AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

UNLOCKING THE SAFETY ACT'S POTENTIAL TO PROMOTE TECHNOLOGY AND COMBAT TERRORISM

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 26, 2011

Serial No. 112–26

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

72–236 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
MO BROOKS, Alabama

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
VACANCY
VACANCY

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

DANIEL E. LUNGREN, California, *Chairman*

MICHAEL T. MCCAUL, Texas
TIM WALBERG, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
BILLY LONG, Missouri
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

COLEY C. O'BRIEN, *Staff Director*
ALAN CARROLL, *Subcommittee Clerk*
CHRIS SCHEPIS, *Minority Senior Professional Staff Member*

CONTENTS

Page

STATEMENTS

The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies 1
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security 3

WITNESSES

PANEL I

Mr. Paul Benda, Acting Deputy Under Secretary, Science and Technology Directorate, Department of Homeland Security:
Oral Statement 4
Prepared Statement 7

PANEL II

Mr. Marc A. Pearl, President and Chief Executive Officer, Homeland Security and Defense Business Council:
Oral Statement 17
Prepared Statement 19
Mr. Brian E. Finch, Partner, Dickstein Shapiro, LLP:
Oral Statement 22
Prepared Statement 24
Mr. Scott Boylan, Vice President and General Counsel, Morpho Detection, Inc.:
Oral Statement 29
Prepared Statement 31
Mr. Craig A. Harvey, Chief Operations Officer and Executive Vice President, NVision Solutions, Inc.:
Oral Statement 34
Prepared Statement 35

UNLOCKING THE SAFETY ACT'S POTENTIAL TO PROMOTE TECHNOLOGY AND COMBAT TERRORISM

Thursday, May 26, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:07 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, Marino, Clarke, Richardson, and Richmond.

Mr. LUNGREN. With the permission of the Ranking Member of the full committee, we are going to start this. We have votes scheduled in about an hour and a half, so I would like to see if we can get both panels done, because I understand we are going to have a long series of votes.

So the Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittee is meeting today to examine the Department of Homeland Security's implementation of the Support Antiterrorism by Fostering Effective Technology, or SAFETY Act. I will begin by recognizing myself for 5 minutes or less.

I want to welcome our witnesses this morning and thank you for your time and effort to assist our subcommittee's oversight efforts. I consider the Support Antiterrorism by Fostering Effective Technology Act, more commonly referred to as the SAFETY Act, a vital Government program in the fight against terrorism.

New companies who are developing and deploying antiterrorism products and services are justifiably concerned that these technologies could leave them and their customers exposed to enormous civil liabilities. Legal precedents such as those emanating from the 9/11 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 clear that civil litigation can intimidate the developers and users of security technologies and services after a terrorist event.

So Congress acted decisively to address this concern by passing the SAFETY Act as part of the Homeland Security Act of 2002. SAFETY Act is intended to encourage the development and deployment of antiterrorism technologies by limiting the liability of sell-

ers of the technology for third-party claims arising out of an act of terrorism where the technology has been deployed to prevent, respond to, or recover from such an act.

It is meant not only to protect technology providers, but also businesses and facilities using them and to encourage people to use them before the fact. After 8 years, 440 technologies have been SAFETY Act-approved.

Initially, in my judgment, the program suffered from poor performance—that is, low number of applications, slow processing times because of lack of awareness of the protections and risk management benefits offered by the SAFETY Act and a burdensome application process.

In 2006 the final rule was issued, and DHS made changes to streamline the application and review processes, which temporarily improved the SAFETY Act results. However, I see some troubling signs the implementation is again stalled with SAFETY Act certifications well below expectations.

I find these statistics concerning. The number and percentage of SAFETY Act awards have decreased from 58 awards out of 70 applications in fiscal year 2006 to 40 awards out of 121 applications in fiscal year 2010. That is an approval rating going from 83 percent to 33 percent.

The number and percentage of SAFETY Act certifications specifically has drastically plummeted from 31 certifications over 70 applications in fiscal year 2006 to one certification out of 117 applications in fiscal year 2010, although I understand this percentage may improve slightly as DHS is still reviewing some of the fiscal year 2010 applications.

Counter to expectations for fast processing times for renewals, the average time it takes to process a renewal, I am informed, is essentially equivalent to the time it takes to process a new application—that is, both approximately 120 days.

The number of companies seeking SAFETY Act renewal for previously SAFETY Act-approved technology appears to be significantly below expectations—that is, less than half. Of the companies seeking renewal, less than—have been successful and been granted continued SAFETY Act award status.

The percent completeness of an application upon submission has dropped from 59 percent in fiscal year 2006 to 24 percent in fiscal year 2010, a 41 percent decrease. This translates, at least it appears on the surface, into an arduous and lengthy process with additional information being requested from companies and a lack of completeness.

Unfortunately, anecdotal evidence from recent meetings with numerous companies support these statistical trends. It has been reported to our staff on several occasions that DHS is applying inconsistent and sometimes what appeared to be unreasonable application criteria, making it increasingly difficult to achieve certification as well as SAFETY Act approvals.

The application of inconsistent criteria in the evaluation process would, of course, undermine the intent of the SAFETY Act and could yield potentially anti-competitive outcomes. The current complaint of all these meetings is widespread frustration with the arduous ordeal of SAFETY Act approval.

I had hoped that the SAFETY Act would be a success story for DHS, for the business community and for our homeland security. As we struggle with tighter Federal budgets, we have to be more creative in developing homeland security technologies and encourage their deployment. Some recent Congressional efforts to poach the S&T budget for revenue create additional budget uncertainty.

So I am a strong believer in the SAFETY Act and its intent and its importance to the business of homeland security. As with every successful business program, the application process should be as user-friendly as possible while upholding the standards that we intend to be included.

The private sector has enormous research and development capability, and tighter Federal budgets will force us to tap these private sector resources even more. In order to do this, I would believe SAFETY Act liability protection is critical, and it provides DHS with a necessary tool to access large private sector investments in the homeland security marketplace for the protection of all Americans.

I hope this hearing will help us to discover why the SAFETY Act hasn't been as effective as we would like. If there are things we need to do on the legislative side, we would like to be informed of that.

Last, in the spirit of being fair and balanced, I have letters written to the committee recently from companies regarding their positive experiences with the SAFETY Act process. Without objection, these documents will be included in the hearing record.

Now I would recognize the Ranking Member of the full committee, Mr. Thompson, for any statement he wishes to make.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I want to thank you for holding this hearing today.

I also want to thank the witnesses of both panels for being here also. I especially want to thank Mr. Craig Harvey from Bay St. Louis, Mississippi, the Minority Member's witness who has come to share his company's experience with us. I might add this is his maiden voyage to come to Washington to serve as a witness, and I assured him that you would be kind to him, Mr. Chairman.

Mr. LUNGREN. We will treat him gently.

Mr. THOMPSON. Okay. Thank you.

The Department of Homeland Security's Science and Technology Directorate is responsible for implementing and overseeing the SAFETY Act. We are going to hear testimony today detailing the application process for companies interested in having technologies designated as qualified antiterrorism technologies under the SAFETY Act.

For this important program, the Government provides immunity from liability to any product or service approved under the SAFETY Act. Congress allowed this kind of liability protection to encourage innovation in the development of products and technologies that would help protect us from the terrorist threat.

I should mention that unlike the patent, trademark, or other license provided by the Government, the Government does not charge a penny to thoroughly review each product for SAFETY Act approval. Mr. Chairman, I am wondering whether our current fis-

cal situation the Congress should consider requesting a small fee, perhaps, for this valuable service.

But after we consider the fee question, we should focus on the number of businesses that have used this program, the outreach that the Department has done to attract small, minority, and disadvantaged businesses, and the effectiveness of the SAFETY Act approval process.

As we all know, small businesses create most of the jobs in America. In this downturn of the economy, a SAFETY Act designation can improve a company's bottom line and help small, savvy companies create jobs. Having read the Department's statistics, I have some hope that the SAFETY Act is living up to its mission that products and technologies enter the process, are quickly reviewed and provided designations and certification in a timely manner.

I hope the testimony reveals that small, disadvantaged, and minority-owned companies can access the SAFETY Act process without the help of $400-an-hour consultants. Now, companies must be able to navigate the process with assurance that their information is being rigorously reviewed, their proprietary information carefully guarded, and their applications are handled expeditiously.

It is disturbing to me that the latest proposed fiscal year 2012 budget level of $398 million for Science and Technology Directorate as introduced in the House appropriations mark would eliminate two-thirds of the research and development funding for the Department. I have serious concerns about these reductions in funding and how they will affect the free SAFETY Act service.

I look forward to the testimony, Mr. Chairman, and I yield back.

Mr. LUNGREN. Thank you very much.

I would just say for the record that any other Member of the committee would be able to submit opening statement for the record.

Now we are pleased to have the distinguished panel of witnesses before us today.

Our first witness is Mr. Paul Benda, acting deputy under secretary for science and technology at the Department of Homeland Security. Prior to joining the Department, Mr. Benda served in several positions at the Department of Defense as an officer in the United States Air Force; program manager of Defense Advance Research Projects Agency; as the director of the Chemical, Biological, Radiological, Nuclear and Explosives program; and finally as the director of the Project Integration Office.

The Chair recognizes Deputy Under Secretary Benda, and we thank you for your service to our country.

STATEMENT OF PAUL BENDA, ACTING DEPUTY UNDER SECRETARY, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. BENDA. Thank you, Chairman Lungren. Thank you full committee Member, Ranking Member Thompson.

I appreciate the opportunity to speak to you today about the SAFETY Act program and appreciate your time. I want you to know that we have used the SAFETY Act as a powerful incentivization for the development and deployment of anti-ter-

rorism technologies, and the Department of Homeland Security Science and Technology Directorate takes extremely seriously our job to evaluate and review these applications.

The mission of the SAFETY Act sometimes gets lost in the rhetoric. That mission is to spur the deployment of anti-terrorism technologies to protect Americans from terrorist attacks. It is our job, it is incumbent upon us, to ensure that when those technologies do receive SAFETY Act awards, that they are effective.

The majority of criteria stated in the SAFETY Act focus on the effectiveness of those technologies. It is inherently a technical review, and it is important that it be a technical review, because it is important that those technologies work as expected when they are deployed. If they don't work, and something happens, someone could die. That is a responsibility that we take very seriously.

I want to talk a little bit about where we have been, where we are, and where we are going. The program has matured, as you stated, Mr. Chairman. In the beginning we were a little slow. We were trying to find our footing. But right now, if you compare our numbers to the early years of 2004 to now, we are processing nearly twice as many applications twice as fast.

We are also focused on making sure our program is accessible to all businesses, not just large businesses, not multinationals. So there is analysis of how many businesses of what types of businesses receive SAFETY Act awards or submit applications. It turns out by a margin of 2:1 small businesses versus large businesses apply for the SAFETY Act. We think that is important.

Small businesses like NVision are the engines of innovation of this country, and we need to support them. So we have done everything we can to ensure that the process is not onerous. We have a pre-application process that allows small businesses to file an expedited application with us. We review that quickly, and then we bring them in for a conference and explain how they can go through the process. The majority of our applicants take advantage of this, and small businesses like NVision are able to navigate the process without any outside help.

What we found was a little surprising. Over 70 percent of applications are done without any outside help at all. What is even more surprising is that those who don't receive outside help are actually processed 20 percent faster. So when we talk about requiring SAFETY Act experts to file an application, that is simply not true. Those that do it on their own with our help can actually do it faster.

Now, I will say that those who use outside help are probably more complex. We have a series of complex applications such as services, and those take a longer time to review. But clearly, the process works for small businesses.

We have heard about the diminished interest, and I think if you look at the unique number of applications that are filed, you could see a trend of that going downward, but I think it is much more important to focus on the awards that are actually granted.

The difference between fiscal year 2010 awards and fiscal year 2009 is likely to be minimal. It will probably be at maybe 2 percent less than what we currently do. In fiscal year 2011 the numbers we showed you have gone up dramatically since we provided that

information on April 13, because as we have generally seen, we see the vast majority of applications to the SAFETY Act in the last quarter.

What is even more important, though, is that the quality of applications has gone up. In 2009, 19 percent of applications were deemed complete. In 2010, 24 percent were complete. So we have worked hard to try, as we said, with this pre-application process, to work with these companies to make them better.

