

THE HOMELAND SECURITY & DEFENSE
BUSINESS COUNCIL

**Why Robust Use of the SAFETY Act is Critical to
Homeland Security & How to Get There**



October 2008

EXECUTIVE BRIEF



The Homeland Security & Defense Business Council would like to thank **Brian Finch** of Dickstein Shapiro for his invaluable work on this important paper. His efforts were critical to this “Executive Brief” and to our SAFETY Act briefing. The Council is grateful for his contribution and for his firm’s co-sponsorship of the event.

The Council would also like to extend our gratitude to **Scott Weber**, Senior Advisor to the Council, former Senior Counselor to Secretary Chertoff of the U.S. Department of Homeland Security, now a Partner with Patton Boggs, for his valuable contributions and insights.

*The **Homeland Security and Defense Business Council** is a non-profit, non-partisan corporate membership organization whose principal representatives are responsible for their companies’ homeland security business units. The Council engages our members and subject matter experts in our members’ organizations to assist in strategic thought leadership, solutions development and program planning. The Council’s work leads to the development and implementation of better and more effective solutions to secure America’s citizens and critical physical and cyber assets. Our members are actively involved in providing the private sector’s voice in determining the strategy and future policy direction of our nation’s homeland security.*

The mission of the Council is to serve as a conduit to help build stronger and more meaningful relationships between senior leadership in the public and private sectors. Our members work together and in concert with government officials and other community leaders invested in providing homeland security solutions to achieve a “culture of preparedness” in our nation.

For more information on the Homeland Security & Defense Business Council, please visit our website at www.homelandcouncil.org

Copyright © 2008 Homeland Security & Defense Business Council. All rights reserved.

Disclaimer: This publication contains general information only and the Homeland Security & Defense Business Council and Dickstein Shapiro LLC are not, by means of this publication, rendering any professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your organization. Before making any decision or taking any action that may affect your organization, you should consult a qualified professional advisor. The Homeland Security & Defense Business Council, its members, related entities, and Dickstein Shapiro shall not be responsible for any loss sustained by any person who relies on this publication.

HOMELAND SECURITY & DEFENSE BUSINESS COUNCIL
EXECUTIVE BRIEF

**Why Robust Use of the SAFETY Act is Critical to Homeland Security
& How to Get There**

EXECUTIVE SUMMARY

The intent of the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (“SAFETY Act” or “Act”) was to incentivize companies to develop, and customers to deploy, anti-terrorist services and technologies without fear of excessive liability in the event an ‘incident’ impacted the customer’s facilities or networks. The Act is a powerful tool that should be better utilized by industry to document and certify anti-terrorism products and services and, in turn, provides organizations with tools and technologies to protect their facilities and operations against attack. The SAFETY Act, coupled with emerging new laws, regulations and other related programs, also provides economic, compliance and, possibly even underwriting protections that directly and indirectly benefit companies that could be affected by terrorism. The Homeland Security & Defense Business Council (“Council”) has prepared this paper to outline the Act’s significance for the private sector – both provider and user of homeland security solutions – as well as to encourage widespread utilization by highlighting complementary legislation and requirements that further support utilization of the SAFETY Act and its protections. Finally, the paper identifies a number of suggested strategies that can be employed to promote and expand the further utilization of the Act. This paper is part of a comprehensive effort by the Council to provide tools, strategies and programs that provide Corporate America with a 360-degree approach to preparedness.

OVERVIEW

Since passage of the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (“SAFETY Act” or “Act”), over 100 “Certifications” have thus far been awarded to companies that have developed “qualified anti-terrorism technologies.”¹ As a result of these companies’ willingness to go through the process, they and their customers are then provided with certain liability protections. Considering the universe of technologies and services applicable to the homeland security community, many believe that countless more companies and technologies eligible and appropriate for DHS certification have chosen *not* to go through the certification process. While experience has shown that there is no lack of companies willing to offer anti-terrorism products and services into the marketplace, many firms remain concerned that the deployment of such technologies could still leave them and their customers exposed to massive liability. The outstanding issue is making these companies more fully aware of the protections

offered by going through the SAFETY Act certification process and bringing those technologies into one's operations.

