AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IMPLEMENTING THE SAFETY ACT: ADVANCING NEW TECHNOLOGIES FOR HOMELAND SECURITY

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

OCTOBER 17, 2003

Serial No. 108–96

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

91–553 PDF WASHINGTON : 2004

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 GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on October 17, 2003	1
Statement of:	
Albright, Parney, Assistant Secretary for Plans, Programs and Budgets, Department of Homeland Security	12
Miller, Harris N., president, Information Technology Association of America; Stan Z. Soloway, president, Professional Services Council; and John M. Clerici, esq., on behalf of the U.S. Chamber of Commerce	36
Letters, statements, etc., submitted for the record by:	
Albright, Parney, Assistant Secretary for Plans, Programs and Budgets, Department of Homeland Security, prepared statement of	15
Clerici, John M., esq., on behalf of the U.S. Chamber of Commerce, prepared statement of	69
Cummings, Hon. Elijah E., a Representative in Congress from the State of Maryland, prepared statement of	122
Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of	4
Maloney, Hon. Carolyn B., a Representative in Congress from the State of New York, prepared statement of	30
Miller, Harris N., president, Information Technology Association of America:	
Application kit	79
Prepared statement of	39
Ruppersberger, Hon. C.A. Dutch, a Representative in Congress from the State of Maryland, prepared statement of	22
Soloway, Stan Z., president, Professional Services Council, prepared statement of	60
Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of	8

IMPLEMENTING THE SAFETY ACT: ADVANCING NEW TECHNOLOGIES FOR HOMELAND SECURITY

FRIDAY, OCTOBER 17, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 10:10 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Tom Davis of Virginia, Ose, Schrock, Duncan, Carter, Waxman, Maloney, Cummings, Ruppersberger, and Bell.

Staff present: Peter Sirh, staff director; Melissa Wojciak, deputy staff director; Keith Ausbrook, chief counsel; John Hunter and David Young, counsels; David Marin, director of communications; John Cuaderes, senior professional staff member; Teresa Austin, chief clerk; Brien Beattie, deputy clerk; Corinne Zaccagnini, chief information officer; Michelle Ash, minority counsel; Jean Gosa, minority assistant clerk; and Cecelia Morton, minority office manager.

Chairman TOM DAVIS. Good morning. A quorum being present, the Committee on Government Reform will come to order.

I want to welcome everybody to today's hearing on the implementation of the Support Antiterrorism by Fostering Effective Technologies Act of 2002 [SAFETY Act]. The private sector is an important partner in providing for the security of our homeland. To ensure that private sellers, manufacturers and service providers contribute to homeland security by developing potentially life-saving technologies without having the fear of crippling or frivolous lawsuits, the government needs to provide litigation and risk management frameworks to adequately prepare for terrorist attacks.

As part of the Homeland Security Act of 2002, Public Law 107–296, Congress enacted the SAFETY Act to provide incentives for the development and deployment of antiterrorism technologies by creating systems of risk management and litigation management. The SAFETY Act seeks to ensure that the threat of liability does not deter manufacturers or sellers of antiterrorism technologies from developing and commercializing technologies that could save lives. The act creates certain frameworks for "claims arising out of, relating to or resulting from an act of terrorism" where qualified antiterrorism technologies are deployed. The act does not limit liability for harms caused by antiterrorism technologies when no acts of terrorism have occurred.

The SAFETY Act directs the Department of Homeland Security to adopt regulations to implement the liability protections conferred by the act for qualified antiterrorism technologies. Under the statute, these qualified technologies would receive several protections, including limiting lawsuits filed under the act to the Federal courts, prohibiting a plaintiff from recovering punitive damages, or permitting recovery of noneconomic damages such as damages for physical or emotional pain, and reducing any recovery from the seller by the amount of any collateral sources such as insurance payments.

Some technologies qualified under the act may also qualify for a rebuttable "government contractor defense." The government contractor defense could provide sellers and manufacturers immunity from product liability altogether when the qualified technology is deployed for the purposes of defending against or responding to a terrorist act.

Under the act DHS can certify that the seller or manufacturer will receive this rebuttable defense if DHS determines that the technology will perform as intended, conforms to the seller's specifications and is safe for the use it's intended. But the defense will not protect sellers and manufacturers against charges of fraud or willful misconduct. The act requires DHS to adopt rules to implement the protections in the act. The timely adoption and implementation of those rules is the reason for our hearing today.

On July 11, 2003, DHS announced the draft regulations implementing the SAFETY Act that were published in the Federal Register for public comment. Over 40 private firms and private sector associations submitted comments. An interim final rule has been released to the public.

By passing the SAFETY Act, Congress acted quickly to resolve uncertainty over liability concerns so that the full power of the American technology could be unleashed in the war on terrorism. We gave DHS responsibility to develop a transparent process to accomplish these objectives. It is imperative that DHS begin qualifying existing and new technologies so that they can be placed in the hands of those who need them now, especially for those high-priority homeland security procurements that have been on hold pending the qualification of antiterrorism technologies already selected for use.

For its part, when DHS issued the draft regulations in July, it stated it would begin accepting applications for SAFETY Act protections on September 1st, but the actual form to be used for private firms to qualify antiterrorism technologies wasn't approved by OMB until this week. Also the interim final rule was only issued by DHS this week. As a result of these bureaucratic delays, private firms have waited to submit applications until they have some finality in the application process and implementing regulations. It's imperative that DHS now mobilize its efforts to accomplish the critical purposes set out in the SAFETY Act.