In 2011, as of today, 44 percent of our applications are complete. Generally, when the initial application is considered complete, 90 percent of those receive award. So the process is improving.

Furthermore, we talk about renewals. In 2009 we only had four renewals that were submitted, which is admittedly a low number. In 2010 that number jumped by 600 percent to 24. In 2011, two-thirds the way through the fiscal year, we are now at 33, and we expect to have even more.

We are on track, if you include unique new applications and renewals, to have the most awards granted by SAFETY Act in its inception. So the thought that this process is going down or decreasing simply doesn't hold true by the facts, when you look at the updated numbers that we have sent in.

Now, where are we going? The SAFETY Act has strong support from the Department, strong support from Dr. O'Toole. She actually requested a Secretary-level policy review on how we can better use the SAFETY Act, how we can better incentivize the adoption of these antiterrorism technologies, and we are actively engaged in that.

One of the areas where we have coalesced is the use of block designations. Block designations leverage existing DHS programs or other standard programs from other Government entities and allow for an expedited review. In fact, block designation applications are generally processed 25 percent faster, and we have identified additional process improvements that should allow us to process them 50 percent faster. We just posted another block designation in partnership with the Domestic Nuclear Detection Office GRaDER Program yesterday.

So we are continuing our outreach. We recognize the importance of this program. Under Secretary O'Toole is actively engaged, and we are working very hard to maintain the accessibility of this program, maintain a rigorous process that is transparent, that is consistent, that is not overly burdensome, but still maintains our ability as the No. 1 criterion of the SAFETY Act that it has demonstrated substantial utility and effectiveness. It is extremely important that we do those reviews, because if the technology fails, Americans can die.

I look forward to your questions, and I will be happy to take any that you have. Thank you, Mr. Chairman.

[The statement of Mr. Benda follows:]

PREPARED STATEMENT OF PAUL BENDA

MAY 26, 2011

THE SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES (SAFETY) ACT OF 2002

Good afternoon, Chairman Lungren, Ranking Member Clarke and distinguished Members of the subcommittee. I am honored to appear before you today on behalf of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T). The Support Antiterrorism by Fostering Effective Technologies (SAFETY) Act of 2002, enacted by Congress as part of the Homeland Security Act of 2002, has had a prominent role in improving the security of the United States. The SAFETY Act provides incentives for the development and deployment of effective anti-terrorism technologies through systems of risk and litigation management. The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers and users of anti-terrorism technologies from developing and commercializing technologies that could save lives. The Act creates certain liability limitations for claims arising out of, relating to, or resulting from an act of terrorism where "qualified anti-terrorism technologies" have been deployed. My testimony will discuss program performance, the application review process and how S&T is using this important tool to incentivize the development and widespread, high-impact deployment of effective anti-terrorism technologies and services throughout the United States.

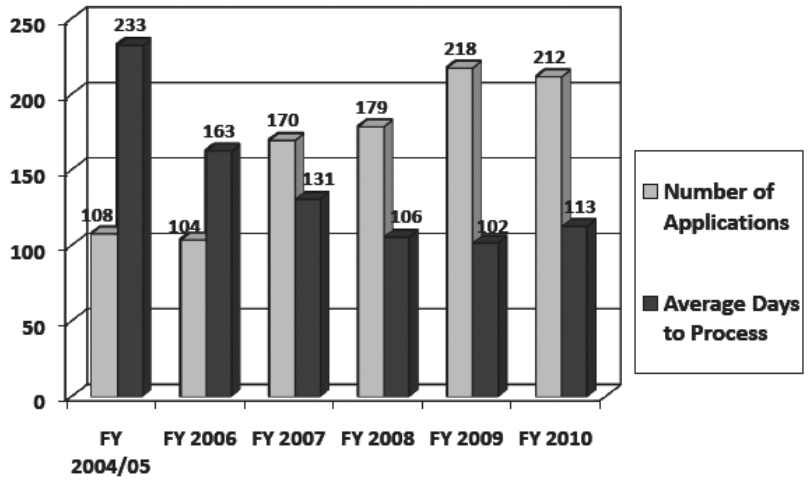
STRONG INTEREST, STEADFAST SUPPORT

The SAFETY Act Program continues to be very popular with the private sector and the Department has continued its steadfast support for the Program. Since the first applications were received in 2004, more than 440 "qualified anti-terrorism technologies" under the SAFETY Act have been approved. These technologies have been widely deployed to protect commercial facilities, critical infrastructure, transportation hubs, ports, borders, sports venues, and commercial aviation. Examples representing the broad scope of SAFETY Act protections that have been approved during Under Secretary O'Toole's tenure include:

1. A technology that provides cybersecurity situational awareness and network security monitoring.
2. A technology undergoing testing and evaluation designed to provide cybersecurity protection for the smart grid.
3. Technologies designed to harden bridges and tunnels in New York City.
4. An integrated system technology undergoing testing and evaluation designed to provide situational awareness for the Port of Long Beach, California.
5. A modular, rapidly deployable floating security barrier system designed to protect targets from high-speed small boats.
6. Anti-terrorism physical security services deployed to detect, deter, and respond to a variety of threats at commercial facilities and adjacent critical infrastructure in the New York Metropolitan area and in New Jersey.
7. A process for the production of an ammonium nitrate fertilizer treated to render it less detonable than standard fertilizer.
8. On-site production system for chlorine at water treatment plants (eliminating transport risk of bulk chlorine).
9. Threatening object- and explosive-detection systems deployed in the Nation's airports.
10. A web-based software tool that integrates a first responder decision support system with geospatial information technology.
11. An acoustic detection system to detect and rapidly triangulate gunshots and explosive event sounds.
12. Explosive containment vessels, allowing for the safe containment, transport, and disposal of explosive devices (used in response to Times Square bombing attempt in May 2010).

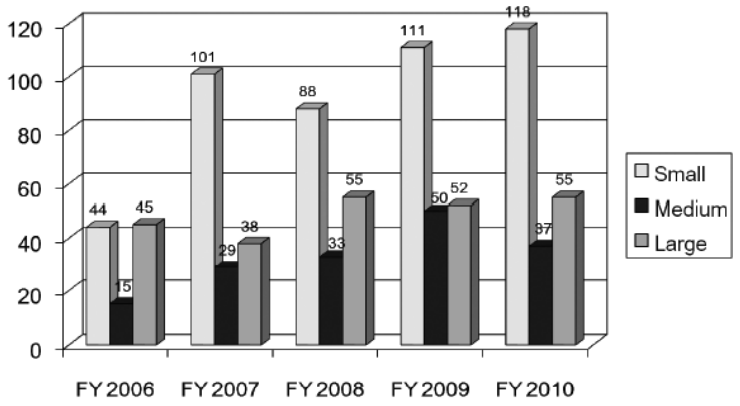
These SAFETY Act Designations and Certifications have increased the Nation's anti-terrorism readiness as well as our domestic industrial capability in the homeland security sector.

Figure 1: SAFETY Act Applications and Processing Time



As shown in Figure 1, applications have doubled since fiscal year 2006, while average application processing times have been reduced by more than 30 percent. This trend has continued into fiscal year 2011, where we are expecting 200 to 250 applications with a processing time currently averaging 113 days. As shown below in Figure 2, the majority of program applicants are from smaller businesses. For the purpose of Figure 2, we have grouped businesses with annual revenues under $50 million as small business. So far in fiscal year 2011, small business applicants comprise two-thirds of the applicant pool, with average annual revenues for this group at less than $11 million.

Figure 2: Applications by Company Size



Small: $0 - $50 million; Medium: $50 million - $1billion; Large: $1billion+

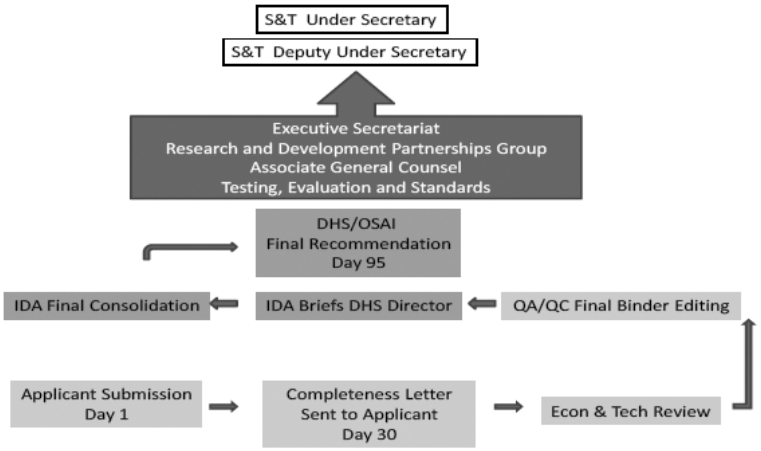
Figure 3 is a flow diagram of the review process used to evaluate SAFETY Act applications. Due to the significance of a SAFETY Act Designation or Certification, considerable thought and effort were devoted to developing a review process that is well-defined, repeatable, and applicable for evaluating both product- and service-based technologies against the SAFETY Act statutory and regulatory criteria.

Applications are filed electronically via the SAFETY Act website at *www.safetyact.gov*. Before an applicant submits a full application, they may choose to submit a pre-application, which is an abbreviated application, primarily containing narrative information. This summary process is designed primarily for first-time applicants or for those with a unique offering so they can receive prompt feedback and guidance on the scope of information they should submit in order to maximize the chance of success. Within 21 days of application receipt, the Office of SAFETY Act Implementation (OSAI) transmits a letter to the applicant's SAFETY Act account on the website and offers to hold a teleconference with the applicant to discuss their technology and prospective application for Designation, or Designation and Certification.[1] OSAI technical and economic reviewers participate in the calls; the length and level of detail discussed during the calls is determined by applicant need.

Applications filed for Designation or Designation and Certification are evaluated as follows:

[1] For a Designation, liability is capped at the amount of liability insurance that DHS requires the technology seller to obtain and maintain. A Certification has a rebuttable presumption that the Government contractor defense applies. The presumption may be overcome only by clear and convincing evidence showing that the seller acted fraudulently or with willful misconduct in submitting information to DHS in its SAFETY Act application.

Figure 3: SAFETY Act Application Review Process



Submission—Completeness Phase

During the completeness phase, a submission undergoes a brief review to determine if the information submitted by the applicant is sufficient to conduct a review of a proposed Qualified Anti-Terrorism Technology (QATT) with respect to the statutory and regulatory criteria. The goal of this phase is to determine whether it appears that there is sufficient information in the application to receive an informed evaluation from the expert reviewers who conduct the full technical and economic review. Review personnel who are employees of the Institute for Defense Analyses [2] (IDA) and who have significant SAFETY Act Program experience perform this completeness review. On or about day 30, if the application appears to have sufficient material to permit a full review, a completeness letter is sent to the applicant. The completeness letter asks the applicant to confirm the technology description drafted by OSAI, and OSAI's summary of the insurance the applicant holds. Completeness letters often have a short list of questions for the applicant, which they should be capable of answering relatively quickly (normally the applicant is given 21 days to provide this information).

If an application appears to not have sufficient material to permit a full review, the applicant receives an incompleteness letter with a listing and discussion of the items that are needed to complete an application. Reasons an application could be determined to be incomplete include: (1) The applicant does not provide enough information to develop a definition of the technology, which is an essential element of any SAFETY Act Designation or Certification; (2) the applicant does not answer significant questions on the application form; (3) the materials submitted support only part of a technology's capabilities (e.g., for an integrated system, information is provided on the video sensor, but no information on the chemical and radiological sensors); (4) the applicant makes a material claim concerning the capability of the technology that is not substantiated by the evidence provided; and/or (5) documents submitted are incomplete or internally inconsistent (training records submitted are inconsistent with stated training policy, test report stating that a significant part of the testing was not conducted, performance report that indicates a significant failure rate).[3] Completeness/incompleteness letters are carefully reviewed and

[2] IDA, a Federally Funded Research and Development Center, provides technical and expert assistance to the Office of SAFETY Act Implementation. IDA is contracted for these services under an Inter-Agency Agreement.