Unfortunately, legal precedent indicates that lawsuits, such as those emanating from the September 11, 2001 attacks as well as those holding the Port Authority of New York and New Jersey liable for the 1993 World Trade Center attacks, make it all too clear that the litigation environment is most certainly not friendly to providers and users of security services – and provides a tangible economic *disincentive* for companies to offer and implement homeland security technologies.

Congress passed the SAFETY Act in order to help mitigate these concerns, while concurrently encouraging businesses to submit for 'certification' and deploy 'certified' anti-terrorist technologies. The SAFETY Act – included as part of the Homeland Security Act of 2002 – offers unique and valuable protections for providers of products or services that can be used to detect, identify, defend against, or respond to acts of terrorism. The process of having a technology "designated" or "certified" as an anti-terror technology is managed by a highly rigorous official review process at the U.S. Department of Homeland Security ("DHS").

However, despite the many benefits of the SAFETY Act, it remains one of the most underreported and underutilized success stories for DHS and for our nation at large. Even more disturbing is what appears to be a continued misunderstanding regarding the overall purpose and intent of the SAFETY Act in the first place. It is crucial that buyers and sellers of anti-terrorism products and services understand the full potential of the SAFETY Act – not only to protect their enterprise but to assure that our nation has at its disposal the most robust and effective anti-terrorism technologies available.

The Council is strongly committed to broadening industry's understanding of the SAFETY Act so that its protections can be more fully utilized by the private sector. Owners and operators – particularly those in critical infrastructure industries, such as commercial real estate, sporting venues, utilities, transportation, healthcare and financial services – can all benefit greatly from the Act and concomitantly protect their patrons and operations.

I. Brief History of the SAFETY Act

The SAFETY Act was drafted in response to concerns that conducting business in the homeland security market would expose companies to nearly limitless legal liability. This fear was generated in part by a number of lawsuits filed against the airlines, security providers, and facility owners directly impacted by the event of September 11, 2001.² When these lawsuits were filed, defendants moved to dismiss the claims, arguing that the terrorist attacks represented an unforeseeable criminal act that should sever any liability. This defense was previously used successfully in lawsuits stemming from the 1995 Oklahoma City bombing. Defendants in 9/11 lawsuits anticipated that these same defenses would apply, but they did not. The US District Court for the Southern District of New York ruled that the lawsuits emanating from the attacks would not be summarily dismissed and that the claims of the plaintiffs could move forward, ruling that the defendants were “warned” of the threat of terrorism, especially against targets in New York City. As a result, the named defendants “might” be held liable because the attacks were within a class of “foreseeable” hazards.

The court’s decision sent shock waves through the nascent homeland security community. Companies considering entering their product or service in the emerging homeland security market were now faced with the added risk that in the event of another attack they could be held liable for a product or service that was deployed to help deter, detect or prevent terror attacks. As a result, both providers and their customers began to look for ways to deploy anti-terrorist homeland security products and services while also being able to lessen or mitigate their liability. Few safe harbors were found, however.

Given the absence of remedies, and the strong possibility that companies would limit or even stop providing homeland security technologies, Congress decided that the Federal government would have to intervene. After significant deliberation across all sectors, Congress determined that what the market most needed was some form of liability protection to incent and encourage companies to develop and make available innovative, useful anti-terror technologies and services. Thus, the SAFETY Act was introduced and then enacted as part of the Homeland Security Act of 2002.

II. Overview of the SAFETY Act

The SAFETY Act allows firms that manufacture or provide a “qualified anti-terror technology” or “QATT” (which includes both products and services) to apply to the U.S. Department of Homeland Security for protections from civil claims following an “act of terrorism” at a site that has utilized and/or deployed the QATT. Such protections are available only after DHS has thoroughly and confidentially reviewed the seller’s product or service, and then approved the QATT for “designation” or “certification.”

SAFETY ACT PROTECTIONS

The SAFETY Act provides two levels of protection known as “Designation” and “Certification.” A product or service that is “Designated” as a “Qualified Anti-Terrorism Technology” is entitled to a number of benefits, including that:³

- (a) Claims against a Seller of a QATT are capped at an amount no greater than the limits of liability insurance coverage required to be maintained by the Seller (the amount set forth by DHS);
- (b) No punitive damages may be awarded;
- (c) Non-economic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff;
- (d) Any recovery by a plaintiff shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of such “Acts of Terrorism” that result or may result in loss to the Seller; and
- (e) Any and all claims must be brought in Federal court.

