Contemporary Legal Notes

Washington Legal Foundation
Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

# THE SAFETY ACT: A VITAL TOOL IN THE FIGHT AGAINST TERRORISM

by

Joe Whitley
Parney Albright
George Koenig

Washington Legal Foundation
CONTEMPORARY LEGAL NOTE Series
Number 52
November 2006

# THE SAFETY ACT:
# A VITAL TOOL IN THE
# FIGHT AGAINST TERRORISM

by
Joe Whitley
Parney Albright
George Koenig

Washington Legal Foundation
CONTEMPORARY LEGAL NOTE Series
Number 52
November 2006

Visit us on the Web at
www.wlf.org

# ABOUT WLF'S LEGAL STUDIES DIVISION

The Washington Legal Foundation (WLF) established its Legal Studies Division to address cutting-edge legal issues by producing and distributing substantive, credible publications targeted at educating policy makers, the media, and other key legal policy outlets.

Washington is full of policy centers of one stripe or another. But WLF's Legal Studies Division has deliberately adopted a unique approach that sets it apart from other organizations.

First, the Division deals almost exclusively with legal policy questions as they relate to the principles of free enterprise, legal and judicial restraint, and America's economic and national security.

Second, its publications focus on a highly select legal policy-making audience. Legal Studies aggressively markets its publications to federal and state judges and their clerks; members of the United States Congress and their legal staffs; government attorneys; business leaders and corporate general counsel; law school professors and students; influential legal journalists; and major print and media commentators.

Third, Legal Studies possesses the flexibility and credibility to involve talented individuals from all walks of life - from law students and professors to sitting federal judges and senior partners in established law firms - in its work.

The key to WLF's Legal Studies publications is the timely production of a variety of readable and challenging commentaries with a distinctly common-sense viewpoint rarely reflected in academic law reviews or specialized legal trade journals. The publication formats include the provocative COUNSEL'S ADVISORY, topical LEGAL OPINION LETTERS, concise LEGAL BACKGROUNDERS on emerging issues, in-depth WORKING PAPERS, useful and practical CONTEMPORARY LEGAL NOTES, interactive CONVERSATIONS WITH, law review-length MONOGRAPHS, and occasional books.

WLF's LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "WLF" or by visiting the Washington Legal Foundation's website at www.wlf.org. All WLF publications are also available to Members of Congress and their staffs through the Library of Congress' SCORPIO system.

To receive information about previous WLF publications, contact Glenn Lammi, Chief Counsel, Legal Studies Division, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, D.C. 20036, (202) 588-0302. Material concerning WLF's other legal activities may be obtained by contacting Daniel J. Popeo, Chairman.

 

# ABOUT THE AUTHORS

**Joe Whitley** is a member of Alston & Bird LLP's Global Security & Enforcement Practice Team. Mr. Whitley served as the first General Counsel for the Department of Homeland Security.

**Parney Albright** is Managing Director with the Civitas Group LLC. He previously served as the Assistant Secretary of the Department of Homeland Security for Science and Technology.

**George Koenig** is a member of Alston & Bird LLP's Global Security & Enforcement Practice Team.

*The authors are grateful to Rory Diamond, a third-year law student at the University of San Diego, for his invaluable assistance in preparing this article.*

 

# THE SAFETY ACT: A VITAL TOOL IN THE FIGHT AGAINST TERRORISM

By

Joe Whitley
Parney Albright
George Koenig

## INTRODUCTION

When President Bush signed the Homeland Security Act of 2002 (HSA) into law on November 25, 2002,[1] one of its most interesting and innovative provisions was the portion of the legislation called the "Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act)."[2] The SAFETY Act is intended to address the liability concerns that often prevent companies with anti-terrorism technologies (or those that purchase them) from selling and deploying them to the field. Thus, the SAFETY Act was enacted to foster the creation, development and use of anti-terrorism technologies, by providing "risk management" and "litigation management" protections for sellers of qualified anti-terrorism technologies and others throughout the supply, distribution, and user chain. On June 8, 2006, the final regulations

[1]Pub. L. No. 107-296, 116 Stat. 2135 (to be codified in various sections of 6 U.S.C.).