[3] The SAFETY Act Program offers a wide variety of opportunities for applicants to learn what level of information/data they should submit in an application. Opportunities and resources include the pre-application process, teleconference, or in-person meeting with senior review and program staff, and the SAFETY Act help desk, a resource that is reachable by phone or email.

signed by the Director of OSAI prior to release to the applicant. An incompleteness letter is posted to the applicant's on-line application account as soon as the letter is finalized. Normally, this occurs near the 30-day point, but could be much earlier, if there are significant deficiencies in the application that are readily apparent to reviewers.

We believe this approach is preferable to proceeding on with a full review, in spite of identified deficiencies in the application, where the likely end result would likely be a denial letter. Receiving an incompleteness letter could result in the applicant receiving a favorable decision on its application earlier than if it had to wait to receive a denial letter at or near the 120-day point to learn what is required to prepare a successful application. It also conserves Government resources. The S&T Directorate frequently uses independent Subject Matter Experts (SMEs) to conduct the technical and economic reviews following the completeness phase. Having these experts file reports which state that insufficient information was submitted for them to render an opinion concerning the efficacy of the technology is not a prudent use of scarce program resources.

Full Technical and Economic Review

If sufficient information for analysis exists, the application enters the economic and technical review phase. The application and supporting documentation is reviewed by economic and technical SMEs to the OSAI. Concurrently, the IDA staff evaluators conduct independent research on the technology of interest (including discussions with points of contact with Federal, State, local, and private sector technology users). Following the SMEs review, summary findings, independent research, insurance and economic information are assessed in relation to the statutory and regulatory criteria by internal, independent experts. Following a thorough internal peer review and quality assurance process, a completed analysis is prepared by IDA for review by the Director of OSAI. The Director, based on these independent findings and his/her own knowledge, on or about day 95 following application submission, provides a written report containing a recommendation concerning the appropriate level of SAFETY Act protection and a proposed liability insurance requirement, and selected application materials to the Office of the Under Secretary, Science & Technology, Department of Homeland Security.

Office of the Under Secretary, S&T Review

During this final phase, the application is first reviewed by the S&T Testing and Evaluation Support executive. Areas of review include evidence of technical efficacy, application of relevant standards, a review of any testing and evaluation performed, and, drawing on extensive background and contacts in the testing and evaluation field, whether there are stakeholders or experts in the interagency who should be consulted. Second, the application moves to the DHS Office of the General Counsel (OGC), which evaluates the sufficiency of the review process (i.e. whether the record adequately reflects adherence to the policies, procedures, and criteria set forth in the SAFETY Act statute and the Department's implementing regulations), the determination of the recommended insurance liability cap, the sufficiency and appropriateness of the description of the covered technology in the Exhibit A Technology Description document, and the content of the proposed SAFETY Act award letters (including the date of first sale of the technology, the correct listing of all named sellers and their States of incorporation and any specific terms and conditions pertaining to the particular award). Third, the application is reviewed by the Director of the Research and Development Partnerships (RDP) Group, who has direct supervisory authority and responsibility over the OSAI. Lastly, the application moves to the S&T Executive Secretariat, where the award documents undergo a brief administrative review, before moving to the Office of the Deputy Under Secretary, who is the Under Secretary's designee for signing SAFETY Act awards. Those applications that present significant policy issues are referred by the Deputy Under Secretary to the Under Secretary for final decision.

Each application's progress is tracked by a spreadsheet, updated weekly, that contains completion of milestones and current status of the review.

SAFETY ACT AS INCENTIVIZER

The SAFETY Act was designed to incentivize the development and wide-spread deployment of effective anti-terrorism technologies. In implementing this powerful tool, the Department has used a two-prong approach: (1) Incentivize private sector entities to build effective antiterrorism capabilities that they determine to be appropriate using their requirements, analyses, and considerable judgment, and (2) increase the accessibility, reach, and impact of Government homeland security initiatives. Most of the Designations and Certifications to date reflect the judgments of

private sector providers and purchasers of anti-terrorism technologies and services delivered through the free market.

Support for Government initiatives is provided principally through two processes: (1) A procurement Pre-Qualification Designation Notice, which provides advance notice that private sector entities selected to perform under a listed Government procurement will likely qualify for SAFETY Act protections related to their performance, and (2) Block Designations or Block Certifications, which provide notice that private sector entities who provide, whether to private sector or public purchasers, certain technologies or services which meet defined performance standards or technical characteristics are likely to be approved for SAFETY Act protections for those products or services.

As an example, a very popular procurement Pre-Qualification Designation (recently converted to a Block Designation) is for the Transportation Security Administration's (TSA) Certified Cargo Screening Program. This Program involves private sector-owned and -operated secure facilities established in accordance with TSA directives for the screening and securing of cargo to be transported on commercial aircraft. We have issued more than 40 Designations under this Program; many participants are small companies who do not have the revenue to purchase large amounts of terrorism liability insurance. Other procurement Pre-Qualification Designation Notices are listed on the SAFETY Act website. Despite this and other noteworthy successes, the Department has recognized the challenges in applying the SAFETY Act with respect to Federal procurements. An effort initiated to better inform the Federal acquisition community of the SAFETY Act and how it can be incorporated effectively is nearing completion. The Federal Acquisition Institute (FAI), in collaboration with the Department, is developing a multimedia, on-line training course that will help acquisition personnel properly apply the SAFETY Act to an acquisition. FAI and DHS anticipate launching the SAFETY Act and Federal Acquisition course by summer.

We are also seeking to use Block Designations and Block Certifications more often as they are powerful tools to incentivize deployment of anti-terrorism technologies and offer an expedited review time line. S&T recognizes that the SAFETY Act application process requires a significant investment by the applicant who would like us to process their applications more quickly. While we consistently meet the application processing time lines set forth in the SAFETY Act Final Rule, we are looking at expanding our use of Block Designations, which are processed 25 percent faster than standard applications. Our goal is to streamline our Block review process and speed processing time lines to be 30 to 50 percent faster than standard applications and provide an expedited review path for appropriate technologies.

An example of a recently approved Block Designation and Block Certification is for standards development organizations who wish to seek SAFETY Act coverage for National standards that have been formally adopted by DHS as DHS National Standards. Recently, as a result of an S&T policy review, the opportunity to receive SAFETY Act coverage for a broader range of anti-terrorism standards has been approved and announced on the SAFETY Act website. The intent of this initiative is to provide incentives for increased use and more widespread implementation of anti-terrorism standards, by significantly expanding the pool of standards eligible for SAFETY Act coverage. This initiative has strong industry interest.

S&T has also partnered with the DHS Domestic Nuclear Detection Office (DNDO) to create a new Block Designation to incentivize the deployment of nuclear detection technologies. The DNDO Graduated Radiological/Nuclear Detector Evaluation and Reporting (GRaDER) Program, which evaluates commercial off-the-shelf Radiological/Nuclear detection equipment against National standards, has developed a mechanism for manufacturers to independently verify the performance of their technologies. The Block Designation will apply to technologies having undergone testing in accordance with the GRaDER program that have fully met the American National Standard Institute N42 standard or applicable published Government standards.

The SAFETY Act is also involved as an integral part of other DHS programs and projects. In S&T, the SAFETY Act will help incentivize private sector involvement in our newest APEX projects, which are projects that have been endorsed by both a DHS component head and the Under Secretary of Science and Technology through a signed charter. The goals of the APEX projects are to transition high-impact technology-based capabilities directly into components operational programs. Our most recently signed APEX project with the U.S. Customs and Border Protection (CBP) is to leverage Customs-Trade Partnership Against Terrorism (C–TPAT) Tier III shipper's approved security plans and operations with an Electronic Chain of Custody (ECoc) lock that S&T developed to create a "Secure Transit Corridor" with supply chain routes originating from Mexico and Canada to allow expedited security

screening at CBP-selected pilot ports of entry. If this pilot is successful, we hope to incentivize adoption of this model by private industry by creating a Block Designation for commercial shippers who agree to deploy the ECoCs and follow the stringent security standards required of C–TPAT Tier III shippers. This effort will improve overall supply chain security while at the same time expedite the free flow of trade and reduce liability insurance costs of participating shippers.

We are also actively engaged in several other initiatives—concerning cybersecurity, infrastructure protection, stadium security, transportation security, and private sector resilience—that will use the SAFETY Act to strengthen and enhance the security of the Nation. As you can see, this is a dynamic program that is continually evolving to meet the needs of the Government in true partnership with the private and public sectors.

CONCLUSION

In closing, I would like to thank you for the invitation to appear before you today and your continuing support of the SAFETY Act. I look forward to answering your questions and to working with you on maintaining the vitality of this very important program.

Mr. LUNGREN. Thank you very much, Mr. Benda. We will start the round of questioning by yielding myself 5 minutes.

The numbers you cited here seem to be somewhat inconsistent with the numbers I have been given before. The numbers I had was that the number of new SAFETY Act applications was 142 in fiscal year 2009, but only 28 at the halfway mark in fiscal year 2011. Did you say you updated numbers and that is not an accurate reflection of this year, fiscal year?

Mr. BENDA. That is correct, sir. I believe you received your numbers on April 13, and what we generally find is we receive the majority of applications the last quarter. We do have updated numbers that we are happy to provide you.

Mr. LUNGREN. Do you believe that you will be somewhere in the neighborhood of where you were in 2009, like 142?

Mr. BENDA. Well, sir, I don't believe that the number of applications is a good metric. I believe the number of awards——

Mr. LUNGREN. Yes, I understand that. But my question is the number of applications, because that would be an indication of confidence in the program by those who wish to participate in the program. So I am just asking you whether you see whether you are trending upward in number of applications to get back to where we were in 2009.

Mr. BENDA. No, sir. We will not see that same number.

Mr. LUNGREN. Is the reason because the universe of those that can be assisted by the SAFETY program and who would assist us by the SAFETY program is reaching its ultimate? Or is it because the usefulness of the program somehow is not apparent to those on the outside? Or is it some other reason?

Mr. BENDA. Well, it is a hard question for me to answer, sir. I am unsure. I think that those who know about it have probably filed. I think the number you are referring to is unique applications.

When I think the expansion, the next level for us in our view is the block designation, sir. We think that is a less onerous process. We think the number of applications we will receive under that with what we are doing with DHS National standards, what we are doing with DNDO's GRaDER Program, where we hope to go with CBP's C–TPAT Program, we hope to see those number of applications significantly improve over the coming years.

Mr. LUNGREN. Do you have an observation about whether or not the SAFETY Act is appropriate for certain sectors, but not other sectors? Has there been an analysis done for outreach in different sectors where you believe it is appropriate for SAFETY Act application?

Mr. BENDA. We have left the aperture wide open, sir. We are interested in incentivizing the deployment of antiterrorism technologies. Any sector that is open and supports that mission, we will support.

Mr. LUNGREN. So do you need to do more outreach? Do you need to make any changes legislatively? Are there any other changes, efforts, emphasis that the Department needs so that we can ensure to a greater extent that the possibility of those who would benefit from this is expanded?

Mr. BENDA. We are attempting to do the best outreach we can. We have actually posted on our website a notice for personnel or for companies that are submitting for procurement that they can have their procurement officer contact us to see if SAFETY Act protections apply. We have worked with the Federal Acquisition Institute to develop an on-line training course for Federal acquisition officers on how the SAFETY Act can work.

But unfortunately, with the 22 percent budget cut that the Science and Technology Directorate took in fiscal year 2011 and the potential 65 percent budget cut we are facing in 2012, it is unlikely that we would have the resources available to do any additional outreach than those already planned.

Mr. LUNGREN. Well, you have got the line drawn.

Mr. BENDA. Thank you, sir.

Mr. LUNGREN. Well, let me ask you this. Why did the Under Secretary delegate her responsibility to review and render decisions regarding the SAFETY Act to you? How does she, if she does, remain involved if, as you say in your prepared testimony, she considers this to be an important area of her jurisdiction?

Mr. BENDA. Well, sir, one of the reasons she delegated that responsibility down is that we are interested in expediting the review process as quickly as possible. Under Secretary O'Toole wanted someone that had the time available to do a good review of these applications. Simply, if you look at her inbox on a daily basis, the SAFETY Act applications were piling up, and she recognized for them to get a timely review, it would be helpful to delegate that down.

Now, she and I have, I would say, not necessarily daily discussions, but certainly multiple times a week, about SAFETY Act applications. She also ensured that any application that has significant policy implications are brought to her for discussion prior to signing.