In so doing, DHS must identify and implement a clear strategy for prioritizing the many applications it will receive for the qualification of antiterrorism technologies. Congress did not intend for the SAFETY Act to be used solely as a means for the development of "new" antiterrorism technologies. While developing new tech-

nology is essential, I believe DHS needs to focus on qualifying "existing" antiterrorism technologies that are ready to be deployed to protect our civilian population. I urge the Department to make as its No. 1 priority the identification, prioritization and qualification of existing antiterrorism technologies that are now being sought by Federal and non-Federal entities. It's imperative that we protect the highest-priority facilities and critical infrastructures in high-risk locations.

In addition, DHS must be careful that its implementing regulations and processes are not so complicated that they defeat the very purpose of the SAFETY Act. They should allow for the rapid deployment of antiterrorism technology necessary to protect the American people rather than create burdensome red tape and bureaucracy. Wherever possible, decisions regarding the suitability of antiterrorism technology should rest with those entities charged with the responsibility of acquiring the technology. It's also imperative that DHS adheres to a disciplined time schedule for processing applications.

Through this hearing the committee intends to learn about the interim final rule promulgated by DHS and whether the rule effectuates the congressional intent of the act. The committee hopes this open discussion will result in effective implementation of the act.

We have assembled an impressive group of witnesses to help us understand the statute, the proposed rules and the private sector concerns about the proposed rules.

I want to thank all of our witnesses for appearing before the committee. I look forward to their testimony, and I now yield to Mr. Waxman.

[The prepared statement of Chairman Tom Davis follows:]

Opening Statement
Chairman Tom Davis
"Implementing the SAFETY Act: Advancing New Technologies for Homeland Security"
October 17, 2003

Good morning. A quorum being present, the Committee on Government Reform will come to order. I would like to welcome everyone to today's hearing on the implementation of the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002. The private sector is an important partner in providing for the security of the homeland. To ensure that private sellers, manufacturers and service providers contribute to homeland security by developing potentially life-saving technologies without having to fear crippling or frivolous lawsuits, the government needs to provide litigation and risk management frameworks to adequately prepare for a terrorist attack.

As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the SAFETY Act to provide incentives for the development and deployment of anti-terrorism technologies by creating systems of "risk management" and "litigation management." The SAFETY Act seeks to ensure that the threat of liability does not deter manufacturers or sellers of anti-terrorism technologies from developing and commercializing technologies that could save lives. The Act creates certain frameworks for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified anti-terrorism technologies are deployed. The Act does not limit liability for harms caused by anti-terrorism technologies when no act of terrorism has occurred.

The SAFETY Act directs the Department of Homeland Security to adopt regulations to implement the liability protections conferred by the Act for Qualified Anti-Terrorism Technologies. Under the statute, these qualified technologies would receive several protections, including:

- Limiting lawsuits filed under the Act to Federal courts;
- Prohibiting a plaintiff from recovering punitive damages, but permitting recovery of non-economic damages, such as damages for physical and emotional pain; and
- Reducing any recovery from the seller by the amount of any collateral sources, such as insurance payments.

Some technologies that qualify under the Act may also qualify for a rebuttable "government contractor defense." The "government contractor defense" could provide sellers and manufacturers immunity from product liability altogether when the qualified technology is deployed for the purposes of defending against or responding to a terrorist act.

Under the Act, DHS can certify that the seller or manufacturer will receive this rebuttable defense if DHS determines that the technology will perform as intended, conforms to the seller's specifications, and is safe for use as intended. But the defense will not protect sellers and manufacturers against charges of fraud or willful misconduct. The Act requires DHS to adopt

rules to implement the protections in the Act. The timely adoption and implementation of those rules is the reason for our hearing today.

On July 11, 2003, DHS announced draft regulations implementing the SAFETY Act that were published in the *Federal Register* for public comment. Over forty private firms and private sector associations submitted comments. An interim final rule has been released to the public.

By passing the SAFETY Act, Congress acted quickly to resolve uncertainty over liability concerns so that the full power of American technology could be unleashed in the war on terrorism. We gave DHS responsibility to develop a transparent process to accomplish these objectives. It is imperative that DHS begin qualifying existing and new technologies so they can be placed in the hands of those who need them now, especially for those high priority homeland security procurements that have been "on hold" pending the qualification of anti-terrorism technology already selected for use.

For its part, when DHS issued the draft regulations in July, it stated it would begin accepting applications for SAFETY Act protections on September 1, 2003. But the actual form to be used for private firms to qualify anti-terrorism technologies was not approved by OMB until this week. Also, the interim final rule was only issued by DHS this week. As a result of these bureaucratic delays, private firms have waited to submit applications until they have seen some finality in the application process and implementing regulations. It is imperative that DHS now mobilize its efforts to accomplish this critical purpose of the SAFETY Act.

In so doing, DHS must identify and implement a clear strategy for prioritizing the many applications it will receive for the qualification of anti-terrorism technologies. Congress did not intend for the SAFETY Act to be used solely as a means for the development of "new" anti-terrorism technologies. While developing new technology is essential, I believe DHS needs to focus on qualifying "existing" anti-terrorism technologies that are ready to be deployed to protect our civilian population. I urge DHS to make as its number one priority the identification, prioritization and qualification of "existing" anti-terrorism technologies that are now being sought by federal and non-federal entities. It is imperative that we protect the highest priority facilities and critical infrastructure in high risk locations.