A company that qualifies for “Certification” receives all the same protections offered for a “Designated” SAFETY Act technology, plus one critical addition. A QATT “Certified” under the SAFETY Act (also known as being placed on the “Approved Product List”) is entitled to invoke the government contractor defense – a rebuttable presumption that all claims relating to

the technology that arise out of, or relate to, an act of terrorism are to be immediately dismissed. In other words, a technology that has been “Certified” under the SAFETY Act is entitled to a presumption of immunity from civil claims.

It is also important to note that under either a “Designation” or “Certification” the only proper defendant in any civil lawsuit is the seller of the SAFETY Act approved QATT. This functionally means that any entity, other than the seller, that has something to do with the technology (customers, suppliers, subcontractors, etc.) is immune from civil claims arising out of or related to an act of terrorism. For example, if a company purchases and deploys or implements a SAFETY Act-approved technology (whether Designated or Certified) and is sued following an act of terrorism for real property or personal injury damages that are proximately caused by the QATT, the customer also has the right to seek immediate dismissal of the civil claims – a very unique and powerful defense. It also serves as a powerful incentive to acquire and implement the DHS-approved technology as a safeguard to detect, deter and/or prevent an act of terrorism.

SAFETY ACT ELIGIBILITY

Both public and private entities are eligible for SAFETY Act protections. The Act’s incentives were designed to help ensure that our country and its citizens have as many tools as possible to deter and defeat terrorist activities. To achieve SAFETY Act protections, a company must demonstrate that its products or services can in some way deter, defend against, identify, respond to, or mitigate an act of terrorism. The fact that a product or service could be used for purposes other than acts of terrorism will not preclude an award of SAFETY Act protections. For example, cameras or other perimeter security that protect against intruders is also applicable to detecting and preventing acts of terrorism. Even if the product or service is only used in limited circumstances for anti-terror purposes, it could still be eligible for SAFETY Act protections.

Any product or service that has an anti-terror application is eligible for protections under the SAFETY Act. Products and services awarded protections under the SAFETY Act include security guard services, database search programs, advanced video surveillance systems, and biological warfare agent detectors.⁴

SAFETY Act applications are submitted to DHS' Science & Technology Directorate. If a company's product or service does not have all the evidence required for certification, DHS has the authority to alternatively grant a limit on the amount of damages that could be awarded against the applicant – a “Designation” rather than a “Certification.” The company may resubmit its application at any time to increase its level of protection. If the application is denied coverage outright, the company can resubmit another application at any time.

III. Why Increased Utilization of the SAFETY Act is Necessary

Sellers of homeland security anti-terror technologies can only benefit from the unique protections of the SAFETY Act if they apply for protection. Once a company's technology is “designated” or “certified” and then deployed, both the seller and its customers will automatically and immediately receive the benefits and protections offered by the SAFETY Act. A better understanding of that among the private sector will result in wider utilization of the SAFETY Act.

In order to achieve a strong, robust anti-terror deployment of technologies, the Federal government, state and local governments, private industry and the nation at large all have a stake in widespread utilization of the SAFETY Act. The focus of attention regarding implementation should not be on its limiting liability, but rather on encouraging greater and more widespread deployment of technologies that could deter, terrorism and protect our citizens. If the technologies certified by the SAFETY Act are not more fully deployed, and its benefits not better publicized, everyone loses: the nation is left with fewer safeguards, and companies that do develop or deploy such technologies are open to limitless litigation. The Council is committed to increasing the understanding and further deployment of SAFETY Act-approved technologies, and encouraging a strong and responsible SAFETY Act application process that gives confidence in the products and services granted SAFETY Act protections.

Continued and widespread utilization will be enhanced by ensuring that DHS' review process is strong and responsible, but not overly and unnecessarily burdensome to the applicants. Throughout its brief history, the SAFETY Act has seen many peaks and valleys with respect to the amount of effort required to obtain protections. Initially – as could be expected from any

new administrative review process – obtaining SAFETY Act protections was a lengthy and complicated process. Applications languished for months on end, and the level of detail expected by DHS was exceptionally difficult to supply. This led many companies to back away from the SAFETY Act process because the route to these protections was too arduous for the ultimate benefits.