Mr. LUNGREN. You are using the impact of budget restrictions. Given the fact we are going to have tough budget times, where are you looking for efficiencies in your program?

Mr. BENDA. The block designations, sir. We really think that this is a great way to expand the program. That will be more efficient for the U.S. Government, as well as for those people that are applying.

Mr. LUNGREN. Thank you. My time has expired.

The Ranking Member of the full committee is recognized for 5 minutes.

Mr. THOMPSON. Thank you, Mr. Chairman.

Mr. Benda, how do you report your approvals? Is it based on company size, employees, amount of business, or how do you do it?

Mr. BENDA. We report our approvals as requested by the committee, sir. The table that you received was surprisingly specific in how the numbers should be put out, even. So we are happy to report them in any way you like. We can do it by company size. We can do it by total number of pools. We can do it by unique applications. We can do it by renewals. We have all that data available.

Mr. THOMPSON. Thank you. I think I would appreciate you providing that information. For the sake of questions this morning, can you tell us where you find the majority of SAFETY Act approvals coming, based on the size?

Mr. BENDA. I do. Most come from small businesses, sir.

Mr. THOMPSON. So small businesses are able to navigate SAFETY Act requirements. Do you see a need to have professional help to fill out the application, or if they would just call you and say, "Look, I have a question. What does this mean?" Is the process onerous that you have to go through significant expense to fill out an application?

Mr. BENDA. I know I wouldn't characterize the process as onerous, sir.

I had a surprising conversation at one of Mr. Pearl's events when I talked with a large company that was explaining to me or asking me why their application fees have gone up so much. I told them we don't charge a fee. They said, "Well, our counsel, our outside counsel, used to charge $30,000 for a SAFETY Act application, and now they charge $60,000." I said, "Well, I don't even know why you are using outside counsel."

We are focused specifically on the technology effectiveness. If you look at the final rule in the criteria, it is mostly due to effectiveness. We have in place a robust pre-application process where companies can submit a shorter version of what they are looking for. I think NVision went through this process.

We convene a conference call with them to discuss the application, the issues. Then we work with them hand-in-hand so that they can get the SAFETY Act designation that is due to them. It is important for us to give them that.

Mr. THOMPSON. So the fees that companies pay are because they have gone and hired somebody to make their application on their behalf.

Mr. BENDA. Yes, sir, at best.

Mr. THOMPSON. As well there is no at this point—the Department itself does not charge any fees for processing the SAFETY Act application.

Mr. BENDA. No, sir. It is important to note that, as I said, 70 percent do not use outside counsel, and those are actually processed faster.

Mr. THOMPSON. Last question, is every SAFETY Act application treated individually for review rather than just some rubber-stamp process? What I am trying to get, so there is no assembly line-type process. It is an individual internal review by your Department.

Mr. BENDA. Yes, sir. It is very important that we do not do a presumption of effectiveness. These technologies protect the American public from terrorists. We can't presume they are effective. We have to look at the data. We have to look at the body of scientific evaluation that is called out in the criteria. If these technologies fail, people die.

Mr. THOMPSON. Thank you.

Yield back, Mr. Chairman.

Mr. LUNGREN. The gentleman yields back.

Now, in accordance with the rules of the subcommittee, I recognize other Members according to their appearance here, so Mr. Richmond of Louisiana is recognized for 5 minutes.

Mr. RICHMOND. I am going to yield back and wait for the next panel, if that is all right.

Mr. LUNGREN. That is fine——

[Laughter.]

Mr. LUNGREN. Since I have been advised we will probably have votes at 11:30 and it may last until 2:30 on the floor. So we would like to get our panel here and not have them sit for 4 hours waiting to come back.

Ms. Richardson, the gentlelady from California, is recognized for 5 minutes.

Ms. RICHARDSON. Yes, thank you, Mr. Chairman. I will be brief. I only had, I think, two questions.

Sir, you noted that since 2004 you guys have had over 400 applications, I believe, that were certified.

Mr. BENDA. We had 400 awards made. Some were designations. Some were certifications.

Ms. RICHARDSON. Out of what number? I didn't find that in the testimony.

Mr. BENDA. I don't have that total number in front of me. I believe it is close to 700-something.

Ms. RICHARDSON. So you would say your percentage is a little more than 50 percent. Would that be accurate?

Mr. BENDA. Yes, ma'am.

Ms. RICHARDSON. Okay. Is that 50 percent total since 2004, or what would it be in the subsequent years? Do you have any idea?

Mr. BENDA. The percentage of applications, based on fiscal year 2011 numbers, ma'am, that are receiving designation or approval, seems to be going up.

Ms. RICHARDSON. Yes, but that doesn't give us really any specifics. Would you mind supplying to the committee for 2004, 2005, 2006, 2007 and each year how many applied and how many were in fact approved?

Mr. BENDA. Yes, ma'am.

Ms. RICHARDSON. You have that. Okay.

Mr. BENDA. I do.

Ms. RICHARDSON. All right. That is my only question.

Mr. LUNGREN. The gentlelady has yielded back.

We thank you for appearing before us. I thank you for your service to our country, and I hope things are as good as you presented them to be. Maybe we will make inquiries of the second panel to see their observations, but the updated numbers are encouraging.

But I want to tell you that we will continue on this subcommittee to look very closely at this program, because, as you have suggested, this is an important program and one that we think is worthy of continuation and, even in difficult budget times, one that we want to make sure it succeeds. Thank you very much.

Mr. BENDA. Thank you, Mr. Chairman. Please feel free to ask me for a button.

[Laughter.]

Mr. LUNGREN. I love the SAFETY Act. Yes, sure.

Mr. BENDA. Thank you, sir.

Mr. LUNGREN. All right. We will ask the second panel to come forward. It consists of Mr. Marc Pearl, Mr. Brian Finch, Mr. Scott Boylan, and Mr. Craig Harvey.

Mr. Marc Pearl is the president and CEO of the Homeland Security and Defense Business Council. He has held numerous positions in the private sector relating to technology and cybersecurity policy issues, previously served as a chief of staff and counsel of our former colleague, Dan Glickman of Kansas. I think I came to Congress with Dan, but that was just a couple of years ago.

Mr. Brian Finch leads the homeland security practice and is a partner in the law firm of Dickstein and Shapiro. Mr. Finch has developed significant private sector experience in assisting companies to obtain protections under the SAFETY Act. He is an adjunct professor at the George Washington University Law School, where he teaches homeland security law and policy, and is a senior advisor to the Homeland Security and Defense Business Council.

Mr. Scott Boylan is the vice president of government relations and general counsel at Morford Detection, Inc., a company specializing in explosives, narcotics, and chemical detection systems. Dr. Boylan previously served at the Department of Treasury, the Department of Justice, and most recently, the Department of Homeland Security, where he was senior advisor to the secretary.

Mr. Craig Harvey worked at the U.S. Geological Survey for nearly 15 years as a field specialist and National instructor and most recently helped found NVision Solutions, a geospatial technology integration company, where he serves as chief operations officer and executive vice president.

Gentlemen, thank you for being here. We appreciate your time and your expertise. We would tell you that your written submissions will be made a part of the record and that we would ask you to summarize your testimony for 5 minutes apiece. Then we will ask questions.

I do acknowledge the attendance of Ms. Clarke, our Ranking Member of the subcommittee.

So if you would start in the order in which I introduced you.

Mr. Pearl, first, you are recognized to testify.

STATEMENT OF MARC A. PEARL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, HOMELAND SECURITY AND DEFENSE BUSINESS COUNCIL

Mr. PEARL. Thank you, Chairman Lungren, Ranking Member Clarke, Ranking Member Thompson and Members of the subcommittee. I thank you for giving the Homeland Security and Defense Business Council an opportunity to appear before you today.

As the Chairman said, I am Marc Pearl. I serve as the president and CEO of the council, a not-for-profit, nonpartisan organization of the leading companies that deliver homeland security solutions to the marketplace.

The council's main mission is to ensure that the perspective, innovation, expertise, and capabilities of the private sector are fully utilized in our Nation's security. Only when there is substantive engagement between the Government and industry can we successfully deliver efficient, effective, and fiscally responsible, high-quality homeland security solutions to our citizens.

The intent of Congress when it enacted the SAFETY Act in 2002 was to focus on the need to be proactive rather than reactive after 9/11 and nurture an environment that put R&D into an anticipatory posture. You gave industry solution providers a valuable legal tool to encourage the innovation, implementation, and deployment of technologies that help make our Nation safer and more secure.

The focus of my testimony is to provide the subcommittee with a perspective on how we can work together to: (1) Improve the process, (2) achieve the priorities of the Act, and (3) to ensure greater public support for the SAFETY Act. I appreciate your putting our full written testimony into the record.

First, with regard to a more effective process, the SAFETY Act has seen many peaks and valleys with respect to the amount of effort by companies who apply for certification to obtain its protection. Initially, the arduous and sometimes burdensome process deterred many applicants.

Many of our members are also concerned that the bases for technological evaluations of technologies of the SAFETY Act have not been consistent or as transparent as they could be. DHS should be encouraged to refrain from applying inconsistent criteria in their technical evaluation.

DHS, as we heard by Deputy Under Secretary Benda, has worked to revise and streamline its review process and has set into place more formal and reliable review mechanisms. But more effort is necessary to further streamline and make consistent the certification process.

The SAFETY Act review process must, of course, continue to be rigorous and thorough and conclusive in order that should a product or service be challenged, there is a strong review record in place. It is critical to ensure that the review process establishes solid 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.

DHS, however, must understand that the Act it is responsible for administrating is fundamentally a legal, not a scientific engineering or technical merit, program. The certification process does not require detailed review of systems, but a determination with reasonable certainty that a product, technology, or service is useful and effective against terrorism. Congress never intended to have the SAFETY Act certified solution be the most useful or the most effective effect tool against terrorism. We cannot let the perfect be the enemy of the good.

With regard to, second, the priorities, the SAFETY Act is meant to provide, as you said yourself in your opening remarks, an incentive to the private sector to continue to research and utilize anti-terrorism technologies. The act should serve to encourage industry to continue to innovate, but DHS must be more actively involved in promoting its benefits and show that it is a priority program.

For example, the Department could improve efforts to educate Federal contracting officials regarding the act and its related changes to the Federal Acquisition Regulations. The SAFETY Act could also be better aligned with the Federal acquisition process as a whole, including the eliminating of redundancies in and expediting technical evaluations of its applications relating to products and services that are procured not only by DHS, but other Federal Government entities.

We also believe that DHS should work more closely with third parties, such as the risk management industry, to better explain the values of the provisions. These could have an enormously positive effect on the underwriting process.

Third, with regard to garnering greater public support, the focus of the attentions regarding successful implementation of the Act should not be on how it limits liability, but rather how it encourages greater and more widespread deployment of technologies that could deter terrorism and protect our citizens.

DHS can ensure that a greater number of beneficiaries will recognize the benefits of the Act and industry can better understand what to expect from a successful application by better promoting it within Government and to the business community.

The rest of my remarks are part of the written record, but I want to say in conclusion that the SAFETY Act is a vital tool that can help us become a safer and more secure Nation by encouraging the successful implementation and deployment of technologies.

We thank you for this opportunity. We pledge to work with the subcommittee and the Department to achieve an environment where an improved and robust SAFETY Act is fully embraced and marketed in an atmosphere ensuring a sound, fair, and responsible certification process.

[The statement of Mr. Pearl follows:]

PREPARED STATEMENT OF MARC A. PEARL

MAY 26, 2011

INTRODUCTION

Chairman Lungren, Ranking Member Clarke and Members of the committee, thank you for giving the Homeland Security & Defense Business Council an opportunity to appear before you today. I am Marc Pearl, president and CEO of the Council, a not-for-profit, non-partisan organization of the leading companies that deliver homeland security solutions to the marketplace. The Council works to ensure that the perspective, innovation, expertise, and capabilities of the private sector are fully utilized in our Nation's security, as well as recognized and integrated with the public sector. Council members employ more than 3 million Americans in all 50 States. We are honored and proud to work alongside civilian, defense, and intelligence agency leaders in support of their strategic initiatives through our individual and collective expertise in technology, facility and networks design and construction, human capital, financial management, technology integration, and program management. Only when there is substantive engagement between the Government and the private sector can we successfully deliver effective, efficient, and fiscally responsible high-quality solutions to our citizens.

