copy" (either traditional paper or CD-ROM), the option is available, although it could delay the start of the evaluation process.

Reference materials, including a full Application Kit and Instructions, are available on the website. Detailed forms, instructions, and guides for completing and submitting an Application are also available on the website. Applicants requesting certification of their technology must complete both the "designation" forms and the "certification" forms.

The application forms require applicants to submit substantial financial and management data, including business plans, lists of customers, sales histories, revenue projections, profit analyses, and detailed cost information. The interim rules state that the application process will take applicants an estimated 36 to 180 hours to complete. These estimates are probably understated for most applicants.

8. *Protection of Proprietary Data*

The interim rules do not provide any unique procedures for protecting propriety information submitted by applicants. The Department has indicated, however, that it will require all contractors and agents of the Department to enter into nondisclosure agreements, and that access to an applicant's confidential information will be granted only after an examination of each application for potential conflicts of interest. The Department has also stated that proprietary information submitted by applicants in connection with their applications will be exempt from disclosure under the Freedom

of Information Act ("FOIA"). Classified information should not be submitted with any applications.

9. *Review Timeline*

Evaluation of the application by the Department proceeds according to the following schedule, which can be slightly extended by the Department:

- Following the submission of an application for designation consideration, the Department reviews the application to ensure that it is complete. The applicant must be notified within 30 days of receipt that the application is complete or that the Department requires additional information.

- Within 90 days of the Department's receipt of the application, the Department evaluates the application against the three basic criteria of Technical, Business, and Insurance. The Department may extend the time to respond up to an additional 30 days.

- Within 30 days of the completion of the initial evaluation, the evaluation is reviewed by the Assistant Secretary for the Science and Technology Division. The Assistant Secretary then provides a recommendation to the Under Secretary of the Department, either denying the application, requesting additional information, or approving the application (describing the scope and limitations for the anti-terrorism technology). The Department may extend the time to review up to an additional 30 days.

- The Under Secretary will then either provide the applicant with formal notice of rejection, request additional information, or issue a Designation as a "qualified anti-terrorism technology" and, if appropriate, provide a SAFETY Act Certification. The Department advises applicants that they can help facilitate the review process by taking the following steps:

1. Submit a separate Pre-Application form. This voluntary step consists of completing a short form detailing the technology. In response, the Department will provide a basic review of the technology capabilities, evaluation results, business plan, and insurance portfolio, as well as speculating as to the likelihood of receiving the requested designation. This step is helpful because it can identify application shortfalls early in the process and assist applicants in improving the application, although the Department is not bound by its pre-application review. Reviews of Pre-Applications typically will be completed within 21 days. Submitting a Pre-Application does not start the clock running on the Department's schedule for the formal application process.

2. Submit an application electronically to ensure timely receipt, and avoid human error that could result from scanning or inputting the application into an electronic form.

3. Assemble a team of experts to address the required Technical, Business, and Insurance questions before submission of the application.

4. Prepare for requests for additional information, and provide prompt and complete responses to questions from DHS.

CONCLUSION

The SAFETY Act offers sellers of anti-terrorist technologies some real protection in the event of a terrorist attack. The interim regulations reflect the broad discretion afforded the Department in "designating" and "certifying" qualified anti-terrorist technologies. To receive these protections, sellers should provide as much detail as possible in their applications about their technology - including information about the purpose and maturity of the technology; the availability of the technology in the absence of liability protection; scientific and testing data; and information concerning potential liability and insurance coverage. Sellers should also seek follow up meetings with Department officials to explain or demonstrate their technologies - particularly if they are seeking "certification" protection.

About the Authors

Doug E. Perry is a partner in the Washington, D.C. office. Mr. Perry has a broad range of experience in qui tam litigation and government contract matters, including claims and appeals, cost issues, commercial item contracting, General Services Administration schedule contracting, teaming agreements, defective pricing and bid protests. He also counsels clients extensively on export compliance obligations under the Export Administration Regulations and the International Traffic in Arms Regulation.

Mr. Perry may be reached at (202) 218-0008 or dperry@sheppardmullin.com

David S. Gallacher is an associate in the Washington, D.C. office. Mr. Gallacher's professional experience includes litigating under the qui tam provisions of the False Claims Act, assisting government contractors in protesting agency decisions on contract awards, representing government contractors on cost accounting issues and contract disputes before the Boards of Contract Appeals, counseling government contractors on the application of federal procurement regulations, and conducting internal investigations.

Mr. Gallacher may be reached at (202) 218-0033 or dgallacher@sheppardmullin.com

WASHINGTON, D.C.

Sheppard, Mullin, Richter & Hampton LLP
1300 I Street, NW, 11th Floor East
Washington, DC 20005
202.218.0000 | Fax: 202.218.0020

LOS ANGELES

Sheppard, Mullin, Richter & Hampton LLP
333 South Hope Street, 48th Floor
Los Angeles, California 90071
213.620.1780 | Fax: 213.620.1398

WEST LOS ANGELES

Sheppard, Mullin, Richter & Hampton LLP
10940 Wilshire Boulevard, Suite 2030
Los Angeles, California 90024
310.824.0097 | Fax: 310.824.9788

SAN FRANCISCO

Sheppard, Mullin, Richter & Hampton LLP
Four Embarcadero Center, 17th Floor
San Francisco, California 94111
415.434.9100 | Fax: 415.434.3947

SANTA BARBARA

Sheppard, Mullin, Richter & Hampton LLP
800 Anacapa Street
Santa Barbara, California 93101
805.568.1151 | Fax: 805.568.1955

ORANGE COUNTY

Sheppard, Mullin, Richter & Hampton LLP
650 Town Center Drive, 4th Floor
Costa Mesa, California 92626
714.513.5100 | Fax: 714.513.5130

DEL MAR HEIGHTS

Sheppard, Mullin, Richter & Hampton LLP
12544 High Bluff Drive, Suite 300
San Diego, California 92130
858.720.8900 | Fax: 858.509.3691

SAN DIEGO

Sheppard, Mullin, Richter & Hampton LLP
501 West Broadway, 19th Floor
San Diego, California 92101
619.338.6500 | Fax: 619.234.3815