

Statement for the Record of Brian E. Finch, Esq.

Partner, Dickstein Shapiro LLP

**Hearing: “Unlocking the SAFETY Act’s Potential to
Promote Technology and Combat Terrorism”**

Before the United States House of Representatives

Committee on Homeland Security

**Subcommittee on Cybersecurity, Infrastructure Protection,
and Security Technologies**

Washington, DC

May 26, 2011

I. Introduction

Chairman Lungren, Vice Chairman Walberg, Ranking Member Clarke, and distinguished Members of the Subcommittee, it is an honor to appear before you to discuss the current implementation of the Support Anti-Terrorism by Fostering Effective Technologies (“SAFETY”) Act by the Science and Technology Directorate of the Department of Homeland Security (“DHS”). I will also discuss how the SAFETY Act can be utilized so that its full potential is reached both by DHS and the private sector.

Since the SAFETY Act was enacted nearly 9 years ago, it has become - relatively speaking - one of the most successful programs managed by DHS. Without the liability protections offered by the SAFETY Act, numerous critical products and services would not be in the marketplace, defending American citizens and property. Moreover, the intrinsic value of the SAFETY Act and its liability protections is easily demonstrated by the numerous customers of anti-terrorism products and services that strongly encourage – or even require – that the anti-terror tools they purchase must have SAFETY Act protections. One cannot step into an airport, public building,

stadium, or commercial shopping centers without likely encountering a SAFETY Act Designated or Certified product or service.

Still, objectively speaking, much remains to be done in order to make the SAFETY Act an absolute success. While several hundred products and services have received a Designation or Certification, that number in reality should be in the thousands. For a variety of reasons I will detail, too many products and services that remain on the sidelines of the SAFETY Act process. Through my remarks today I will detail why the SAFETY Act is so critical to the security of the nation, as well as offer some suggestions on ways the implementation of the SAFETY Act can be improved so that it will be viewed as an unqualified success.

I will also state up front that not much needs to be done to turn the SAFETY Act into a true success. The statutory and regulatory language governing the SAFETY Act is robust and well developed. It arms DHS with the broad authority to rapidly and effectively process applications, and sets up a framework to inspire confidence in that review. Key then to fully unlocking the SAFETY Act is to make certain that the original intent of the SAFETY Act is honored and the program is implemented in a way that is transparent, consistent, and ensures accountability for DHS in its management of the program.

I would also be remiss if I did not mention that the SAFETY Act is perhaps the most critical program administered by the Science & Technology Directorate of DHS. If the Science & Technology Directorate is truly going to encourage the deployment of technologies to combat terrorism, it must continue to expend the resources necessary to make the SAFETY Act a priority. This hearing is absolutely essential then, because if the Science and Technology Directorate gets only one thing right, it has to be the SAFETY Act. Without a successful SAFETY Act program in its portfolio, it will have lost a large amount of credibility with the private sector and will have failed in executing one of its core missions as defined by the Homeland Security Act of 2002.

II. Why The SAFETY Act Is Still A Critical Incentive For The Deployment of Anti-Terrorism Technologies

The motivation for the SAFETY Act being included in the Homeland Security Act of 2002 could not be clearer. At that time the country was still reeling from the devastating attacks of September 11, 2001. Buildings had to be rebuilt, wounds had to be heeled, and the nation was struggling to determine how best to prepare to defend against or respond to future terrorist attacks. Even when DHS was stood up, it was still going to have limited authority and resources to develop and deliver security solutions. Ultimately then, the nation was going to have to depend on solutions developed and deployed by the private sector to protect itself from terrorist threats.

The private sector was well aware of the demands placed on it, and its representatives were eager to help provide the tools needed to stop another terrorist attack. Given the size and scope of the destruction caused in the September 11 attacks, however, companies were forced to reflect on the significant liability that could follow a terrorist attack. Such concerns reached the point that makers of anti-terrorism technologies began to seriously consider whether they could deploy

existing or possible solutions. After all, a few thousand dollars earned on a risk assessment paled in comparison to the untold millions of dollars in costs that could arise from a court finding that their work was inadequate, and thus are responsible for the damages suffered in a terrorist attack.