In addition, DHS must be careful that its implementing regulations and processes are not so complicated that they defeat the very purpose of the SAFETY Act. They should allow for the rapid deployment of anti-terrorism technology necessary to protect the American people, rather than create burdensome red tape and bureaucracy. Wherever possible, decisions regarding the suitability of anti-terrorism technology should rest with those entities charged with the responsibility of acquiring the technology. It is also imperative that DHS adheres to a disciplined time schedule for processing applications.

Through this hearing, the Committee intends to learn about the interim final rule promulgated by DHS and whether the rule effectuates the Congressional intent of the Act. The Committee hopes this open discussion will result in effective implementation of the Act.

We have assembled an impressive group of witnesses to help us understand the statute, the proposed rules, and the private sector concerns about the proposed rules. We will first hear from The Honorable Parney Albright, Assistance Secretary for Plans, Programs, and Budgets of the Department of Homeland Security. Next, we will hear from private sector witnesses: Mr.

Harris Miller, President of the Information Technology Association of America; Mr. Stan Z. Soloway, President of the Professional Services Council; and Mr. John Clerici, representing the U.S. Chamber of Commerce.

I would like to thank all of our witnesses for appearing before the Committee, and I look forward to their testimony.

Mr. WAXMAN. Thank you very much, Mr. Chairman. I agree that the private sector can and should develop new and innovative technologies to respond to the ever-changing threats to the American people. I support all efforts to make the people of the United States safer, and I believe that the private sector has a role to play. I'm glad that the representatives of the private sector are here today to discuss their intentions to create these new technologies.

However, the SAFETY Act, which we are discussing today, is a disappointment and moves in the wrong direction. This law is not about encouraging innovation, but rather its goal is to limit the legal liability of the defense contractors and other manufacturers of antiterrorism products and, in many circumstances, to give them absolute immunity. Even in those cases where there may be limited liability, the law bars access to State courts, eliminates punitive damages, eliminates joint liability, limits all forms of liability to the cost of, "reasonably priced," insurance, and reduces judgments by the amount of insurance or other collateral source benefits. And while limiting or eliminating the liability of manufacturers, the law also severely restricts the ability of claimants to recover damages for their injuries, because it fails to provide for any alternative form of compensation or indemnification.

This act is ironically called the SAFETY Act, when in reality the only safety it provides is to corporate wrongdoers. Corporations that sell defective products will now have nothing to fear. They will either have very limited liability or no liability at all. Let me give an example. Suppose the Homeland Security Department approves a process designed to test the water supply for contamination. The sellers of this service later discover that their process is ineffective, but continue to earn huge profits by falsely promising the safety of the water supply. If terrorists exploit this weakness, and citizens are poisoned by contaminated water, the sellers of the service are totally immune from all forms of liability if the product was certified for the government contractor defense. This is true even though their misconduct was intentional. This makes absolutely no sense. Why would we want to give corporations protection for intentional, knowing misbehavior?

Mr. Chairman, as you know, I supported the Turner amendment to the Homeland Security Act extending indemnification protections to antiterrorism technologies. I believe Mr. Turner's amendment would have appropriately mitigated the seller's risk of proposal liability. Unfortunately, the Turner amendment lost in the House by 1 vote, and thus we are left with the SAFETY Act—immunity instead of indemnity.

Although I did not support the SAFETY Act, I will agree that the SAFETY Act, like all laws, should be properly enforced by the administration. Therefore, I appreciate that we are having this oversight hearing today, and I look forward to hearing and reading the testimony on how the administration intends to implement this act.

Chairman TOM DAVIS. Well, thank you very much.

[The prepared statement of Hon. Henry A. Waxman follows:]

Statement of Henry A. Waxman
Committee on Government Reform
Hearing on "Implementing the SAFETY Act:
Advancing New Technologies for Homeland Security"
October 17, 2003

Mr. Chairman, I agree that the private sector can and should develop new and innovative technologies to respond to the ever-changing threats to the American people. I support all efforts to make the people of the United States safer and I believe that the private sector has a role to play. I am glad that representatives of the private sector are here today to discuss their intentions to create these new technologies.

However, the SAFETY Act, which we are discussing today, is a disappointment and moves in the wrong direction.

This law is not about encouraging innovation. Rather, its goal is to limit the legal liability of the defense contractors and other manufacturers of anti-terrorism products and, in many circumstances, to give them absolute immunity. Even in those cases where there may be limited liability, the law bars access to state courts, eliminates punitive damages, eliminates joint liability, limits all forms of liability to the cost of "reasonably priced" insurance, and reduces judgments by the amount of insurance or other collateral source benefits.

And while limiting or eliminating the liability of manufacturers, the law also severely restricts the ability of claimants to recover damages for their injuries because it fails to provide for any alternative form of compensation or indemnification.

This Act is ironically called the SAFETY Act when, in reality, the only safety it provides is to corporate wrongdoers. Corporations that sell defective products will now have nothing to fear. They will either have very limited liability or no liability at all.

Let me give you an example. Suppose the Homeland Security Department approves a process designed to test the water supply for contamination. The sellers of this service later discover that their process is ineffective but continue to earn huge profits by falsely promising the safety of the water supply. If terrorists exploit this weakness, and citizens are poisoned by contaminated water, the sellers of this service are totally immune from all forms of liability if the product was certified for the government contractor defense. This is true even though their misconduct was intentional.

This makes absolutely no sense. Why would we want to give corporations protection for intentional, knowing misbehavior?

Mr. Chairman, as you know, I supported the Turner amendment to the Homeland Security Act extending indemnification protections to anti-terrorism technologies. I believe Mr. Turner's amendment would have appropriately mitigated the sellers' risk of potential liability. Unfortunately, the Turner amendment lost in the House by one vote and thus, we are left with the SAFETY Act — immunity instead of indemnity.