DHS has since revised and streamlined its review process and set in place more formal and reliable review mechanisms. As a result, approval has been granted to a large number of applications, including some innovative anti-terror services like commercial shopping center security guards and professional security certification programs. DHS has continued on this path of a reliable and thorough – but not overly burdensome – review process. This should continue regardless of who is leading the next administration, in part because it is critical to have a review process that establishes a strong presumption of reliability, inspires confidence that the approved product or service truly has a utility against terrorism, and encourages customers to utilize and deploy approved technologies.

The strong and thorough review by DHS benefits industry. Rigorous review under the SAFETY Act assures that the certification is reliable and is not open to challenge. The SAFETY Act review process must be widely perceived as rigorous, thorough and conclusive so that should the utilization or performance of a product or service be challenged, there is a strong review record in place. A comprehensive documentation process will alleviate any review concerns and reinforces the Council's support for the underlying intent and foundation of the federal law – to help ensure the widespread deployment of anti-terrorism products and services.

IV. The SAFETY Act Is An Incentive to Deploy Anti-Terror Technologies

The purpose of the SAFETY Act is to provide an incentive to the private sector to research, develop, deploy and utilize anti-terror technologies to best protect our nation, its citizens and critical assets. The protections under the Act should not be viewed as a liability shield to companies providing homeland security technologies. Congress recognized this when it passed the Act and DHS itself has memorialized the intent in its Notice of Proposed Rulemaking (“NPRM”) for the SAFETY Act. The NPRM stated that the SAFETY Act

“provides incentives for the development and deployment of anti-terrorism technologies by creating a system of ‘risk management’ and a system of ‘litigation management.’”⁵ The NPRM went on to state that the “purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or Sellers of anti-terrorism technologies from developing and commercializing technologies that could save lives. The Act thus creates certain liability limitations for ‘claims arising out of, relating to, or resulting from an act of terrorism’ where qualified antiterrorism technologies have been deployed.”

DHS reaffirmed this position and the urgency associated with the SAFETY Act in its Interim Final Rule⁶ – stating that:

“The Department believes the current development of anti-terrorism technologies has been slowed due to the potential liability risks associated with their development and eventual deployment. In a fully functioning insurance market, technology developers would be able to insure themselves against excessive liability risk; however, the terrorism risk insurance market appears to be in disequilibrium. The attacks of September 11 fundamentally changed the landscape of terrorism insurance.”

DHS went on to add in the June 8, 2006 Final Rule that:

The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of “risk management” and a system of “litigation management.” The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of antiterrorism technologies from developing, deploying, and commercializing technologies that could save lives.

Consistent throughout these iterations of the SAFETY Act is a key concept – the SAFETY Act is an incentive to companies looking to deploy anti-terrorism products or services. There are some who do not fully understand the full intent behind the Act, and have questioned whether the SAFETY Act represented some sort of “gift” to industry, the legislative history as well as the interpretations (and actions) of DHS have conclusively demonstrated otherwise.

Legitimate fears that adequate technologies might not be deployed for fear of exposure to lawsuits led Congress to create the SAFETY Act, and the reliance of industry that it would provide viable and effective mechanisms for controlling liability.

It is important for all stakeholders to recognize that the SAFETY Act is an incentive to develop, deploy and use the most advanced and necessary technologies to help in the fight against terrorism.

V. Laws and Programs Complementary to the SAFETY Act

Numerous other initiatives have been enacted designed either to increase preparedness against terrorist threats or to force corporate America to better disclose risks and mitigate liability. The SAFETY Act can play a critical part in supplementing, augmenting or enhancing these laws and programs.

TITLE IX – 9/11 LEGISLATION

Title IX of Public Law 110-53 (better known as the 9/11 Legislation), sets forth certain business continuity requirements to be carried out by DHS. Through the requirements of Title IX, DHS must create an “Accreditation and Certification Program” for private sector preparedness that provides businesses and organizations to increase the resilience of the private sector and to strengthen preparedness, response, recovery, and the ability to continue operations in the event of a terrorist attack.