At the outset, we want to express our appreciation to the subcommittee and the Members of the entire Homeland Security Committee for your leadership on the full range of critical issues associated with improving the effectiveness of the laws and programs that would serve to make our Nation safer and more secure. A major part of that effort is the recognition that only when Government and industry are in direct communication and cooperation can we truly create a "culture of readiness and of preparedness."

Congress must continue to take the responsibility to encourage constant, open, and reliable communication between industry and Government to achieve its mission. Additionally, we look to Congress to provide the oversight and support necessary to ensure that we collectively as a Nation maintain our continued vigilance and preparedness, and are fully utilizing all the tools at our disposal.

Needs shift, priorities are altered, and threats continue to evolve. Over the past decade we have—all too often—found ourselves in a reactive posture, responding to the crisis du jour. We also must focus on the need to be proactive and nurture an environment that puts our research and development into an anticipatory posture.

That was the intent of Congress when it enacted the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act. Congress gave industry solutions providers a valuable legal tool to further encourage the innovation, implementation, and deployment of technologies that would serve to make our Nation safer and more secure.

The holding of this hearing today—the first specifically on this topic in 5 years—is allowing the Department of Homeland Security (DHS) and industry to join with you in giving voice to an important program that helps to give our Nation the ability to provide effective deterrent measures against those who would seek to destroy or kill innocent citizens.

The focus of the Council's testimony today is to provide the subcommittee with industry's collective perspective on the SAFETY Act and how we can work together to: (1) Improve the Process; (2) Achieve its Priorities; and (3) Ensure Greater Public Support.

A MORE EFFECTIVE PROCESS

Throughout its brief history, the SAFETY Act has seen many peaks and valleys with respect to the amount of effort required to obtain the protections it provides to companies that have gone through the application process. Initially—as could be expected from any new administrative review process—the ability to obtain 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 worked to revise and streamline its review process and set in place more formal and reliable review mechanisms. The Science & Technology (S&T) Directorate—tasked with implementing the SAFETY Act—has put forth new procedures indicating recognition that the application process is a collaborative one with the Office of SAFETY Act Implementation. As a result, they are reporting that approval has been granted to a larger number of applicants, including some innovative anti-terror services like commercial shopping center security guards and professional security certification programs. DHS has indicated a desire to continue on the path of managing a reliable and thorough review process while showing greater sensitivity to the potential burden to applicants. We are desirous of seeing as streamlined a certification process as is feasible and reasonable, and the implementation of the Act in a full and complete fashion.

We are also concerned that the bases for technical evaluations of technologies for SAFETY Act purposes have not been as consistent or transparent as they could or should be. DHS should be encouraged to refrain from applying inconsistent criteria in their technical evaluations.

Having said this, however, the SAFETY Act review process must be rigorous, thorough, and conclusive, in order 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. 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.

Industry recognizes that the SAFETY Act—in some ways—takes S&T out of its "comfort zone" of engineering and scientific research. But DHS must understand and recognize that the SAFETY Act it is charged with administering is fundamentally a legal, not a scientific, engineering or technical merit program. The certification process does not require a detailed review of systems, but a determination with reasonable certainty that a product, technology, or service is useful and effective against terrorism. Congress never intended to have a SAFETY Act-certified solution be the most useful or most effective tool against terrorism. We cannot let the perfect be the enemy of the good.

MORE EFFECTIVE PRIORITIES

The SAFETY Act was meant to provide an incentive to the private sector to continue to research, develop, deploy, and utilize anti-terror technologies to best protect our Nation, its citizens, and critical assets. If utilized fully, the SAFETY Act encourages industry to continue to innovate. Has it been marketed as successfully as it could within Government and to the business community at large?

Unfortunately, there has been a negative trend of reductions in the total number of SAFETY Act applications and approvals in recent months.

SAFETY Act-certified technologies are suggested as part of the Federal acquisition process, but DHS could further improve efforts to educate Federal-contracting officials regarding the Act and its related changes to the Federal Acquisition Regulation (FAR). Implementation of the Act could also be better aligned with the Federal acquisition process, including eliminating redundancies in and expediting technical evaluation of SAFETY Act applications relating to products and services procured by DHS and other Federal Government entities.

The Department should also vigorously publicize the value of the SAFETY Act to the business community at large, and continue to work with solutions providers in streamlining the application process. It should also work more closely with third parties—such as the risk management industry—to better explain the value of the provisions. As a result, this could have a subsequent positive effect on the underwriting process.

By making the SAFETY Act a higher priority of the administration, and better promoting it within Government and to the business community, a greater number of beneficiaries will recognize the benefits of the Act and industry can better understands what to expect from a successful application.

GREATER PUBLIC SUPPORT

The Council and its members are committed to increasing the understanding and further deployment of SAFETY Act-approved technologies, and encouraging a strong and responsible application process that gives confidence in the products and services granted SAFETY Act protections.

The focus of attention regarding successful implementation of the SAFETY Act should not be on its limiting liability, but rather on how it encourages greater and more widespread deployment of technologies that could deter terrorism and protect our citizens. Everyone loses if certified technologies are not more fully deployed and the benefits of the Act are not better publicized. Our Nation would be left with fewer safeguards, and companies that do develop or deploy such technologies would be open to limitless litigation.

Congress' role—as you are doing through this hearing today—is to encourage constant, open, and reliable communication between industry and Government. Additionally, Congress must continue to provide the oversight and support necessary to ensure we collectively as a Nation concerned about continued vigilance and preparedness are fully utilizing all the tools at our disposal.

Lastly and briefly, transportation security; border security; and the protection of people, facilities, goods, and networks, all have an international component that requires cooperation and communication among all our country's friends and allies. Promoting the benefits of the SAFETY Act—its incentives to develop, implement, and deploy the best of breed tools and solutions to fight terrorism—no matter where they are developed, manufactured, or deployed would be enormously helpful in our fight to protect our own homeland. The Act provides protections for the manufacturers and providers of certified technologies and services for cases under the jurisdiction of the U.S. court system, but no such protections exist outside U.S. borders. Is it foolish to ask our strategic partners for enhanced international cooperation on third-party liability protections for terrorist attacks? Shouldn't this issue be put on the agenda when Government officials meet with their Legislative and Executive branch counterparts—particularly now that we all recognize that terrorism is a global threat and homeland security a global mission?

CONCLUSION

"Success" against those who would seek to destroy our way of life, wreak havoc on our economy, and kill innocent citizens will ultimately depend on our ability to fully implement and deploy technologies and tools that fully deter and prevent a devastating catastrophe.

To achieve greater and active participation by everyone is not just the responsibility of Congress to enact the necessary laws, the administration to develop real, tangible, and "embraceable" regulations and programs to carry them out, industry to develop and help deploy the solutions, or the greater citizenry to take on its share of the responsibility to be vigilant. It is a combination of all of the above. The SAFETY Act is but one vital tool that helps us become a safer and more secure Nation.

On behalf of the Homeland Security & Defense Business Council, I once again express our appreciation for the opportunity to provide our comments on the important issues before the subcommittee. The Council and its members pledge to provide this committee and the Department with the appropriate support, expertise, and input needed to achieve mission success.

We are prepared to work with the subcommittee and DHS to mutually achieve an environment where an improved and robust SAFETY Act is fully embraced and marketed the Department in an atmosphere ensuring a sound, fair, and responsible certification process.

Mr. LUNGREN. Thank you very much, Mr. Pearl.

Mr. Finch.

STATEMENT OF BRIAN E. FINCH, PARTNER, DICKSTEIN SHAPIRO, LLP

Mr. FINCH. Chairman Lungren, Ranking Member Clarke, distinguished Members of the committee, it is an honor to appear before you today to discuss the current implementation of the SAFETY Act by the DHS Science and Technology Directorate.

Post-9/11, Congress deliberately chose to offer the liability protections of the SAFETY Act to ensure a healthy anti-terrorism marketplace. Not 3 hours ago, I was reminded of those by the former Speaker of the House, Dennis Hastert.

Since it was enacted, the SAFETY Act has been, relatively speaking, one of DHS' most successful programs. Without it, numerous critical products and services would not be in the marketplace. The SAFETY Act is not an absolute success, however. While 400-plus products and services have received the designation or certification, that number should be in the thousands.

The good news is 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 arms DHS with broad authority to rapidly and effectively process applications and implement them in a transparent, consistent, and accountable manner that will unleash its potential.

I must state that this hearing is absolutely essential, because if S&T gets only one thing right, it has to be the SAFETY Act. Without a successful SAFETY Act program, S&T will not be moving forward completely in its mission to help deploy effective technologies into the marketplace.

SAFETY Act is more critical than ever, because companies can now easily be held liable for damages, if they fail to take reasonable steps when it is shown that they knew or should have been aware they faced possible terrorist attacks. Unfortunately, "reasonable" can mean anything, including even the most stringent security measures.

All of this came from the decision in New York holding victims two-thirds liable for the death and destruction caused by terrorists, leaving the other third to others, including the terrorists themselves. Also include that when litigation happens following a terrorist attack, security providers will be the ones to have their pockets turned inside out.

Terrorists are not going to honor damages awards stemming out of a civil lawsuit—plus, of course, right now there is only one group with a proven record of tracking down terrorists, and I feel confident in saying that the Navy SEALs are unavailable to act as process servers.

Given the realistic possibility of ruinous litigation following a terrorist attack, the question then becomes: How best can the SAFETY Act be implemented? Let us remember that DHS itself stated, "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 from saving lives."

DHS must heed its own words. It can do so by first working to try and have each application approved. At times there is a sense that applications are presumptively denied, unless there is an overwhelming case for approval. Right or wrong, that has been a powerful disincentive for current and potential applicants.

Second, the Department should accept all sorts of data demonstrating effectiveness, not just the kind that is generated when a product has been through the wringer of a Federal procurement.

Third, DHS should manage the SAFETY Act with relatively few boundaries in what can be approved. Applications for products or services that could protect sports facilities, hospitality chains, iconic structures, technology support outside the United States, or otherwise would protect against terrorism, should all be eligible for approval.

Some simple process changes would go far in creating a customer-friendly SAFETY Act. First, DHS should increase transparency. Even the most experienced applicants face a guessing game at times as to what is required of them to navigate the SAFETY Act process. That is terribly frustrating and gives companies serious pause as to whether they want to participate. DHS should be clear about what information it wants and should work with applicants to develop it.

Second, the SAFETY Act needs consistency. Companies have complained about similar applications being subjected to different standards of review, and that has to stop. Also, the renewal phase of the SAFETY Act has turned into something akin to a de novo review. That is difficult to understand, especially in circumstances where the applicant has done nothing wrong in the intervening years.

Accountability is a third factor. It must be clear to all who actually sets the metrics for a SAFETY Act application and that there is a mechanism in place to ensure that they are being followed. Such accountability will reduce instances of unconstrained fact-finding and will allow parties to know who they need to work with in order to get on the same page.

Another point is that certification under the SAFETY Act has become far less common. Whatever the reason, it is sufficient to say that this trend should be reversed immediately.

One last note is that—and this perception might exist among some—that once a SAFETY Act award has been issued, it is irrevocable. Simply put, we all should remember that Federal courts will play a strong adjudicatory role when the time comes for litigation.

Acknowledging the limited budgets facing our Government, now more than ever DHS must use the SAFETY Act to incentivize the private sector. Doing so will help promote some of the highest priority areas for DHS, including matters this committee has jurisdiction over, such as C–TPAT and cybersecurity. We must all work together to create a transparent, consistent SAFETY Act imbued with accountability.

I thank the committee for the opportunity to testify and look forward to taking your questions.

[The statement of Mr. Finch follows:]

PREPARED STATEMENT OF BRIAN E. FINCH

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 healed, 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 U.S. 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 United States, 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 most 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 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 anyway 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 cybersecurity, 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.

Mr. LUNGREN. Thank you very much.

Mr. Boylan.

STATEMENT OF SCOTT BOYLAN, VICE PRESIDENT AND GENERAL COUNSEL, MORPHO DETECTION, INC.

Mr. BOYLAN. Chairman Lungren, Ranking Member Clarke, thank you for inviting me and having me speak here.