[2]6 U.S.C. §§ 441-44 (2006).

implementing the SAFETY Act (Final Rule) were promulgated by the Department of Homeland Security (DHS).[3] More recently, on August 16, 2006, DHS posted on its website its new SAFETY Act application kit (Kit)[4], which accounts for the changes contained in the Final Rule. According to DHS, the Kit states with greater specificity the information required to properly evaluate a SAFETY Act application. Companies that are involved in the security business, whether as manufacturers of anti-terrorism technologies or those that provide professional, design or consulting services will benefit from the protections offered under the SAFETY Act and Final Rule. This CONTEMPORARY LEGAL NOTE discusses the SAFETY Act and this Final Rule.

The events of September 11th inspired Congress to address, through the SAFETY Act, the threat that potential legal liabilities would discourage companies from investing in the research, development, and production of new technologies needed to protect the American public from the threat of terrorism, and also inhibit potential buyers from deploying them to the field. In late 2003, DHS published an interim rule detailing how the SAFETY Act would be implemented. As of July 2006, there are more than 80 anti-terrorism

[3]Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) 71 Fed. Reg. 33147-168 (June 8, 2006) (to be codified at 96 C.F.R. pt. 25).

[4]The Kit can be found at www.safetyact.gov.

technologies that have been designated or certified[5] under the SAFETY Act; many of these have been deployed to the field and are protecting the Nation. The publication of the Final Rule and the Kit, coupled with the maturation of the implementation processes both within DHS and the applicant community, should prove even more beneficial to the American public for several reasons. First, the private sector community has become more educated about the process and therefore is submitting better prepared SAFETY Act applications. Second, there are now more trained personnel at DHS to review applications, and in addition the need for substantial, "back and forth" dialog with applicants has been greatly reduced, resulting in considerable improvement in response time. Third, the Final Rule improves upon the interim rule, addressing many of the concerns raised by developers of anti-terrorism technologies. For example, the Final Rule allows a more seamless integration of the SAFETY Act with the government procurement process.

Significantly, the SAFETY Act covers *all* sales to *anyone* and not just government contracts. This leads many corporations to proudly market their product's placement on the DHS "Approved Products" list. The Final Rule and the consequently more effective implementation of the SAFETY Act enhances the ability of firms and organizations that develop and deploy anti-terrorism technologies by providing critical protections and, in many cases, with a

[5]These terms, and the distinction between them, are explained *infra* at 7-10.

substantial marketing advantage.

For developers of anti-terrorism products and services, the Final Rule reaffirms the significant protections provided by the SAFETY Act. These benefits for Designation are:

- exclusive federal cause of action and federal court jurisdiction;
- liability caps at a level so that purchased protection does not unduly affect the price of the technology;
- no joint and several liability for non-economic damages, and no punitive damages or prejudgment interest;
- plaintiffs' recovery reduced by any amounts collected from collateral sources.

In the case of Certification, there are additional benefits:

- a rebuttable presumption that the seller is entitled to the "Government Contractor Defense" (GCD), which extends governmental immunity to the seller for certain claims. This defense (now statutorily realized in the SAFETY Act) was originally a judicially-created extension of governmental immunity to those entities providing the Federal government with products and/or services the specifications of which were created or adopted by the government. Substantial legal authority exists for GCD. In the case of a certified SAFETY Act technology, the availability of the defense will be determined by whether the technology conforms to the technology description *as defined by the Seller;* the defense is not limited to sales made on the basis of a government specification or even a sale to the government. The GCD applies to *all* sales to *anyone* and remains in effect *ad infinitum* for sales made during the period of the QATT[6] designation. The rebuttable presumption will only be overcome by "clear and convincing evidence showing that the seller acted fraudulently or with willful misconduct in submitting

[6]Qualified Anti-Terrorism Technology.

information to [DHS]."[7] This must include a "knowing and deliberate intent to deceive" DHS.[8]

- Certification also results in receiving a "Certificate of Conformance," and also publication on the "Approved Product List," which is maintained by the Office of Safety Act Implementation at www.safetyact.gov.