In July the U.S. Department of Homeland Security selected, and signed an agreement with the ANSI-ASQ Accreditation Board (ANAB) to administer the accreditation and certification of businesses under the “Voluntary Private Sector Preparedness Accreditation and Certification Program.” Recommended by the 9/11 Commission and authorized by the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53),⁷ the program seeks to “enhance nationwide resilience in an all hazards environment by improving private sector preparedness. Participation in the program will be voluntary and intended to be driven by the marketplace.”⁸

The new program is directed by the Federal Emergency Management Agency (FEMA) Administrator who is responsible for the Voluntary Standards program and Chairs an internal “Private Sector Preparedness Council” made up of leadership from the Science & Technology Directorate, Private Sector Office, and the Office of Infrastructure Protection. The council will select program standards, define and promote the business case for private sector entities to work toward voluntary certification. The program will allow “private sector organizations to demonstrate through formal certification their compliance with voluntary preparedness and business continuity standards and requirements.”

While this accreditation process is “voluntary” under the law, its mere existence creates an unmistakable appearance of a standard of care that the private sector cannot ignore. This is particularly true since the program “shall assess whether a private sector entity complies with voluntary preparedness standards.”

Private sector entities are likely to feel compelled to go through this voluntary process, even though it may or may not serve to verify that they are prepared for a terrorist event or shield them from challenges that they were indeed unprepared. SAFETY Act protections for complying with the voluntary standards, or utilizing SAFETY Act approved technologies to comply with any standards established could serve to mitigate such concerns. By using the SAFETY Act to comply with Title IX standards, companies can achieve some measure of confidence that they will have some tangible liability protection even though the standards were voluntary.

SARBANES-OXLEY

Certain sections of Sarbanes-Oxley could be interpreted as complementary to SAFETY Act protections. The Sarbanes-Oxley Act of 2002 was enacted to enhance responsible corporate governance practices and to facilitate disclosure to investors. A company utilizing SAFETY Act approved technologies could well be meeting requirements established under the Sarbanes-Oxley law.

For instance, the language contained in §409 of Sarbanes-Oxley governs real time issuer disclosures, requiring each reporting company to disclose to the public on a “rapid and current

basis” additional information concerning material changes in the financial condition or operations of the issuer in plain English. The expansive language in §409 could possibly trigger an obligation to report a company’s actions (or lack thereof) with respect to implementing SAFETY Act technologies. If a company was on notice that there was a heightened risk of liability associated with the use of or access to its facility or network, for example, it might have the duty and want to report new developments with respect to the implementation of QATTs in their operation.

BUSINESS JUDGMENT RULE

The SAFETY Act can also help directors and officers satisfy the duty of care owed to shareholders. When considering what steps a company must undertake in a particular area – e.g., ensuring the security and safety of a company’s assets, employees, etc. – typically the “business judgment rule” serves as the benchmark against which to evaluate the actions of company’s directors and officers. That rule operates as a presumption that in making business decisions, the directors and officers of a corporation acted on an informed basis, in good faith, and in the honest and reasonable belief that decisions were made in the best interests of the company. Given the powerful protections of the SAFETY Act and the publicly available information identifying QATTs, it is likely that under the “business judgment rule,” the failure to consider and where appropriate use QATTs, could subject directors and officers to personal liability if an act of terrorism that resulted in damage could have been prevented or mitigated by a QATT.

This is particularly true as the risk management industry becomes more sophisticated about the SAFETY Act. Many insurance companies are now starting to adjust premiums to reflect the receipt of SAFETY Act protections. As insurance companies and their underwriters assign greater tangible value to the SAFETY Act certification, there should be a parallel increase in the urgency to pursue such protections.

These few examples provide a snapshot of the many laws and programs that complement the protections offered by the SAFETY Act. They illustrate that as companies comply with corporate requirements in such areas as preparedness or disclosure requirements, the SAFETY Act certification serves to protect them, their customers and their shareholders.