Although I did not support the SAFETY Act, I will agree that the SAFETY Act, like all laws, should be properly enforced by the Administration. Therefore, I appreciate that we are having this oversight hearing today and I look forward to hearing how the Administration intends to implement this Act.

Chairman TOM DAVIS. Mr. Ose, any opening statement? Any other Members wish to make an opening statement?

Well, let's move to our first panel. I want to thank the honorable Parney Albright, the Assistant Secretary for Plans, Programs and Budgets of the Department of Homeland Security. It's the policy of this committee to swear people in before they testify. Would you rise and raise your right hand?

[Witness sworn.]

Chairman TOM DAVIS. We have your whole statement in the record. We have a light in front of you; when it turns orange, you'll be 4 minutes into your statement; red, 5 minutes, and if you could sum up about that time. Thanks for being with us.

STATEMENT OF PARNEY ALBRIGHT, ASSISTANT SECRETARY FOR PLANS, PROGRAMS AND BUDGETS, DEPARTMENT OF HOMELAND SECURITY

Mr. ALBRIGHT. Thank you, Mr. Chairman, Mr. Waxman, committee members. I'm pleased to appear before you today to discuss the Department of Homeland Security's implementation of the Support Antiterrorism by Fostering Effective Technologies Act of 2002 [SAFETY Act]. As you may know, the SAFETY Act provides incentives for the development and deployment of qualified antiterrorism technologies by creating a system of "risk management" and a system of "litigation management." The SAFETY Act is part of the Homeland Security Act of 2002, which is the organic legislation of the Department of Homeland Security.

With the creation of the Department of Homeland Security, President Bush envisioned an organization that would engage entrepreneurs and tap America's inventive spirit in the war on terrorism. The Science and Technology Division of the Department is specifically tasked with marshalling the intellectual capital of the engineering and scientific communities to develop fresh and effective approaches to safeguard the American public from terrorist attacks. The SAFETY Act is an important vehicle for removing obstacles to the deployment of these capabilities to the field.

Now, the purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential manufacturers of qualified antiterrorism technologies from developing and commercializing technologies that could significantly reduce the risks or mitigate the effects of large-scale terrorist events. The act does create certain liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified antiterrorism technologies have been deployed. The act does not limit liability for harms caused by antiterrorism technologies when no act of terrorism has occurred, as was pointed out by the chairman.

Clearly, the issue Congress is addressing concerns the uncertain risk environment born out of the threat of terrorism. The potential risks and liabilities that stem from the technologies deployed in our war against terrorism are very difficult to quantify. As a result, in many cases insurance has been largely unattainable or so costly as to leave the technologies in question without a market. It is hardly surprising that companies are unwilling to bet their existence by developing and deploying services and products in this uncertain climate. This means that key capabilities needed to secure the

homeland may not be available for deployment. The SAFETY Act does serve to encourage the development and deployment of antiterrorism technologies that will significantly enhance the protection of the Nation by providing certain liability protections to allow the vast resources of the national research and development enterprise to be engaged for securing the homeland.

Given the significance and complexity of this groundbreaking statute, the Department of Homeland Security decided to develop and publish a regulation setting forth the Department's policies and procedures for its implementation. The Department solicited comments on the proposed SAFETY Act regulation this summer and published an interim final rule that was signed by Secretary Ridge on October 10th, incorporating suggestions from many of the thoughtful comments provided by almost 45 organizations and individuals during the first public comment period. Under the interim rule, we will continue to accept and entertain comments as we begin the process of executing the act. The Department is, under the rule, implementing the SAFETY Act within the Science and Technology Division and I, as Assistant Secretary, am responsible for evaluating applications and recommending to the Under Secretary for Science and Technology whether antiterrorism technologies should be approved or rejected for a designation or certification under the authority delegated to him by the Secretary under the regulation.

Users of a technology designated as a qualified antiterrorism technology under the SAFETY Act enjoy significant liability protection. Specifically, liability is limited in scope to only the seller of the technology and is limited to an amount where the requisite insurance coverage does not unreasonably distort the price of the technology. The statute provides for a very broad definition of "technology," including tangible products, software and services, including support services.

The seven criteria specified in the statute for designation of a technology seek, in essence, three kinds of information. The first is technical. Does the technology work? Does it provide useful levels of performance in scenarios of interest? Is it mature? What specific threats does the technology address? What is the level of risk exposure to the public if the technology is not deployed? And then there are economic and actuarial issues. How does the risk of liability affect demand for the product toward its deployability? What are the liability risks? There are additional criteria associated with certification. In particular, detailed safety and hazard data are required in the statute in order for a technology to qualify for the government contractor defense presumption.

This presents a very complex and unusual analytic challenge. We are striving for consistent and equitable methodologies that implement the intent of Congress while retaining flexibility to assess the vast array of potential technologies within a constantly changing threat environment. To do this we have created a SAFETY Act Office to house permanent Federal staff to oversee the effort. We have over 100 government scientists and engineers in the Science and Technology Directorate along with the vast resources of our national labs to help evaluate the required data and perform the requisite analyses.

We have, to assist us in these efforts, the support of Mr. Joe Whitley, the DHS General Counsel. He and his staff have played a pivotal role during the rulemaking process and are available to address legal policy issues as they arise.