The risk mitigation options available to anti-terror solution providers were few and generally inadequate: insurance – especially immediately after September 11, was sparsely available and uncertain in its coverage, indemnification from customers was also rarely available, and only served to shift risk, and government bailouts in the event of another act of terrorism were considered highly unlikely. In light of this list of undesirable alternatives, Congress was faced with the stark choice of either allowing the anti-terror solution market to sink to an unacceptably small size or to take proactive measures to mitigate liability. Congress, in its wisdom, chose to offer liability protections in the form of the SAFETY Act. In other terms in the battle between preserving opportunities for massive litigation or pushing out solutions that would prevent terrorists from attacking, Congress chose the latter by creating the SAFETY Act.

One would have hoped the intervening years would have served to lessen concerns about crushing liability from terrorist events. Unfortunately, the legal landscape for providers of anti-terror solutions has become even more fraught with danger. Perhaps the most troubling development was the decision related to the liability of the Port Authority of New York and New Jersey arising from the 1993 attack on the World Trade Center. In 2008, a New York appellate court upheld the liability of the Port Authority for injuries and deaths resulting from that attack. That decision set a dangerous precedent that gave pause to companies throughout the United States.

Specifically, the New York courts created a whole new standard of liability under which it would be difficult - if not impossible - for defendants to avoid liability after a terrorist attack. The court found that if defendants knew or should have been aware that they were under threat from a terrorist attack, they must then take “reasonable” steps to mitigate the potential for a terrorist event.

Under the “knew or should have been aware” 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. This presents endless opportunities for plaintiffs to establish that a defendant should have been aware of terrorist threats. Even something as seemingly innocent as the provision of extra anti-terrorism funding for the geographic region the defendant resides in could satisfy this notice requirement.

Once notice has been established, a defendant then must undertake “reasonable” steps to mitigate a potential terrorist attack. While a seemingly common sense requirement on its face, the devil here is in the details. The Court made it clear that “reasonable” mitigation steps could be ones that were more burdensome than anything the defendant had previously considered, and could go all the way up to situations where a defendant had to enact even the most stringent security recommendations provided to it. The end result of this decision is that now potential terrorist targets have no assurance that any measure they offer or seek to implement will be considered “reasonable,” and thus the door to liability is far too open for anyone’s comfort. And, let’s not forget that all this stemmed from a decision where it was held that the Port Authority was held

two-thirds liable for the death and destruction caused by terrorists, leaving the one-third to others - including the terrorists themselves.

Liability concerns do not end there, however. Far from it. Additional events have shown that when it comes time for litigation following a terrorist attack, security providers will inevitably be the ones to have their pockets turned inside out. Consider this reasonable proposition for a moment: why not seek recovery from the terrorists? After all, they were the ones who committed these terrible events. The simple answer is that holding a terrorist accountable in a civil lawsuit has a very low probability of success. Suits have been filed against terrorists and their sponsors, and inevitably fail because – to no one’s great surprise – the terrorists chose not to respond to the complaints. The litigation did not even proceed to answering fundamental process questions: as of right now there is only one group with a proven record of tracking down terrorists, and I feel confident in noting that US Navy Seals are not available to serve civil action complaints.

Even in the rare cases where litigation proceeds without the presence of defendants, recovery is still essentially impossible. Successful litigation against state sponsors of terrorism, where billions of dollars have been awarded to plaintiffs, still remains an abstract process with little chance for realistic recovery. Even the presiding judges admit that such victories are symbolic as the sponsors are usually estranged from the U.S., deny responsibility for the attack anyway, and once again chose not to respond to the lawsuit.