My company, Morpho Detection, is one of the leading providers to the Department of Homeland Security of explosive detection

technology. We are a pioneer in explosive detection technology, and we are also a pioneer in the SAFETY Act. SAFETY Act is extremely important to our business, because when you think about what our business is, it is very risky.

What we do every day, almost every hour of every day in the United States, is we scan bags for explosives that get onto commercial aircraft, commercial aircraft that we all in this room probably fly at one time or another. The risk of error is quite large.

My company, when it was acquired from GE by Safran, one of the pre-conditions to that transaction was transfer of the SAFETY Act certifications. Closing would not occur without that happening. I have to say one of the success stories, I think, we were one of the first companies to do that, and the folks sitting behind me here from the SAFETY Act were very, very helpful in achieving that and getting our closing done. So that is positive.

Most of my technologies, our company's technologies, are certified by the Transportation Security Laboratory. At one time it was a part of TSA. It is now part of Science and Technology.

The process of that certification can take over a year. It involves testing. It involves providing multimillion-dollar pieces of equipment for free to the Government. At the end of the process, we have a certification. What that certification does for us is allow us to sell into the homeland security market.

I have had the situation with SAFETY Act certification where I have had certified technology that I hadn't had SAFETY Act certified. I have had the renewal of our CTX baggage screening technology take quite a long time and put us in a difficult position as to whether we could deploy new equipment, because we hadn't got the recertification of the explosive detection equipment that we were contracted to at the time to sell to the Department of Homeland Security.

So our scanning devices actually seemed to have a higher standard for SAFETY Act certification. I have been informed that SAFETY Act certification is now a predicate—excuse me, TSL certification is a predicate to SAFETY Act certification.

That is nowhere in the Act. I would expect that SAFETY Act certification would actually be less onerous than the testing and certification that our equipment undergoes.

Second, the testing involves operational and reliability determinations for the equipment. The TSL does this, but recently for new products that we have developed, and one of which is deployed and has been deployed for over a year in San Jose airport, we have only gotten designation, not certification.

We have certification for that equipment from the Transportation Security Laboratory, but we have designation from the SAFETY Act. That does not make any sense to me.

I think it is possibly a misunderstanding of how the certification process is done by the TSL on the part of the SAFETY Act and the Science and Technology office that reviews these applications, because they keep telling me that there is not enough data on reliability—by the way, that is never mentioned in the Act, reliability—whereas that is tested and evaluated by the very same Science and Technology department that the SAFETY Act office is a part of.

So my suggestion is if I have certification from one part of the Science and Technology Directorate, why can't SAFETY Act certification flow relatively easily from that? That is just designation.

Like I said, the coverage that is provided to us from the SAFETY Act is extremely important to our business. It is a very risky business, and the caps on the liability—we don't have immunity from liability, we have caps. We are still responsible for multi-millions of dollars that we can get from insurance coverage.

But without that, without that insurance, there are questions as to what direction our business will go and where we will invest. I think, like previous witnesses have said, this is easily fixed. I think there are just a few key directional points that the SAFETY Act office can be directed to, and we can have a much better process. Thank you.

[The statement of Mr. Boylan follows:]

PREPARED STATEMENT OF SCOTT BOYLAN

MAY 26, 2011

Chairman Lungren, Ranking Member Clarke, and Members of the committee: Thank you for the opportunity to testify and for holding these hearings today on the Department of Homeland Security's implementation of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act"). My name is Scott Boylan, and I am vice president and general counsel at Morpho Detection Inc. ("MDI"), a subsidiary of the Safran Group. MDI has more than 560 U.S.-based employees and factories in California and Massachusetts. We are a leading supplier of explosives and narcotics detection technology globally and support Government, military, transportation, first responder, critical infrastructure, and other high-risk organizations. We integrate computed tomography (CT), Raman Spectroscopy, trace (ITMS™ technology), X-Ray and X-Ray Diffraction (XRD) technologies into solutions that deliver detection results quickly with a high degree of accuracy, while ensuring efficient security operations.

MDI and our predecessor companies have a rich legacy in homeland security. After the Lockerbie tragedy, we were the first company to develop and deploy computed tomography-based explosives detection systems in partnership with the Federal Aviation Administration. Today, our technology is used throughout the United States to protect American citizens and infrastructure from terrorist attacks. The Transportation Security Administration relies upon MDI's technology to screen over a million bags each day for explosives. The State Department uses our technology to protect embassies and consulates around the world. The Department of the Interior protects National treasures, such as the Statue of Liberty, using our equipment. The Department of Defense protects military facilities and personnel with MDI equipment as a key part of their threat detection arsenal. We are proud of our work in developing innovative technologies to protect people and infrastructure around the world.

MDI's core mission is to develop and provide anti-terrorism technologies. The protections that the SAFETY Act affords are integral to our business plan and investment decisions. We were one of the first companies to apply for SAFETY Act coverage and value our on-going partnership with the Department of Homeland Security. Today, I would like to discuss the value of SAFETY Act protections in encouraging development of new and innovative anti-terrorism products, discuss recent trends in SAFETY Act operations, and provide recommendations as we approach the 10-year anniversary of passage of the SAFETY Act.

VALUE OF THE SAFETY ACT

The SAFETY Act legislation and implementing regulations provide incentives for the development and deployment of anti-terrorism technologies by creating a system of "risk" and "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 and protect the American people. As such, the SAFETY Act is a critical tool in expanding the creation, proliferation, and use of anti-terrorism technologies.

In light of the potential liability MDI faces in developing and deploying anti-terrorism technology, MDI highly values the risk management and litigation management provisions of the SAFETY Act. We are not alone in this view. Investment decisions involve an evaluation of risk—SAFETY Act protections limit and define risk allowing investors to have confidence in their decisions. The transfer of SAFETY Act coverage, for example, was a pre-condition to closing when our company was sold by GE to Safran in 2009. This only serves to illustrate how important this coverage is to investment decisions.

RECENT TRENDS IN IMPLEMENTATION

The Department of Homeland Security's implementation of the SAFETY Act must be assessed with a view to the purpose of the legislation. To encourage technological innovation and to facilitate the fielding of technologies that support our Nation's homeland security efforts, Congress established a set of liability protections for technology providers so companies could develop and provide anti-terrorism technologies without the threat of crippling lawsuits. Congress deserves credit for recognizing the need for the SAFETY Act, and the legislation's risk management, and liability protection provisions are at least as important today as when the Act was originally promulgated. In fact, there is increased awareness of the importance of technology in tackling our staggering homeland security mission, including defending our land and sea borders; protecting key resources and critical infrastructure—including cyber resources; preventing chemical, biological, radiological, and nuclear ("CBRN") attacks; and improving preparedness and emergency response capabilities. Unfortunately, DHS' recent SAFETY Act implementation efforts have raised serious concern about the Department's commitment to the program as well as questions as to whether the Department is administering the program in a manner consistent with Congressional intent and the Act's statutory and regulatory mandates.

MDI's recent experience and communications with the Science & Technology Directorate concerning certain MDI SAFETY Act applications illustrate that the SAFETY Act application process is neither consistent nor "user-friendly." Moreover, the manner in which the SAFETY Act is being implemented today is discouraging applicants from continuing to support the program—at the expense of the laudable objectives of the SAFETY Act. There is growing concern, not only at MDI but also among colleagues across industry who are engaged in developing and providing homeland security technologies, that efforts to implement the SAFETY Act have been compromised by an apparent lack of understanding or commitment to the goals that led to the promulgation of the SAFETY Act. For instance, there is particular concern regarding the sharp decline in the number of technologies receiving SAFETY Act coverage generally, and SAFETY Act Certification in particular. It is also clear that the SAFETY Act application process has become more protracted and burdensome.

Our experience with the administration of the SAFETY Act by the Science & Technology Directorate over the past year has been particularly frustrating. Renewal of SAFETY Act Certification for our key product line of explosive detection technology for checked luggage was delayed beyond the regulatory required time limits.[1] New product models in the same product line were only given SAFETY Act Designation, not Certification, for "lack of operational test data" in spite of the fact that all of these products had been extensively tested and their performance certified by the Transportation Security Laboratory ("TSL")[2] before being purchased and deployed by TSA. One of these new models had been operationally deployed and had scanned millions of bags that had been loaded upon commercial aircraft. The delay in Certification renewal forced us to consider whether we would deploy more machines without SAFETY Act coverage.

Other MDI technology that has been SAFETY Act Certified for years was recently denied Certification renewal along with a new model developed for the critical infrastructure protection market. This technology is mature and is used every day to detect and deter threats at very sensitive facilities where Federal regulations require that explosive detection technology be deployed. It provides some of the best explosive detection capability available—but it has been denied SAFETY Act coverage. This scenario has injected an element of arbitrariness that we have not previously experienced.

While the SAFETY Act and its implementing regulations set forth criteria to be considered in evaluating whether a technology should receive SAFETY Act Designa-

[1] MDI's SAFETY Act Certification renewal application filed in October 2010 was finally approved on February 17, 2011.

[2] The TSL is also part of the DHS Science & Technology Directorate.

tion, the Under Secretary for Science & Technology is directed to exercise discretion in evaluating these factors and "to give greater weight to some factors over others." Further, the SAFETY Act regulations state in particular that "the Under Secretary is not required to reject an application that fails to meet one or more of the criteria" and that the "Under Secretary may conclude, after considering all of the relevant criteria and any other relevant factors, that a particular Technology merits Designation as a Qualified Anti-Terrorism Technology even if one or more particular criteria are not satisfied." Recent decisions on SAFETY Act applications suggest a misunderstanding of the evaluation process to be performed in determining whether to issue a SAFETY Act Designation for a particular technology as well as the relative weighing of the factors to be considered. The fact that DHS has denied SAFETY Act renewals based upon a purported lack of operational and testing data is clearly contrary to the Act's intent to encourage the development and deployment of new anti-terrorism technologies.

MDI is in the business of providing technologies that protect the American people. To date, MDI has looked to the SAFETY Act to provide important liability coverage for its anti-terrorism technologies. Should the SAFETY Act's risk management and litigation management provisions not be afforded to MDI's technologies, the company would be compelled to reevaluate whether and to what extent it should continue to deploy the technology that today is on the front lines of our homeland security efforts. The decision not to renew existing SAFETY Act approvals certainly does not incent MDI to provide anti-terrorism technologies and seems incongruous with the fact that SAFETY Act coverage is now being denied for the very technology that was integral to the TSA's effort to protect the traveling public and continues to deter terrorism in other contexts.

RECOMMENDATIONS

SAFETY Act protection is critical to ensuring that technology tools are available today for homeland security and even more critical to driving the next generation of anti-terrorism technologies. In the current economic climate, companies are forced to make difficult investment decisions. Homeland security sales can be unpredictable from year-to-year and are typically event-driven. Some smaller companies with innovative ideas may not have the backing or resources to weather this volatile marketplace and may face significant barriers to entry. This, in addition to uncertainty about potential liability, could force some companies to make a difficult decision—to exit homeland security technology development. With an ever-more-sophisticated adversary, our homeland security frontline deserves the best technology available and continued investment in the tools they need to deter, detect, and thwart the next attack. Strong implementation and execution of the SAFETY Act is an important aspect in supporting security technology innovation.

We have a few recommendations for the committee's consideration:

- Streamline SAFETY Act Certification by recognizing formal test certification by the DHS TSL or by other DHS component agencies. DHS has invested in establishing test certification processes throughout the Department. In addition, the Department of Defense has a well-established test and evaluation process that should also be recognized by DHS in SAFETY Act Certification. The SAFETY Act office should recognize successful completion of one of these DHS or DoD certification processes and expedite approval of applications for these companies. Implementation of this recommendation would eliminate duplicative processes and reduce Government costs associated with the SAFETY Act Certification processes.
- Provide greater transparency in the SAFETY Act review process. The SAFETY Act office should provide processing time metrics on its website *(www.safetyact.gov)* and should be required to notify the committee in the event that processing times exceed those defined in the SAFETY Act Final Rule.
- Provide administrative remedies for denial of SAFETY Act Certification. This measure would provide redress for companies who have been denied certification.
- The intent of Congress in establishing the SAFETY Act—to enable and encourage U.S. companies to develop and provide vital anti-terrorism technologies to help prevent or respond to terrorist attacks without the threat of enterprise crippling potential liability—is clear, and the importance of the SAFETY Act in facilitating industry's support of our Nation's overall homeland security mission has only grown. The Department of Homeland Security must recommit to vigorous implementation of the SAFETY Act, and the Department's leadership must prioritize efforts to reverse the negative trend of reductions in the total number of SAFETY Act applications and approvals. Implementation of the

SAFETY Act should be better aligned with the Federal acquisition process, including eliminating redundancies in and expediting technical evaluation of SAFETY Act applications relating to products and services procured by DHS and other Federal Government entities.