We have contracted with an FFRDC—or actually, we are in the process of contracting with an FFRDC to provide analytic support, and they bring a broad-capacity performing requisite, proven objectivity and ability to access both classified and proprietary data. They also provide a broad and deep capacity for performing the requisite economic analyses and have supplemented their expertise with specialists from a number of academic institutions. We're also working with academia, in particular Georgia State University, the University of Georgia and others to evaluate actuarial data.

And then finally, we have contracted with Integrated Data Systems to develop and implement a Web-based application and evaluation tracking process. This is intended to provide an online tracking capability so that businesses can check the status of their applications and for the government to efficiently evaluate, monitor and archive the application.

We've implemented a pre-application process to assist particularly small businesses in this process so they can get an initial read on their application without having to go through the trouble and expense of filling the full application out.

Recently, I and my SAFETY Act team went on the road and held seminars and fielded questions in Dallas, Los Angeles, Atlanta, Chicago and, just this past Tuesday, in Washington, DC, to inform the American business community about the act and its implementation. The interim rule is in place. The application kit is available. The information seminars are complete. We are now initiating implementation of the act.

Thank you for the opportunity to address this important issue with you today, and I look forward to your questions.

Chairman TOM DAVIS. Thank you.

[The prepared statement of Mr. Albright follows:]

Statement for the Record

Dr. Penrose Albright
Assistant Secretary for Science and Technology
Department of Homeland Security

Before the Committee on Government Reform
U.S. House of Representatives

Introduction

Mr. Chairman, Mr.Waxman, Committee Members, I am pleased to appear before you today to discuss the Department of Homeland Security's implementation of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 ("the SAFETY Act"). As you may know, the SAFETY Act provides incentives for the development and deployment of qualified anti-terrorism technologies (ATTs) by creating a system of "risk management" and a system of "litigation management." , The SAFETY Act is part of the Homeland Security Act of 2002, which is the organic legislation of the Department of Homeland Security.

With the creation of the Department of Homeland Security, President Bush envisioned an organization that would engage entrepreneurs and tap America's inventive spirit in the war on terrorism. The Science and Technology (S&T) Division of the Department is specifically tasked with marshalling the intellectual capital of the engineering and scientific communities to develop fresh and effective approaches to safeguard the American public from terrorist attacks. The SAFETY Act is an important vehicle for removing obstacles for the deployment of these capabilities to the field.

Implementation of the SAFETY Act

The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential manufacturers of qualified ATTs from developing and commercializing technologies that could significantly reduce the risks or mitigate the effects of large-scale terrorist events. The Act thus creates certain liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified ATTs have been deployed. The Act does not limit liability for harms caused by ATTs when no act of terrorism has occurred. Clearly, the issue Congress is addressing concerns the uncertain risk environment born out of the threat of terrorism. The potential risks and liabilities that stem from the technologies deployed in our war against terrorism are very difficult to quantify. As a result, in many cases insurance has become largely unobtainable or so costly as to leave the technologies in question without a market. It is hardly surprising that companies are unwilling to bet their existence by developing and deploying

services and products in this uncertain climate. This means that key capabilities needed to secure the homeland may not be available for deployment. The SAFETY Act thus serves to encourage the development and deployment of ATTs that will significantly enhance the protection of the nation by providing certain liability protections to allow the vast resources of the national research and development enterprise to be engaged for securing the homeland.

Given the significance and complexity of this groundbreaking statute, the Department of Homeland Security decided to develop and publish a regulation setting forth the Department's policies and procedures for its implementation. The Department solicited comments on the proposed SAFETY Act regulation this summer and published an interim final rule that was signed by Secretary Ridge on October 10th, incorporating suggestions from many of the thoughtful comments provided by almost 45 organizations and individuals during the first public comment period. Under the interim rule, we will continue to accept and entertain comments as we begin the process of executing the Act.

The Department is, under the Rule, implementing the SAFETY Act within the Science & Technology Directorate and I, as Assistant Secretary, am responsible for evaluating applications and recommending to the Under Secretary for Science and Technology whether ATTs should be approved or rejected for a designation/certification, under the authority delegated to him by the Secretary under the SAFETY Act.

Users of a technology designated as a qualified anti-terrorism technology under the SAFETY Act enjoy significant liability protection. Specifically, liability is limited in scope to only the seller of the technology, and is limited to an amount where the requisite insurance coverage does not unreasonably distort the price of the technology. The statute provides for a very broad definition of "technology," including tangible products, software and services (including support services).

The seven criteria specified in the statute for designation of a technology seek, in essence, three kinds of information:

- Technical –Does the technology work? Does it provide useful levels of performance in scenarios of interest? Is it mature enough for near-term deployment?

- Threats addressed — What specific threats does the technology address? What is the level of risk exposure to the public if the technology is not deployed?

- Economic and actuarial — How does the risk of liability affect demand for the product or its deployability? What are the liability risks?

Additional criteria are associated with Certification. In particular, detailed safety and hazard data are required in the statute in order for a technology to qualify for the government contractor defense presumption.

This suite of criteria presents a very complex and unusual analysis challenge. We are striving for development of a consistent and equitable methodology that implements the intent of Congress, while retaining flexibility to assess a vast array of potential technologies within a constantly changing threat environment.

I will now describe the infrastructure that has been created to fulfill our responsibilities to implement the SAFETY Act effectively.

We have created a SAFETY Act Office to house permanent federal staff to oversee this effort. The technical experts in my office — supported by over 100 government scientists and engineers in the Science and Technology Directorate along with the vast resources at our national labs— will be responsible for evaluating the required data and analyses. These highly skilled professionals work with me to provide the basis for my recommendation to the Under Secretary regarding the granting of Designations and Certifications.