Some of the key features of the Final Rule are:

- **Reaffirmation of the principle that the seller is the only appropriate defendant in all causes of action and claims**: this implies that no cause of action may be brought on a buyer of a technology, or on a subcontractor or supplier providing to the seller a component or subsystem.

- **Reaffirms the enduring protections associated with Designation and Certification**: this states that any technology deployed over the time period covered by Designation or Certification enjoys SAFETY Act protections for all time.

- **Reaffirmation of the expansive statutory language defining the broad range of technologies covered**: includes anti-terrorism products, equipment, devices, information technology, design services, consulting services, engineering services, software development, software integration, threat assessments, vulnerability studies and other analyses relevant to homeland security.

- **Significant improvement of coordination between government procurement and QATT reviews**: allows government agencies to

---

[7] § 25.8(b)

[8] *Id.*

[10] The term "Act of Terrorism" under the Final Rule has three components: (1) the act must be unlawful; (2) the act must cause harm, including financial harm, to a person, property, or entity in the United States (or U.S. air carrier or flag-vessel abroad); and (3) the actor must use or attempt to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the U.S. 6 C.F.R. § 25.2 (2006). Significantly, the Rule is silent on who would determine that an event qualifies as an "Act of Terrorism" and thus allowing SAFETY Act protections to apply; presumably the matter would be left to the courts.

seek conditional pre-approval from DHS for anti-terrorism products and services they intend to procure.

- **Strong statement of confidentiality**: reaffirms that DHS will treat all applications for either QATT Designation or Certification as confidential. Confidentiality also extends to the fact that a business has filed an application. It should be noted however, that while DHS states in the regulation its position that this confidential information is exempt from Freedom of Information Act (FOIA) requests, residual concerns remain that until that assertion is tested in court the matter is unsettled.

- **Reaffirmation of coverage of some acts of terrorism outside the United States**: under DHS rules, an act of terrorism must occur before SAFETY Act protections apply. The SAFETY Act limits a seller's liability when the seller's product is deployed during or in response to an act of terrorism.[10] The Final Rule includes protection for acts of terrorism that occur outside of the United States, but cause harm within the U.S., as in the case of a cyber attack launched overseas but affecting the United States. One obvious point worth mentioning is that, of course, the SAFETY Act has no direct impact on claims made outside of the U.S. judicial system.

- **Provides protection for technologies undergoing field testing and evaluation**: provides for Developmental Testing and Evaluation (DT&E) designations so that a seller may deploy a system still in development (and thus with as yet unknown performance characteristics) to the field for testing and evaluation purposes without concern for liability.

The most significant feature of the Final Rule is the **QATT Designation or Certification** process. To take advantage of these protections, a seller's anti-terrorism product or service must be "Designated" or "Certified" as a QATT by the Secretary of DHS. A QATT "Designation" will allow a seller to benefit from all of the protections, except the explicit protection of the Government Contractor Defense. A seller of a "Certified" technology may also invoke the Government Contractor Defense, which in effect makes the seller

immune from any liability risk should an act of terrorism occur.

In order to receive SAFETY Act protection, a seller must submit an application to the Under Secretary for Science and Technology of DHS utilizing the previously referenced Kit. The application requires a full description of the technology and a full analysis of the seller's liability insurance coverage.[11] A seller must specify the earliest date of sale of the QATT and, to the extent practical, include standards, specifications, requirements, performance criteria, limitations, or other information DHS may deem appropriate relating to the QATT. Within 90 days of acknowledging to the seller that their application is complete, the Under Secretary will either approve or deny the application. However, it is within the Under Secretary's discretion to extend that deadline.

The Under Secretary may designate an anti-terrorism product or service as a QATT if it qualifies as being "designed, developed, modified, provided or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause."[12] In assessing a technology's potential QATT Designation, the Under Secretary will take into account nine criteria:

1. Prior U.S. government use or demonstrated substantial utility and effectiveness.

---

[11]This includes: names of insurance companies, policy numbers, expiration dates, descriptions of coverages, dollar limits per occurrence and annually of insurance, insurance deductibles, policy exclusions and limitations, price of insurance, and the scope of insurance coverage. § 25.5(f)(3).