Thank you for your attention to these issues. I am happy to answer any questions you might have.

Mr. LUNGREN. Thank you very much for your testimony.

Now we would ask Mr. Harvey to give us his 5 minutes.

STATEMENT OF CRAIG A. HARVEY, CHIEF OPERATIONS OFFICER AND EXECUTIVE VICE PRESIDENT, NVISION SOLUTIONS, INC.

Mr. HARVEY. Chairman Lungren, Ranking Member Clarke, Ranking Member Thompson from my home State, Members of the committee, thank you for asking me to testify today on the SAFETY Act. It has been very important to me personally and to our business.

My name is Craig Harvey. I am the chief operating officer for NVision Solutions. We were founded in 2002 and are a growing, award-winning, minority woman-owned and economically disadvantaged company headquartered on the Mississippi Gulf course. NVision is a geospatial company technology, specializing in emergency management services and products for industry and Government.

With over $1 million in small-business contracts and grants from NASA, NVision built a high-tech crisis management information system called the Real-Time Emergency Acts and Coordination Tool, or REACT.

In 2007 the Center for Asymmetric Warfare at the U.S. Naval postgraduate school invited NVision to participate in a 3-year series of Federal, State, and local multi-agency homeland security exercises along Puget Sound. During this activity, NVision worked with the Pacific Northwest National Laboratory, who used REACT to monitor these exercises. During that time they began to understand the enormous risk to a small business that emergency management and terrorism products represent.

In 2009, at the recommendation of a partner company, we began to investigate the SAFETY Act as a pathway to Nation-wide deployment. Our goals were to have the Government review our software within the context of the National response plan, mitigate litigation risk, and bolster product credibility.

Our process began the SAFETYact.gov website, which provided us with step-by-step application instructions. We did participate in the pre-application process. A DHS specialist spent 45 minutes with us, describing the application process, discussing our product, and answering all of our questions.

Among the important pre-application facts learned was that existing customers like NASA and St. Tammany Parish, Louisiana, were critical as real-world performance references and examples of customers potentially benefiting from the SAFETY Act.

The REACT application was started in 2009, including everything from company financial statements to product documentation, technical descriptions, and marketing strategy. The technical application we felt was comparable to an applicant patent application. It was 30 pages long. Our entire application totaled hundreds

of pages and took 6 months to complete, minding that we started from scratch.

We submitted the application in early 2010 and began the minimum mandated 4-month review. During that time we exchanged 17 e-mails and at least a dozen phone calls with DHS, providing additional information. Through the entire process, we dealt with the same individuals. We felt like our application process was moving forward.

We received a notice of our SAFETY Act designation in July 2010. DHS informed us we had 30 days to cover a $1 million insurance liability before we were officially protected to the indemnification clause. This was the only requirement during the whole process that represented a problem for us. We had significant difficulty locating an insurance broker or agent that understood the SAFETY Act and when you said "counterterrorism," they were backing up faster than an I-don't-know-what.

Ultimately, armed with the help and encouragement from DHS folks, we finally found a broker that would provide affordable insurance and finalize the SAFETY Act designation. To our knowledge, we are still the only organization in Mississippi with a SAFETY Act-designated product.

While the SAFETY Act application took nearly a year and hundreds of pages of documentation, it wasn't bureaucratic. We feel strongly that thoroughness of the process gives a SAFETY Act designation meaning and provides tangible benefits to Government users, citizens, and protects individuals and countries, and at the end, the taxpayers themselves.

We believe the SAFETY Act provides a tremendous National security benefit on incentives to risk mitigation for industry to develop homeland security solutions. The process gives DHS early insight into product development and the opportunity for constructive dialogues with potential suppliers.

The SAFETY Act also provides a conduit to Government to identify solutions well before the crisis strikes, instead of attempting to deploy poorly understood technologies in the midst of a chaotic event.

By leveling the playing field and capping financial exposure, the SAFETY Act encourages innovation. Without the SAFETY Act, our desire to bring REACT to market may have never been realized.

We would like to thank the Members of the subcommittee for a chance to tell my company's story. I would be happy to answer any questions you may have.

[The statement of Mr. Harvey follows:]

PREPARED STATEMENT OF CRAIG A. HARVEY

NVision Solutions Inc. was founded in 2002 and is a growing, award-winning, minority, woman-owned, small business headquartered on the Mississippi Gulf Coast. NVision is a geospatial technology company specializing in emergency management services and products for industry and government.

With over 1 million dollars in small business contracts and grants from NASA, NVision built a high-tech crisis management information system called the Real-Time Emergency Action Coordination Tool or REACT. In 2007, The Center for Asymmetric Warfare at the U.S. Naval Post-Graduate School invited NVision to participate in a 3-year series of Federal, State, and local multi-agency homeland-security exercises along the Puget Sound. During this 3-year activity, NVision worked with the Pacific Northwest National Laboratory who used REACT to mon-

itor and report on first-response training involving hundreds and sometimes thousands of participants. The positive attention garnered by REACT highlighted the product's potential. At the same time we began to understand the enormous risk to a small business realm of homeland security.

In 2009, at the recommendation of a partner company, we began investigating the SAFETY Act as a pathway to Nation-wide deployment. Our goals were to have the Government review our software within the context of the National Response Plan, mitigate litigation risk, and bolster product credibility.

Our process began at The SafetyAct.gov website which provided clear step-by-step application instructions. In the pre-application process, a DHS specialist spent 45 minutes with us describing the application process, discussing our product, and answering all our questions. Among the important pre-application facts learned was that existing customers like NASA and St. Tammany Parish, Louisiana, were critical as real-world performance references and examples of customers potentially benefiting from SAFETY Act protection.

The REACT application we started in 2009 included everything from company financial statements to product documentation, technical descriptions, and marketing strategy. The technical application, comparable to a patent application, was 30 pages long. Our entire application totaled hundreds of pages and took us 6 months to complete. We submitted the application in early 2010 and began the minimum mandated 4-month review. During that time we exchanged 17 e-mails and at least a dozen phone calls with DHS providing additional information. Through the entire process we dealt with the same individuals and always felt the application process was moving forward.

We received notice of our SAFETY Act Designation on July 27, 2010. DHS informed us we had 30 days to cover a $1 million insurance liability before we were officially protected by the Act's indemnification clause. This requirement is the only part of the process presenting us with difficulty. We found insurers unfamiliar with the SAFETY Act and unwilling to cover "acts of terrorism". Despite the fixed liability we were unable find affordable insurance. Ultimately, armed with help and encouragement from DHS, we finally located a broker willing to provide affordable insurance and finalized our SAFETY Act designation. To our knowledge, we are the first organization in the State of Mississippi to have a SAFETY Act-designated product.

While the SAFETY Act application process took nearly a year and hundreds of pages of documentation, it was never "bureaucratic". We feel strongly that the thoroughness of the process gives the SAFETY Act designation meaning and provides tangible benefits to the Government users, the citizens it protects, and the individuals and companies that develop innovative products.

We believe the SAFETY Act provides a tremendous National security benefit and provides incentives, through risk mitigation, for industry to develop homeland security solutions. The process gives DHS early insight into product development and the opportunity for constructive dialogues with potential suppliers. The SAFETY Act also provides a conduit for the Government to identify solutions well before a crisis strikes instead of attempting to deploy poorly understood technologies in the midst of chaotic events.

By leveling the playing field and capping financial exposure The SAFETY Act encourages innovation. Without the SAFETY Act, our desire to bring REACT to market may have never been realized.

Mr. LUNGREN. Thank you very much.

I thank all the panelists for their testimony. I recognize myself for 5 minutes.

The purpose, as I see it, of the SAFETY Act is to improve the opportunity for companies to be proactive, as suggested by Mr. Pearl. In some ways that means making these kind of products successful to the bottom line of your company. It seems to me if somehow in the process of implementing the SAFETY Act, it becomes a burden—that is, it provides a disincentive for you to be involved in the system—then we have defeated ourselves.

So, Mr. Harvey, I would like to ask you this. If you were to be told that when your possibility for renewal comes up, you would have to go through exactly the same thing and spend exactly the same amount of time before renewal of the application for which you had been previously approved, would you think that would be

an incentive for you? Would you think that would be—does that make sense to you?

Mr. HARVEY. Given the risk involved, we would comply.

Mr. LUNGREN. I know you would comply, but does that seem to make sense to you if, in fact, you went through this process to prove the efficaciousnes of your program, and then when it comes around for renewal, instead of giving you—I will put it this way in non-legal terms—the benefit of the doubt, because you have already been approved, you basically have to go through the same thing all over again?

Mr. HARVEY. I think starting completely over would be somewhat of a waste of time. I think the Act itself for redesignation should be what happened since the last time we saw your technology.

Mr. LUNGREN. Mr. Pearl, what is your experience in terms of renewal? Am I wrong in what I had been told by some companies that that appears to be a do-it-over-again type of process rather than give you the benefit of the doubt, based on the fact that you have already been approved the first time?

Mr. PEARL. Well, Mr. Chairman, not only is it a do-it-over-again process, it is that the level of non-renewals is so high over the last 4 or 5 years that it has become a disincentive, and companies are just basically going back to, well, what has changed with regard to the criteria, so that in essence it not only sends a message to companies that have gone through a process and are not renewed, but whether or not any new technologies that they have developed subsequent to that—why would they go through the process again when the chances of renewal are not going to——

Mr. LUNGREN. Let me ask you this: In terms of the marketplace, if you are a company that has, say, SAFETY Act certification, and you are having trouble getting renewal, what does that do with your ability to present yourself to purchasers?

Mr. PEARL. Well, I would rather take it for the macro level.

Mr. LUNGREN. Okay.

Mr. PEARL. The macro level is, as I think Mr. Finch talked about, is that there is no question that having a couple hundred in essence, and there is a major designation that the public doesn't realize that there is, which is that there is a difference between a SAFETY Act-certified and a SAFETY Act-designated.

You can't, in essence, present yourself into the marketplace, for example, as having been a designated—as having been a certified SAFETY Act. You cannot present yourself in the marketplace at this point in time to have gone through the designation process, for example.

So, in essence, the number of technologies that you just know anecdotally over the last 10 years in our country that have—the IT and the services that exist out there are significantly greater than 400. Therefore, that shows in and of itself that this potentially very successful program is probably the most under-reported and underutilized program, so that it is not about the renewal process just existing, it is about whether or not companies even know out there that they can and should take advantage of this important Act.

Mr. LUNGREN. Mr. Boylan, I am somewhat concerned about your suggesting that the left hand doesn't know what the right hand is

doing. I am sure that in your contact with the Department—you have mentioned it—what kind of response have you been given?

Are they so far apart geographically that they can't talk to one another? Does the one side not recognize the worth of the other? Are the goals or the specific purposes of the two operations so disparate that there is no way to have commonality?

Mr. BOYLAN. The TSL is in Atlantic City, and the SAFETY Act office is here. But it has gotten better, because I have been a squeaky wheel, I must admit, on this, because I have no choice. I have to have SAFETY Act certification for my technologies, or I can't deploy it. So it has gotten better.

I just got designation for a new product last week, and I have worked to put the TSL and the SAFETY Act people in contact with each other. But I think they are talking to each other.

But there is still a disconnect, from my view, on the operational reliability focus that the SAFETY Act office has at this point in time. That is an element of the TSL. You know, I told you it is over a year process. That is definitely a part of the process, and I think they get confused with some of the procurement processes that then occur thereafter.

Mr. LUNGREN. Has anybody cited to you legislative language, statutory language that prohibits them from working in concert?

Mr. BOYLAN. No.

Mr. LUNGREN. Okay.

My time has expired.

I recognize the Ranking Member of the subcommittee, Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

I would like to thank you all for your testimony here this morning.