To assist us in these efforts, I am fortunate to have the full support of Mr. Joe Whitley, the DHS General Counsel. He and his staff have played a pivotal role during the rulemaking process and are available to address legal policy issues as they arise.

We are contracting with the Institute for Defense Analyses (IDA), a Federally-funded Research and Development Center (FFRDC), to provide analytic support. IDA has long provided similar support to the Department of Defense (DOD), including DoD's Operational Test & Evaluation Office. IDA understands how to evaluate test data when applied to a variety of threat scenarios, how to perform experimental design and have experience with a wide range of national security technologies. As an FFRDC, they provide proven objectivity and ability to access both classified and proprietary data. They also provide a broad and deep capacity for performing the requisite economic analyses and have supplemented their expertise with specialists from Yale, Cornell, the University of Michigan, the University of California – Davis, and Syracuse. They are also working closely with academia, including Georgia State University, the University of Georgia, Carnegie-Mellon, and the University of Wisconsin, to assist us in establishing a process to evaluate actuarial data.

We have also entered into a contract with Integrated Data Systems (IDS) to develop and implement a Web-based application and evaluation tracking process. IDS has created similar systems for DoD's Technical Support Working Group in their web-based proposal system, and we are using their secure and user-friendly approach as a springboard. In addition to providing a process to file an application, IDS also provides an on-line tracking capability so that businesses can check the status of their applications, and for the Government to efficiently evaluate, monitor, and archive application information.

We are implementing a "Pre-Application process" to assist businesses—particularly small businesses—in this process. This voluntary pre-application process allows businesses to get an "initial read" on the likelihood that their technology will meet the criteria for designation before going through the expense of preparing a full application. It also allows businesses of all types to get a similar advisory opinion early in the development process.

Recently, I and my SAFETY Act team went on the road, holding seminars and fielding questions in Dallas, Los Angeles, Atlanta, Chicago and, just this past Tuesday, in Washington, DC, to inform American business people about the Act and its implementation.

The interim rule is in place, the application kit is available, and the information seminars are complete. We are now initiating the implementation of the Act. We expect that as we move

forward we will learn more efficient and effective ways to facilitate the deployment of technologies important to securing the homeland.

Thank you for this opportunity to address this important issue with you today. I look forward to your questions.

Chairman TOM DAVIS. Mr. Ruppersberger, I know you had to make——

Mr. RUPPERSBERGER. Thank you for letting me go, Mr. Chairman. First I applaud the committee and you, Mr. Chairman, for holding this hearing today on implementing the SAFETY Act. It is refreshing to be assessing the progress of implementation as that process is underway. It seems these issues often occur and come to our attention after a problem arises. As one who was not a Member of Congress when this legislation passed—and I understand the liabilities debate that took place—I think this oversight hearing is extremely important at this point in the process.

I'm encouraged that Congress is working with the Department of Homeland Security and the other stakeholders to acquire the technology and tools we need so desperately to protect our country. Technology is an integral part of our world today. It is a critical tool to solve both business and government problems. Never has the need for advanced technology solutions been more important than in the war on terror.

I agree with the research incentives the SAFETY Act provided to encourage the private sector to find the best tools available to help us achieve this victory but, as we all know, technology is not perfect, and there are inherent difficulties. Balancing the good with the problematic is the difficult challenge the Department of Homeland Security faces today. Balancing the realities of indemnity versus immunity is a difficult challenge for Congress. I commend the Department for making the rule process so open and public, and I hope that the comments offered will be carefully reviewed and incorporated into the final rule. Thank you.

Chairman TOM DAVIS. Thank you very much.

[The prepared statement of Hon. C.A. Dutch Ruppersberger follows:]

Congressman C.A. Dutch Ruppersberger
Committee on Government Reform
Implementing the Safety Act: Advancing New Technologies for Homeland Securities
Opening Remarks
10.17.03

Thank you Mr. Chairman. I applaud the committee and its leadership for holding this hearing today on Implementing the SAFETY Act.

It is refreshing to be assessing the progress of implementation as that process is underway. It seems these issues often come to our attention after a problem arises.

While I was NOT a Member of Congress when this legislation passed and I understand the liabilities debate that took place, I think this oversight hearing is extremely important at this point in the process. I am encouraged that Congress is working with the Department of Homeland Security and the other stakeholders to acquire the technology tools we so desperately need.

Technology is an integral part of our world today. It is a critical tool to solve both business and government problems. Never has the need for advanced technological solutions been more important than in this war on terror. I agree with the research incentives the SAFETY Act provided to encourage the private sector to find the best tools available to help us achieve victory.

But as we all know, technology is not perfect and there are inherent difficulties. Balancing the good with the problematic is the difficult challenge the Department of Homeland Security faces today. Balancing the realities of indemnity vs. immunity is the difficult challenge for Congress.

I commend the department to making the rule making process so open and public. And I hope that the comments offered will be carefully reviewed and incorporated in their final rule.

I look forward to the important testimony today and again, Mr. Chairman, I thank the committee for such timely engagement in this process.

Chairman TOM DAVIS. Let me ask, what has taken so long to get this thing up?

Mr. ALBRIGHT. Well, Mr. Chairman, we—as you know, the Department—the SAFETY Act in principle was signed into law on January 24th. The departmental resources became available on March 1st, and we published a draft rule, as you pointed out, this summer. As you well know, this is normally an 18-month process to get——

Chairman TOM DAVIS. But we're fighting a war on terrorism, and we want to get these products in there. If it's business as usual in terms of moving things through, we're not going to accomplish the mission.