Finally, there are these simple facts: civil litigation following terrorist attacks will happen, it will be lengthy, and it will be extraordinarily expensive. A survey was conducted a few years back of persons who were eligible to participate in the 9/11 victims compensation fund or actually did so. Out of that survey came some salient points, including:

- Many people who took payments from the fund stated that if they could do it again, they would have elected to not waive their rights and instead would have sued. Several stated that they felt “dirty” after taking the money;
- Families who chose to sue various companies whose products were involved in the 9/11 attacks viewed the Compensation Fund as “hush money.” Some participants went so far as to say that “People were being paid off not to go to court”; and
- Those same people viewed litigation as a way to get accountability. Some noted that “What I’m looking for is justice ... someone held accountable ... there are people who did not do their job.”

Not in that survey, but well known is that the defendants have been forced to spend hundreds of millions of dollars to defend themselves from claims that most would agree will likely be denied at the end of the day.

Thus, the totality of that situation then is as follows: the civil liability environment for providers of anti-terrorism products and services is far more toxic than ever; dangerous standards of care are being established; and expensive and protracted litigation following a terrorist attack – against the people who tried to stop the attack, mind you – is now a virtual certainty. Therefore the need for the effective and efficient implementation of the SAFETY Act is greater than ever.

III. Improvements In The SAFETY Act Application And Decision-Making Process

A. *The original intent of the SAFETY Act should be followed*

Given the realistic possibility of ruinous litigation following a terrorist attack, the question then becomes how best can the SAFETY Act (which represents the only realistic solution to that threat) be implemented to mitigate such events? As is clear from the statute and its implementing regulations, the purpose of the SAFETY Act is to preempt such litigation following a thorough, meaningful, but not unduly burdensome review of how the given technology works and is to be deployed. The Department itself stated in the Preamble to the Final Rule that “[t]he purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers anti-terrorism technologies from developing, deploying, and commercializing technologies from saving lives.” 71 Fed. Reg. 33,147, 33,148 (June 8, 2006). The Department even took an unassailable position on its view of the intended purpose of the SAFETY Act, stating that:

“Congress was clear, both in the text of the SAFETY Act and in the Act’s legislative history, that the SAFETY Act can and should be a critical tool in expanding the creation, proliferation, and use of anti-terrorism technologies.”

71 Fed. Reg. at 33,147.

If the SAFETY Act is to succeed, the Department needs to fully commit to implementing the Act in a manner consistent with its own interpretation of its intent. This would include ensuring that all technologies, whether novel or commonplace can obtain SAFETY Act protections so long as it can be shown that they have some type of utility in deterring, defending against, responding to, or mitigating acts of terrorism.

This requires a commitment from DHS in several areas. First, the Department should work to try and have each application approved. This would require the Department adopting a policy of presuming that each application it receives merits approval. While this might sound like an obvious policy, at times there has been a sense that applications are presumptively denied unless an applicant can build a strong case for approval. Right or wrong that perception has existed, and it has acted as a disincentive for potential and current applicants as well as for current applicants. DHS should understand that the Act as written favors approvals, and that Congressional intent in this area has not changed at all. Obviously there will be applications that simply will not merit SAFETY Act protections, but there should also not be a perception that obtaining SAFETY Act protections for proven technologies will involve a long and arduous review process.

Second, the Department should actively encourage applications of all sorts, not just those for technologies that have been through some form of Federal vetting or procurement process. At times there has been a sense that an application only has a fair chance of success if it has been

thoroughly vetted or deployed by the Federal government. In part, that sense has stemmed from the concern that often times the Department will essentially rely only on very specific efficacy data collected from customers. Typically that data does not exist for commercial deployments, and so applicants are left scrambling to assemble it, or have a difficult time collecting it from their government customers. DHS needs to work collaboratively with applicants to help them determine what information is needed, and also appreciate what can realistically be collected. This would include DHS gaining a realistic sense of how data is kept by businesses, and taking the position that the absence of information that would normally be collected during a procurement is not a barrier to SAFETY Act protections.

Third, DHS should recall that Congress put in its hands a powerful liability management tool with the intent of the Department approving a large variety of applications. Too often applicants have walked away with the impression that the SAFETY Act process is reserved for products with a proven track record. Companies that deploy security-related services in particular have felt that the process is too oriented towards products, and companies that deploy technologies to risky areas – especially overseas – have expressed concern that DHS has a greater hesitancy to approve such precedent setting applications.