[12]§ 25.4(a).

2. Availability of the technology for immediate deployment in public and private settings.

3. Existence of an extraordinarily large or unquantifiable potential third party liability.

4. Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the SAFETY Act are extended.

5. Magnitude of risk exposure to the public if the 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. Whether the technology is effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat, and 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. This criterion was rendered explicit in the Final Rule.

9. Any other facts that the Under Secretary may consider to be relevant to the determination or to the homeland security of the United States.

The Under Secretary may give greater or lesser weight to some factors over others. For example, under the 1st, 6th, and 8th criteria above great weight may be given to the determination (through, e.g., licensure) by the FDA, that a particular medical countermeasure should be Designated. On the other hand, a determination by a local official, who has relied on vendor claims regarding the appropriateness of a technology may be given little if any weight; a local official would presumably not be allowed to set what would be a de facto national

performance standard without a substantial review of the technology's efficacy by DHS. Indeed, a QATT might not satisfy some of the listed criteria at all. The relative weighting of the various criteria varies depending upon the particular technology at issue and the threats that the technology is designed to address. Moreover, the Under Secretary may adopt official standards the compliance with which will also be taken into account when evaluating a potential QATT designation. Similarly, the Under Secretary may recognize the substantial equivalence between a technology in a new application and an already QATT designated technology.[13]

In order to get a technology "Certified," a seller must first apply for a QATT Designation (that is, Designation is a prerequisite for Certification). In practice, sellers may apply for both a QATT Designation and a Certification at the same time.

In determining whether to issue Certification, the Under Secretary conducts a comprehensive review of the design of the technology and determines whether: (1) it will perform as intended; (2) conforms to the seller's specifications; and (3) is safe for use as intended. It is entirely possible for a technology to be Designated but not Certified. In practice, failure to receive Certification will most likely be the result of a failure to demonstrate that the

[13]To be deemed an equivalent technology, a potential QATT must have the same intended use and the same or substantially similar performance or technological characteristic as the prior technology and it must have. § 25.4(d).

product will "perform as intended." It is certainly unlikely that DHS would issue even a Designation to a product not considered "safe" (though it is unclear what objective criteria might be applied), and it is also highly unlikely that a product submitted would receive Designation if it failed to meet the *seller's* own specification.

To illustrate how a product might receive Designation but not Certification, consider the real world challenges that might exist with technologies that involve both products and services. For example, screening is a "technology" under the broad definition of the SAFETY Act. The screening equipment in particular might be required to meet fairly stringent performance requirements, and the overall performance of *the system* (which *includes both the equipment and the operator*—the screener) would require periodic testing or auditing. Conceivably, it may be in the national interest to deploy the technology in question sooner rather than later, but the Under Secretary may determine that there is not sufficient empirical evidence for the application to receive Certification. Initially, the Under Secretary may be more inclined to give the technology (here, the overall system of equipment, operator, training regimen, etc) Designation status rather than Certification. However, at a later date, Certification could always be reapplied for if it can be shown through field data, or a determination by DHS, that the achieved level of performance can in fact be judged to "perform as intended."

The new rules provide for Developmental Testing and Evaluation (DT&E) designations. These are designations that limit liability for a fielded technology *for a proscribed period of deployment*. This new feature was intended to address a conundrum: there are technologies whose performance in a laboratory environment, while suggestive, does not indicate (even approximately) the performance that might be expected in a field environment (this is particularly the case for many types of sensor systems). Thus, in order for the SAFETY Act office to be comfortable with the efficacy of a technology for which this is an issue, some field testing is needed. However, developers were concerned that such a field deployment, despite its nature as a "test," would create for them a liability risk should an act of terrorism occur during the test. Hence, recognizing this legitimate concern, DT&E Designation was incorporated in the Final Rule.