Now, we had a huge fight on the Hill whether to take Mr. Turner's indemnification or to take this. The administration wanted this. I actually prefer Mr. Turner's, but I gave deference to the administration in terms of the way we do this. This act was passed so that we could encourage companies who have products that can help us fight the war on terrorism to participate in the government procurement process. These are companies that traditionally don't do it. That is the goal of this legislation, and we have companies out there screaming and not knowing what is going on. And, you know, the faster we get these products up and running, the safer we are. And I think that has been the purpose of it. I mean, Mr. Waxman talked about—his example really I don't think is correct under the law. My understanding is a SAFETY Act designation isn't valid if the technology doesn't perform as it's stated when it's approved by DHS. DHS will put the criteria around each approved designation. If the criteria aren't met, then there's liability. If the criteria are met, then you obviously don't have the same vulnerability. That was the purpose of this.

Mr. ALBRIGHT. Mr. Chairman, I would agree with you. This is not a situation where we want to perform business as usual. As I started to say, what we've done is we have taken a process that normally takes 18 to 24 months, and we've compressed it to 7. This is an extraordinarily complex piece of legislation. It's short in the act, but it's very complex, and the complexities of the implementation are what led us to, in fact, publish a rule—have the desire to publish a regulation in the first place. And then as I pointed out in my opening comments, we've got a lot of very thoughtful responses from industry and from individuals about the draft rule that we felt it important to carefully consider and include where relevant in the draft interim rule. So actually I'm actually very proud of the fact that this Department has managed to get, as I said, a very lengthy regulatory process compressed to an extraordinarily short period of time.

I do agree with your point. Let me just add that technologies that don't work, we intend, for example, to fully look at the set of technical data that is available for technologies and the test and evaluation data that's available, and look at the scenarios that are relevant to those technologies, and assess whether or not it, in fact, is effective. And if it turns out that it is not effective, then I would agree with you. I think that would then cause the technology to fall outside the contours of the designation——

Chairman TOM DAVIS. Let me ask you this. Since this process is so complicated, since it's highly interactive, it's specific to each individual application, do we have any internal appeal process of the decision by the Secretary? Then it makes sense to provide some review process within DHS rather than subject applicants in the Department to a court review, which is what you get otherwise.

Mr. ALBRIGHT. I think actually the way you stated the question, that actually is a rationale for why we have not included a formal appeal process in this. This is, as you said, an extraordinarily complex and nuanced process with a great deal of interaction that occurs between the applicant fix and the reviewers. To put in an appeals process by someone who really hasn't been exposed to that very complex review of technical and financial and actuarial data would leave us open, frankly, to capriciousness, we think, and second-guessing. Or the person who would be conducting the appeal would be in a situation where they would just simply ask the Under Secretary for their opinion again, and they would get it again. So it either would fall into the category of a pro forma appeal or, I think, lead us down the path toward a capricious implementation of the act.

Chairman TOM DAVIS. Well, let me ask you this. Do you think you're taking into account the users of the technology and their needs as opposed to what you think they need? I mean, do you have any conversations——

Mr. ALBRIGHT. Absolutely. Of course we're going to consider and provide considerable weight to the needs of the user community when considering the efficacy of the technology in question. There's a wide variety of such needs, and very different threat environments, large differences in the availability of existing countermeasures, and all of those things drove the need to maximize the flexibility of the implementation of the act and to avoid a one-size-fits-all implementation, as you're implying in your statement—in your question.

It's important to know, however, that translating a user's effectiveness needs into measurable technical performance parameters is a complex and often difficult process, and as I would expect very close interaction between the scientists and engineers who must review the technical performance data and the user community, which, of course, is—they just want something that works.

Chairman TOM DAVIS. Thank you.

Mr. Bell.

Mr. BELL. Thank you, Mr. Chairman. And thank you for your testimony here today.

Since the Department is now seeking further comment on the interim rule, I'm curious as to when we could expect any new regulations from the Department coming forward.

Mr. ALBRIGHT. Let's see. The comment period is open for an additional 60 days, and at that time we would have to assess and review the comments and determine what changes are necessary in the finalization of the rule, if any, and then we would begin the process of finalizing the rule at that time.

Mr. BELL. How long do you think the review process of the comments will take?

Mr. ALBRIGHT. It clearly depends on the complexity of the comments, but I would expect—in the last case it took a few weeks—so I would expect that to be the case this time around as well.

Mr. BELL. As far as a timeline goal, do you have one as we——

Mr. ALBRIGHT. Let's see. You know, I always hesitate to nail myself down to a date, but let's say that—as I said, a comment period closes in 60 days; that's mid-December. So there's no reason why after the holidays you wouldn't see a final rule, say mid-January, something like that.

Mr. BELL. As the Chair pointed out, it is a rather complex process, and I'm curious as to what is in place to protect the proprietary information throughout the entire process.

Mr. ALBRIGHT. It is our belief and the belief of our general counsel that current FOIA exemptions protect the proprietary nature of the information that would be provided in the application. And then, of course, there's also the Federal Trade Secrets Act which provides for criminal penalties for those who unlawfully disclose proprietary information to the public. So that is our belief at this time. We are, of course, continuing to review that. As you know, that is a comment we have received. We've received quite a few comments on that issue, and so we're continuing to review that, and should we find that, in fact, there is a need for additional protection of proprietary information, we will certainly work with Congress to make that happen.

Having said that, I should point out that a Federal regulation can't trump FOIA, and so that's a statute. So if there is, in fact, a need for a change in law, then we would have to work with you to make that happen. But otherwise, it is our belief at this time that the current regulations, in fact, do provide adequate protection.