My first question goes to Mr. Pearl. I wanted to just sort of reach a little bit deeper beneath the surface of your testimony today, where you spoke about the inconsistencies in the certification application process. Could you just sort of identify, maybe, the top three inconsistencies that you have been able to identify?

Mr. PEARL. Well, as I just alluded to, Congresswoman, the No. 1 is the inconsistency goes to the refusal to renew SAFETY Act already-designated applications, so that if you have gone through the process, the dramatic drop in the number of applications that are successful suggests that the Department has possibly changed its ways of administering the program. That sends out a message of inconsistency.

When you had the competitiveness issues arise, that if I had the same technology, for example, that another company had, and yet I could not receive the designation, but that company has, that sends a message of inconsistency as well.

I am encouraged by what the deputy under secretary mentioned with respect to the block approach, but we have not seen that, in essence, out in the marketplace yet. That has not been translated. So if I was going to focus on any one particular issue of inconsistency and the lack of transparency, it would be on the issue of the renewal issue.

Ms. CLARKE. Then you also spoke about the distinction between the being certified versus designated. Could you go a little bit deeper into that as well?

Mr. PEARL. Well, I mean, I think that you even hear it in the testimony today when with the numbers that come out of S&T are the number of, in essence, successful applicants. The vast majority of those—and you can correct me, and Brian may know even more—the vast majority of those are simply designated, not certified.

When you are a designated and not certified, and as part of our original testimony, many of our companies were very concerned that they couldn't sell that into the marketplace, that in point of fact, when you are certified you can, but when you are designated, and you have gone through the same application process, you cannot use the SAFETY Act seal. You cannot let the market know.

It may in fact be, as our other witnesses might attest to, it is going to be incredibly more difficult to get insurance coverage, because the insurance industry doesn't understand the difference.

Ms. CLARKE. The distinction between the two.

Mr. Finch, would you sort of add your insight into that particular, because that seems to be the crux, or one of the major issues here is the distinction between certification versus designation and, you know, what you have found?

Mr. FINCH. Absolutely. I mean, the numbers and the experiences of this panel would attest to the number of certifications has decreased over time. It decreased significantly. I believe the number was one for——

Ms. CLARKE. Is it that there is a higher block for the——

Mr. FINCH. Actually——

Ms. CLARKE. Okay.

Mr. FINCH [continuing]. When you go through the application process, I mean, functionally the way it works is that you have to have proper processes, procedures, quality control measures, and demonstrable effectiveness in order to be designated.

Then when you go to certification, there appears to be additional data detailing reliability and additional layers of effectiveness, et cetera. When you go through the application process, I can tell you, having prepared any number of them, the certification questions, you simply say, "See previous responses in designation section," because you lay all that out already.

So what we seem to be encountering is that there needs to be more evidence of effectiveness, more evidence of reliability stretched out over a period of years. That has been frustrating.

As Mr. Pearl is alluding to, then you get into situations where companies were certified 2005, 2006, et cetera, and they come back, and they are not getting certification upon renewal. The response is, "Well, we want to see more specific types of reliability. We want to see more specific types of effectiveness."

I don't have a problem with the Office of SAFETY Act limitation asking for more specific information. What I do have a problem with them is, and what I do have a challenge understanding is, how did it get to the point where years of deployment successfully certified with demonstrable data spread out over 6, 9, 12 months in a particular forum, that is not acceptable for certification?

In the absence of anything being glaringly wrong, I am having trouble understanding why something would drop from certification to designation and why, generally speaking, certification isn't the default at the end of the day.

Ms. CLARKE. Okay.

Mr. Harvey, would you tell us a little bit more about your company? I understand it is located near a large research and applied technology center, the Stennis Space Center in Mississippi. How has the physical location helped you collaborate with other technology companies, and what benefit has that been to your company?

Mr. HARVEY. Yes, ma'am. Our company started in an incubator at NASA Stennis Space Center. We started down this path on the technology side in 2003, and we have worked—our product itself has products that are rolled up from four or five different small technological companies that are also co-located in and around Stennis Space Center.

Having ready access, then, to the NASA scientists and the requirements specifically for NASA requiring emergency management and crisis management provided us all of the requirements that we needed to build our product to. It was built largely funded through the SBIR program or the dual-use broad area announcements, so.

Ms. CLARKE. Could you just sort of give us some insights into how you worked with Boeing on the development of your product?

Mr. HARVEY. Yes, ma'am. Boeing technically was a collaborator. There was no funds or technology that changed hands. We were working on the civil side of our application, and they were building a handheld unit. They introduced us to the California group and as well as the Puget Sound and the Pacific Northwest Laboratory.

It was Boeing and their reluctance to accept risk that pointed us as "you really need to consider the SAFETY Act." We really hadn't heard about it until that point. So if, you know, granted we are on a coast, and we are on the south coast of the United States, but where the Federal center, and it seems to me with the amount of technology development, there should be placards or signs or something advertising, you know, the SAFETY Act and its benefits.

I would think that, you know, it is something that the SBA should help with. I mean, they have got offices in every major, you know, city in the country. I don't think it is very well advertised, to be honest with you.

Ms. CLARKE. Very well.

Thank you very much, Mr. Chairman.

Mr. LUNGREN. I think we have time to ask a few more questions before we have votes.

Mr. Harvey, it is great to hear that while you are very much geographically connected with the Ranking Member of the full committee, that you did have to work with a California company. We appreciate that.

[Laughter.]

Mr. LUNGREN. I have a question, and I will start with you, Mr. Harvey, but I would like others to make an observation on this.

You said that the application process took over a year, or about a year, required hundreds of pages of documentation. You said both

in your spoken testimony and your written testimony that it was never bureaucratic, yet you also went on to say that the technical application was comparable to a patent application.

Some would say those are incongruous statements you made. I am trying to figure out whether you believed that the process was so rigorous because it is necessary that it means something or that it is just the nature of things that, when we go through these things we have gotten into, you don't call it bureaucratic paperwork requirements.

So I am trying to figure out whether you are saying we understand they had to be that thorough and therefore it would have to take a year and all this paperwork and all this amount or it wasn't. Can you give me some guidance on what you are trying to tell me?

Mr. HARVEY. Yes, Mr. Chairman. If you want me to complain about the Government, I can find lots of topics.

Mr. LUNGREN. Oh, no, no, what I am trying to do is ask for an assessment, because I want this thing to work. Everybody loves it. I mean, the representative of the Department comes here and gives me a button that says, "I love the SAFETY Act." Well, if you use a yellow button like this, it means you want it to work. You folks want it to work.

Yet I hear that we only had 400-and-some-odd people that are—companies that are taking advantage of it, when it literally should be thousands, if we really believe it. So I am trying to figure out what I can do to make it work even better so we can all love it together. So give us your best shot.

Mr. HARVEY. Mr. Chairman, I believe it works. What I really believe is the reason it took us a little longer than average was because we didn't have a lot of technical documentation at hand. We are a very small company, and when we started this, we had 20-something people, so we didn't have a lot of the technical writing done. So we had to go back, when I say we started from scratch, documenting our product, really.

I think it is a very onerous process, but it is not bureaucratic. It is time-consuming, but it is a level of detail that I personally believe has to be there to have any credibility whatsoever. I say that both from a technologist and a taxpayer perspective. If we didn't have that level of detail, it wouldn't have the credibility that it has.

Mr. LUNGREN. The real attraction, of course, is the protection, in a sense, from civil liability. I spent a number of years as a lawyer in the courtroom. I understand the importance of the litigation system, but I also understand the abuses of the litigation system. I want this to be rigorous. I want this to be thorough. I want it to mean something. But I also want to make it workable.

So, Mr. Pearl, how do we hit the sweet spot? How do we make sure that it is fair but at the same time not bureaucratic? How do we make sure that it is timely but not take too much time? How do we make sure that there is an incentive that hasn't dissolved into disincentive?

Mr. PEARL. Well, I think that part of it is that the entity that is administering the program, it is a scientific component part of the Department. It is an important one, and one that is very valuable, the science and technology.

The connection point to that and the legal community is a little tenuous in terms of how do lawyers talk to engineers in terms of making things right? I think that one of the problems is, as I think, you know, Mr. Boylan pointed out, is that in point of fact if you are going through a heavy, rigorous process like the Transportation Security Lab, and they are not talking with the S&T, then in point of fact you are missing the whole point of what Congress intended.

If, in fact, Federal contracting procurement officials have to be educated by the company as to the value of the SAFETY Act, you are not achieving what Congress intended in the first place.

So the encouragement of exactly the greater reporting of this process will, I think, raise—you know, the high tide will raise all ships and that in point of fact people will, if they choose to go to, you know, Mr. Finch for the purposes of getting legal advice on the application, or they choose to do it on their own, we need to have an encouraging process and a platform on which these companies can take off and develop the kind of designation that they are looking for.

Mr. LUNGREN. Ms. Clarke, do you have some questions?

Ms. CLARKE. Thank you, Mr. Chairman.

Mr. Pearl, I would like to sort of investigate with you some ways in which you think the S&T can encourage the successful deployment of these technologies. You talked about the need for there to be that of encouragement. Certainly, the rigors and the challenges of connecting all the dots are where we are stuck right now.

But, you know, where do you see those bridges built, and where do you see the capacity of the agency to really use this type of encouragement? Is it through collaboration or MOU with SBA? What would you say?

Mr. PEARL. Well, I think the first—there are two levels. One is the internal component part of Federal officials, whether it be at SBA, whether it be at other directorates at the Department, whether it be at, you know, at DOD or at Energy, anybody who is actually looking at the issues of, in essence, anti-terrorism technologies and services should be well aware of what is going on. That is not a budget issue. That is internal communication issue.

Three years ago the council—and I would ask the staff to possibly include that as part of the written record—put together an executive brief on how we could encourage greater embracement of the SAFETY Act. Part of that was greater communication to the community in the private industry.

We are standing ready to want to do this. We think it is in all of our interests to, in essence, promote this as an under-reported program, and we want to work with the Department. If the budget doesn't exist, then we will in the community—in the private sector are willing to do our fair share in terms of promoting this.

That is part of our outreach, and we have been in discussions with S&T about just those very things in light of the realities of today, which is there isn't a lot of money, as Mr. Benda said, to in essence do more on that. But the private sector, because it wants it to be successful, is prepared to step in and take on its role and responsibility.

Ms. CLARKE. Thank you.

Mr. LUNGREN. Mr. Pearl, do we have a copy of that report you are talking about?

Mr. PEARL. I sent it electronically, and if you can include it in the——

Mr. LUNGREN. Okay. Without objection, we will include that as part of the record.*

Mr. PEARL. Thank you.

Mr. LUNGREN. All right. I just want to thank all of you for your testimony. It has been very, very helpful.

I still have some questions that I am going to work out. I mean, if renewal is so important, why aren't more companies attempting to get renewal? That would either tell me that either the companies don't find certification to be that important or somehow there is a stumbling block to get recertification, and it would work against the intent of the program.

We are going to try and work with the Department and work with you and others to make sure this works. This subcommittee wants it to work effectively, and so we are going to exercise vigorous oversight over this program.

I am going to request that we have quarterly briefings for our subcommittee by the Department on this issue, because I just happen to think—this is a bipartisan thing. There is no partisanship involved here. My comments were directed towards DHS both under Republicans than Democrats.

I know it is a maturation process, but maturation, hopefully, results in not only better understanding, but ease of application. I think everybody seems to agree we need to get the word out to more people so that they would see the importance of it.

I guess we ought to make sure that the Federal procurement officers are aware of this and that that may be one of the best outreach programs we have got. But I don't want it to be another sense of bureaucracy, that a procurement officer mentions it to a potential supplier and all of a sudden they go, "Oh, my god, I can't get it" or "I have heard the horror stories" or "once I get it, do I keep it" and all those sorts of things.

So thank you. Your testimony has been very, very helpful. We are committed to making sure this works. You have helped us greatly on this. You have also been very helpful—every one of you stayed within seconds of the 5 minutes we asked you to begin with, which I must tell you is very, very rare here.

So I thank you for your valuable testimony, and the Members who were in attendance for their questions. The Members of the committee may have some additional questions that they would submit to you in writing, and we would ask you to respond in writing, if possible. The hearing record will be held open for 10 days, and this subcommittee stands adjourned.

[Whereupon, at 11:22 a.m., the subcommittee was adjourned.]

○

*The information has been retained in committee files.