The attitude should be the exact opposite. DHS should manage the SAFETY Act with relatively few boundaries on what can be approved. By way of example, applications for products or services that protect sports facilities or hospitality chains, provide compliance with security regulations, protect Americans and other innocent persons outside U.S. borders, or otherwise protect against terrorism in some way shape or form should all be eligible for approval. This attitude would be far more reflective of the intent of the SAFETY Act, which is to ensure the widespread deployment of anti-terrorism technologies.

B. *Greater focus should be placed on transparency, consistency, and accountability*

From a process oriented perspective, DHS has gone through periods where the application process was smooth, predictable, and resulted in a “customer friendly” experience. At other times, some would say that the Department has moved away from such an experience. I am certain that Members of this Committee and others have heard complaints to that effect.

In order to combat such concerns – whether real or otherwise - I would propose some simple solutions that will go far in creating a smooth and robust SAFETY Act application process. The key theme for these suggestions is to have an application process where applicants know that they will be working with DHS in a collaborative manner toward the common goal of getting the application approved.

First, DHS should aim to significantly increase transparency related to the SAFETY Act application process. Too often applicants face a guessing game as to what is required of them in order to successfully navigate the SAFETY Act application process. Even if a company is familiar with the application process, each time a new application is submitted they potentially face a path with many twists and turns. This leads to great frustration among applicants as they have undoubtedly invested significant time and effort in their application, yet they are simply

told in return that there are numerous pieces of missing information to be presented before DHS will even review the application.

A key note for the Committee to remember is that often takes two or three tries before DHS accepts an application for formal review. As the Committee is surely aware, DHS will not conduct a substantive review of an application unless it finds that it is “administratively complete.” Apparent, the threshold for an application being complete is that there is enough information provided so that the Department believes it can complete its full review and render a decision within the next 90 days.

While this may not seem like a significant obstacle, it truly is a painstaking and time consuming process. Companies will put together application packets consisting of nearly 100 pages of text, backed up by dozens of supplemental exhibits and references from numerous customers. Far too often, despite all that work, the application is deemed “incomplete,” and the applicant must go back and start the application process over again. This is terribly frustrating to applicants, and I can tell you from personal experience that it gives companies serious pause as to whether they would like to resubmit an application.

Even after an application is found to be complete, companies are still regularly asked for large amounts of information. While it is natural for DHS to request follow up information related to the application, these requests are often lengthy, and explore areas not always relevant to the application’s subject matter.

With that in mind, the health of the SAFETY Act would benefit from much greater transparency on the part of DHS. The SAFETY Act should not be administered like a closed book exam, with little to no guidance as to what information the teachers are seeking. Instead, the application process should be administered in a way that encourages an active dialogue between applicant and reviewer, where each party understands exactly what the other is looking for and they work together to develop acceptable answers. Moreover, if there is a change in the expectations of DHS, that should be made clear to the applicant as quickly as possible. Too often standards shift as an application proceeds through review, making an already stressful situation even more difficult. Fundamental to all this, however, is DHS maintaining clear lines of communications with applicants about expectations. Building such a partnership will go a long way to improving the health of the Act.

A second needed area of progress for the SAFETY Act relates to consistency. One of the most frustrating elements for SAFETY Act applicants is the apparent disparate treatment various applicants receive. Concerns have been expressed over the years that the success of an application depends as much on when the application was submitted as it does on the substance included. Companies in particular have expressed frustration that similarly situated companies have received SAFETY Act protections while they have struggled to eke out even the smallest of protections through the approval process.

Such concerns are more than academic. Acceptance of the SAFETY Act among customers has reached the point where holding SAFETY Act credentials is critical to earning or keeping security-related business. Because of such competitive concerns, it is vital that applicants know

that they will not unnecessarily be subjected to a higher standard of review than other applicants. Closer scrutiny for similarly-themed applications should occur in situations where it is clearly merited, such as where it is obvious that the applicant has repeatedly had material performance issues. Even then DHS should only look to see if the applicant has demonstrated its ability to be useful and effective against terrorist acts, and should not look to create some sort of higher threshold of proof for their application.