VI. Missed Opportunities: Creative Applications of the Act

The benefits from the SAFETY Act are tangible – and the consequences for entities that do not avail themselves of those benefits are severe. A recent decision by a New York court,⁹ held that the Port Authority of New York and New Jersey was liable for damages resulting from the 1993 World Trade Center bombing – a dramatic and costly example of what can happen when terrorists strike and insufficient liability protections are not in place.

The circumstances surrounding the underlying case are well known: On February 26, 1993, a small number of terrorists drove a rental moving van loaded with fertilizer-based explosives into the public parking area of the World Trade Center, lit a time-delay fuse and left. The subsequent explosion created a crater six stories deep, killed six people, and injured hundreds more.

The evidence at trial focused on the level of security screening at the World Trade Center and the fact that the Port Authority ignored two security vulnerability assessments that were conducted in 1985 and 1986. Those studies, prepared by outside consultants, warned of the potential for the very scenario that occurred during the February 1993 attack. Based on that, and other information, the defendants were found liable for damages suffered as a result of the terrorist attack.

The decision to sustain the verdict against the defendants turned in part on two critical issues: (1) whether the defendant was on notice of the possibility of such an attack; and (2) what steps were reasonable or necessary to mitigate the consequences of such an attack in light of that knowledge.

On the issue of notice, the law previously required actual notice of the possibility of an attack, satisfied by such facts as a previous attack at the same facility. The trial record established that, in 1993, there “had been no remotely comparable precedent event” at the World Trade Center. However, the Court sustained the verdict against the defendant by finding that “notice” of potential terrorist attacks was the appropriate standard to apply. The Court added that “notice” occurs when a defendant knew or should have known that a terrorist attack was possible.

Under the “should have known” standard, facility owners now face the unenviable task of deciding whether they are “on notice” of the possibility of terrorist events taking place at their property. In the post-September 11 environment, a facility owner may be charged with knowledge of all of the information that is available through law enforcement and private sector intelligence entities, and through vulnerability assessment experts. Given that the Court indicated that notice can occur when an owner is or “should be” aware of a threat, the owner must reach out and determine what information a reasonable investigation will uncover, and a jury could consider, as to what knowledge the owner should be charged with. Ignorance of an actual threat is not a reliable defense.

Assuming notice, the next question becomes what steps must be undertaken in light of that threat. The Court made it clear that “reasonable” mitigation steps could be ones that were previously considered “burdensome,” and that the Court could readily foresee circumstances where even the most stringent of mitigation measures suggested in the course of a vulnerability assessment would be considered reasonable. This means that facility owners may now face the very real possibility of having to take fairly burdensome measures to satisfy a reasonable standard of care.

Most alarming is that there are no assurances that any actions taken will be considered “reasonable.” Even if the steps taken were in adherence with carefully crafted voluntary standards or best practices, the New York decision certainly leaves open the possibility that such actions will be insufficient.

That level of uncertainty leaves many in an unacceptable position. Application of the SAFETY Act, however, avails owners of some tangible remedies to lessen their potential liability. Companies that adhere to any voluntary standards or best practices should fully explore whether they can take advantage of the unique liability protections offered by the SAFETY Act. Entities that adhere to voluntary standards or best practices that have been protected under the SAFETY Act would automatically be entitled to some liability protections. Companies could also present to DHS how they specifically have followed the voluntary standards or best practices and ask that they receive SAFETY Act protections for doing so.

Through those steps and others, the SAFETY Act can ameliorate the great level of uncertainty fueled by the recent decision in New York, especially as related to determining whether “reasonable” mitigation steps were undertaken. Doing so will help provide some concrete advantages to adhering to voluntary standards or best practices that might otherwise be deemed inadequate during litigation.

INTERNATIONAL APPLICABILITY

Although the SAFETY Act provides many benefits – there is still room for improvement. For instance, some have expressed concern about how strong the protections of the SAFETY Act are if an act of terrorism occurs overseas. The SAFETY Act certainly applies to US property attacked overseas, and DHS has also strongly stated in its regulations that if an attack overseas impacts the United States (including if the impact is financial), the SAFETY Act will also apply. More should be done, however, to solidify the position on the international applicability the SAFETY Act set forth by DHS. Steps that can be taken include pursuit of protections similar to the SAFETY Act in foreign nations or encouraging foreign nations to formally recognize the applicability of the SAFETY Act for acts of terrorism occurring on their territory. Such steps are critical, particularly given that many terrorist attacks overseas are impacting US businesses and interests. As a result, there should be serious consideration given to widening the international applicability of the SAFETY Act.