The Final Rule also allows the Under Secretary to create a block Designation and provide SAFETY Act protections for a whole category of technologies. What this means is that the Under Secretary may announce that any embodiment of a technology that can demonstrate that it meets some specified performance criteria will be presumed to have satisfied the criteria for SAFETY Act Designation (or Certification), and thus all a seller needs to do is work with the SAFETY Act office to determine the liability cap.

It is this Block Designation (or Certification) that allows far greater integration with government procurement. Thus, as a procurement is being considered within the government (federal, state, or local), the agency can work with the SAFETY Act office to determine whether the technology (as broadly defined) to be procured is eligible for SAFETY Act protection, and if so whether the specified performance requirements would satisfy the criteria for either Designation or Certification. The agency can then include in the solicitation a statement as to the applicability of the SAFETY Act to the procurement and its pre-approval as a Designated or Certified technology. Once a contract is awarded, the seller would then need only to work with DHS to agree on a liability cap. It is anticipated that this process will ultimately be first incorporated within the DHS Acquisition Regulations and then the Federal Acquisition Regulations.

It will be interesting to watch how this process is implemented, since it in effect inserts DHS and the SAFETY Act office into the requirements process of other agencies; for example, any change in the performance requirements that might be contemplated over the course of a procurement that has been deemed pre-approved for SAFETY Act protection would require DHS acquiescence. It furthermore should have the beneficial effect of forcing a more precise definition of requirements (and acceptance testing protocols) in affected procurements. It is also worth noting that when the SAFETY Act was enacted,

Executive Order 10789 was modified (*See* Executive Order 13286) to require any federal agency (other than the Department of Defense) considering whether to extend indemnification in a procurement to seek from DHS a determination of SAFETY Act applicability, and if applicable, either require pursuit of SAFETY Act protection in lieu of indemnification, or an exemption from OMB.

The insurance requirements of the SAFETY Act are seen as fairly rigorous. To attain a QATT Designation for a technology, a seller must obtain liability insurance in such types and amounts as designated by the Under Secretary. Ultimately, the Under Secretary decides the amount and types of liability insurance required by each entity applying for QATT status. In making this determination, the rules allow, but do not require, the Under Secretary to take into account the following:

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.

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.

Notably, the Under Secretary cannot require insurance that is not available on the world market or require any type or amount of insurance that would "unreasonably distort the sales price of the seller's technology."[14] The Final Rule reaffirms this important point by noting that applicants cannot be compelled to self-insure to meet SAFETY Act insurance requirements if insurance is not otherwise available on the world market.

Designation or Certification is valid for a term of five to eight years, as determined by the Under Secretary, and will last the entire term as long as the proper insurance is maintained and the technology is not modified so that it no longer falls within the designation.[15] At any time within the two years prior to the expiration of the term, the seller may apply for a renewal of Designation. The term applies to the period over which the seller can assert that the technology was deployed as a Designated or Certified technology; however, the associated protections apply over the lifetime of the product so deployed. That is, any technology deployed over the term of a SAFETY Act Designation or Certification will be protected for perpetuity provided it hasn't been modified

[14] § 25.5(b)(viii)(2).

[15] Should a technology be modified so that it no longer falls within the designation parameters, a seller must notify DHS with a "Modification Notice." § 25.6(k).

or proper liability coverage no longer exists.

* * * * * *

The SAFETY Act is a necessary and innovative legislative tool for encouraging the development of anti-terrorism technologies. Yet, as noted by Secretary Chertoff, there has not been "enough done to take advantage of this powerful tool to spur new technologies and new systems."[16]

With the modifications in the Final Rule, the Kit, improved processes both by applicants and within DHS, and a better understanding of the tremendous benefits that SAFETY Act Designation and Certification can bring, applications are likely to increase. This could be good news for companies engaged in the security business whether as manufacturers, contractors, service providers or consultants. Hopefully, the promise of this important tool in the fight against terrorism will be more fully realized in the coming months and years.

[16]Speech by Department of Homeland Security Secretary Michael Chertoff to the Commonwealth Club in Santa Clara, Cal. (July 28, 2005).