The renewal phase of the SAFETY Act process also lacks consistency. As a reminder, SAFETY Act protections must be renewed periodically, typically every 5 years. The renewal process was created to ensure that technologies continue to be effective and useful against terrorism. At times, unfortunately, the process has turned into something akin to a *de novo* review, requiring applicants to essentially start from scratch with respect to proving the merits of their application. I have seen levels of protection fall from Certification to Designation, or even SAFETY Act protections being rescinded. Such changes in protection are difficult to understand, particularly when the applicant has done nothing that could be considered as negatively impacting the usefulness or effectiveness of their technology. It only seems appropriate then that renewal applications as well should not be subjected to constantly shifting review standards.

One other critical point to emphasize with respect to the implementation of the SAFETY Act is that there should be a degree of accountability with respect to the approval process. By this, I mean that it should be obvious to an applicant who is establishing the criteria for approving an application, and that these criteria are the ones being utilized in the actual review.

Many times it is unclear to an applicant who is actually making decisions as to the standards being utilized or metrics that must be met before an application will be approved. While it is well known that the Office of SAFETY Act Implementation is charged with conducting a substantive review of an application, it is not clear who is establishing the metrics used to determine whether the application will be approved. Similarly it is unclear whether there is a mechanism in place that will ensure that those metrics are being followed, or if they are deviated from that there is a compelling reason for doing so.

Establishing a level of accountability in the SAFETY Act process, particularly one that is visible to the applicant community, is therefore critical. Applicants need to understand who ultimately is making decisions about applications, and have a level of assurance that decisions are not being made simply based on administrative records developed through unconstrained fact finding. Just as importantly, everyone – including Congress – would benefit from knowing who ultimately is setting the requirements for approval. By knowing who is in charge of that process, there can be one central point of contact for determining whether that person has set metrics that are reasonable and consistent with the original intent of the SAFETY Act. And this will also work to the benefit of DHS, as it will allow both the private sector and Congress both to know who they need to interface with in order to make sure that all parties are on the same page with respect to how the Act should be implemented.

One last point with respect to the implementation of the SAFETY Act is that the end goal of any review should be the Certification of the technology. As time has passed, Certifications under the SAFETY Act have become less common. Whatever the reason, it is sufficient to say that this

trend should be reversed immediately. Awarding Certifications is an important signal that the technology is useful and effective. Certification awards also signal that the Department fully believes in the purpose of the SAFETY Act, namely that the threat of liability should be eliminated. While there are certainly cases where a Designation is merited, the Department should be working with applicants to find ways to move an approval to the level of Certification.

III. Conclusion

The threat from terrorism has not gone away nor, sadly, is it likely to go away any time soon. Given that ever present threat, it is absolutely vital that DHS take every step possible to help ensure the safety of American lives, infrastructure, and treasure. Acknowledging the limited budgets facing our government, now more than ever DHS must do what it can to incentivize the private sector to develop and fully deploy anti-terror solutions. At this time, the best way it can do so is by unleashing the fantastic potential contained within the SAFETY Act. In terms of the most effective way to immediately transition technologies into the hands of the private sector and ensure that they are used, the SAFETY Act is the greatest resource DHS has at its disposal.

Using that resource will help promote some of the highest priority areas for DHS, including matters this Committee has jurisdiction over such as Chemical Facility Anti-Terrorism Standards and cyber security, where DHS should be making active links to expedite SAFETY Act protections. Most of all, I would urge DHS, this Committee, and the private sector to come together so that a revitalized program can emerge, one that is transparent, consistent, and imbued with accountability. There are so many solutions that should be wearing a badge of SAFETY Act approval but do not as of yet. That can only happen if DHS fully supports the SAFETY Act and embraces the original intent of Congress, specifically that this is a program intended to fully support the deployment of useful and effective technologies.

I thank the Committee for the opportunity to testify and will be happy to take any questions at this time.