VII. Increasing the Reach of the Act

It is often said that an ounce of prevention is worth a pound of cure. The Homeland Security & Defense Business Council is committed to ensuring that the benefits of the SAFETY Act are broadly utilized by providers and customers alike. More companies that go through the ‘certification’ process and more widespread deployment of QATTs in businesses throughout the country will further encourage the development and deployment of the latest anti-terror technologies and to facilitate a responsible corporate approach to risk management. Recent legislative trends indicate that voluntary and mandatory initiatives employed by the private sector that incorporate a greater degree of “preparedness” beyond the traditional understanding of physical protection and business continuity could stave off mandates. “Preparedness” must

filter through from a corporation's emergency response plan, through the mitigation of business and legal impacts as a result of a terrorist or other event that causes a business disruption. The tools and mechanisms are at corporate America's disposal and the Council wants to ensure that corporations are fully aware of the legal protections offered by the SAFETY Act, other initiatives and basic common sense preparedness in the workplace.

This Executive Brief, the first in a series of papers taking a critical, detailed look at initiatives relevant to the private sector, is part of a comprehensive effort by the Homeland Security & Defense Business Council to provide corporate America with a 360-degree perspective on preparedness. The SAFETY Act is an important place to start because of its implications both for the providers of anti-terror technologies and their customers. It adds tremendous value to all private and public sector actors engaged in the homeland security industry. Corporations that do not utilize the protections under the Act may suffer incalculable losses in the event of another attack – losses that neither they, nor the homeland security industry in general -- can afford.

VIII. CONCLUSION

The SAFETY Act is powerful tool, and one that is as useful as ever. Companies that develop and/or deploy QATTs have at their disposal a unique method to mitigate their liability. Just as important, DHS-approved technologies help ensure that the country and its citizens have as many tools as possible to fight against terrorism. More fully utilizing the SAFETY Act for such purposes is precisely how Congress intended the program to be run – as an *incentive* to industry to make sure that our arsenal of homeland security products and services is robust. In order to maximize the utility of this important tool, industry must work hard to ensure that it provides solid technologies capable of meeting the DHS requirements for SAFETY Act protections and companies must continue to implement the technologies that have gone through the rigorous 'designation' and 'certification' processes. Concurrently, industry should use the Act to protect "outside the box" applications in such areas as financial services and cyber security products as well as for compliance with voluntary standards.

With such work, the SAFETY Act will continue to grow and become an ingrained and key part of the nation's homeland security efforts.

¹ www.safetyact.gov

² In re September 11 Litigation, 280 F.Supp.2d 279 (S.D.N.Y. 2003).

³ 2002. Homeland Security Subtitle G of Title VIII of the Homeland Security Act of 2002 The Support Anti-terrorism by Fostering Effective Technologies Act of 2002, also known as The SAFETY Act.

<https://www.safetyact.gov/DHS/SActHome.nsf/HomeTop?ReadForm#> (accessed October 7, 2008).

⁴ A list of approved QATTS can be found at www.safetyact.gov.

⁵ Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the Safety Act), 68 Fed. Reg. 133 (proposed July 11, 2003) (to be codified at 6 C.F.R. pt. 25).

⁶ http://www.dhs.gov/xabout/laws/editorial_0878.shtm

⁷ Public Law 110-53, August 3, 2007: "Implementing Recommendations of the 9/11 Commission Act of 2007." Section 524: Voluntary Private Sector Preparedness Accreditation and Certification Program.

http://www.ise.gov/docs/nsis/Implementing911_Act.pdf

⁸ U.S. Department of Homeland Security: "DHS Selects ANSI-ASQ National Accreditation Board to Support Voluntary Private Sector Preparedness Certification Program." July 30, 2008, DHS Release Number: FNF-08-068.

<http://www.fema.gov/news/newsrelease.fema?id+45288>

⁹ Nash v. Port Auth. of N.Y. & N.J., 856 N.Y.S.2d 583 (1st Dep't, 2008).