Mr. BELL. What are some of the additional protections that have been discussed as possibilities?

Mr. ALBRIGHT. Well, the exemptions that exist today within FOIA, there's two of them. I think it's Exemption 4, which is disclosure of proprietary information, and then there's Exemption 1, which has to do with national security information. And as I pointed out, there's the Federal Trade Secrets Act. As I said, at this time we don't believe we need additional statutory relief in order to further protect the data. However, if, in fact, additional legal analysis indicates that there may, in fact, be an issue there, then we would have to come back to you with some specific proposals, I would suspect. We don't have those right now, though.

Mr. BELL. And would that be after the comment period if that kind of recommendation——

Mr. ALBRIGHT. Actually, we are looking at this issue now as we speak.

Mr. BELL. How did the Department determine that liability should only be against the seller?

Mr. ALBRIGHT. That was in the statute.

Mr. BELL. And how does the Department decide that the designation should only be valid for a term of 5 to 8 years?

Mr. ALBRIGHT. OK. Good question. There is no magic to the 5- to 8-year period. That was a judgment that we came to based on

our understanding of the technology, the technological cycle and the potential changes in the threat environment.

It's important to understand, though, that the period of designation just tells you that period over which you can sell technologies that, in fact, have these kinds of protections. A technology that is sold during the period over which the designation is applicable, those protections exist in perpetuity. I mean, we are rendering certain the protections granted to the seller for a particular technology. However, every 5 to 8 years, depending on the technology, they've got to come back and ask us if they can continue to sell that technology and continue to get that kind of protection.

Mr. BELL. Thank you very much.

Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much.

The gentleman from Tennessee.

Mr. DUNCAN. Thank you, Mr. Chairman.

Mr. Secretary, I'm curious about how much interest there is in this so far. Do you have any idea, a rough guess, as to how many applications or any indications as to how many applications you might be receiving on this?

Mr. ALBRIGHT. Sir, that's an excellent question. So far we've received a very small number of applications. We hear anecdotally there is pent-up demand, but I couldn't tell you if we're going to get 50, 500 or 5,000.

Mr. DUNCAN. How many people from the private sector have been showing up at these seminars or meetings that you've been holding?

Mr. ALBRIGHT. The one we had in Washington, DC, for example, had over 200 people present.

Mr. DUNCAN. What about outside of Washington?

Mr. ALBRIGHT. Outside of Washington it ranged from 50 to 75 typically.

Mr. DUNCAN. And how many comments have you received thus far roughly?

Mr. ALBRIGHT. During the rulemaking process we received comments from 45 organizations. The total number of comments I don't have off the top of my head. It was——

Mr. DUNCAN. And have almost all of these comments been favorable or supportive, or have some of the comments pointed out problems or questions about the law thus far?

Mr. ALBRIGHT. You're referring to the comments we got when we were out on the road in places around the country? I would say that the vast majority of comments we got were extraordinarily favorable. In fact, a uniform comment we got was they couldn't believe the Federal Government was doing this, going out and reaching out to the community in the way we were. But still this is a very complex rule, and it is something that needed to be explained. No, I don't recall any direct negative comments on the rule.

Mr. DUNCAN. All right. Thank you very much.

Chairman TOM DAVIS. Thank you very much.

Mr. Schrock, questions?

Mr. SCHROCK. Thank you, Mr. Chairman.

Mr. Secretary, in putting forth the rules to implement this act, has DHS found specific statutory limitations that in your esti-

mation hinder the full realization of the act, and if so, what recommendations do you have to the committee for potential changes to this act?

Mr. ALBRIGHT. That's an——

Mr. SCHROCK. Is it going to be substantive enough for people to say, "OK, we trust the government?" Because as you said, whenever the government shows up with a briefcase and says, "I'm here to help," people are automatically suspicious.

Mr. ALBRIGHT. Well, we've done everything we can to try to change that attitude with the private sector. I would say that I think it's premature to discuss any potential changes to the act. I think, as with anything that's as groundbreaking as this legislation is, I would not be at all surprised that as we get into the implementation process and start to execute the act, we're going to find a lot of issues that we may at some point come back to you and ask for some statutory relief. But right now I think it would be premature for me to say that there's anything that leaps out at us as being problematic.

Mr. SCHROCK. I can certainly understand why the private sector would be hesitant to produce anything that might be put in place that they could get sued over. You know, suing is a national pastime in this country. Until last night we thought baseball was. I think that worries me, because we've got some wonderful technology out there, and I'm afraid we're going to stymie those folks who would come up with the technology, because they're scared to death they will get sued. I really worry about that.

Mr. ALBRIGHT. We couldn't agree with you more. We've heard anecdotally that contractors are having riders attached to their insurance forms that don't apply to—I mean, you're absolutely right. So we are obviously on board with this landmark legislation, and our job is to implement it as efficiently as we possibly can.

Mr. SCHROCK. Thank you.

Chairman TOM DAVIS. Thank you very much.

Mr. Carter, any questions?

Mr. CARTER. Thank you, Mr. Chairman.

Mr. Secretary, will the DHS utilize an expedited renewal process for applications?

Mr. ALBRIGHT. A renewal process for applications? Yeah. I think the answer is yes.

Mr. CARTER. Expedited?

Mr. ALBRIGHT. Sure. If the technology hasn't substantially changed, if the insurance regime that they are operating in hasn't substantially changed, and the threat environment hasn't substantially changed, then I would imagine it would be fairly straightforward.

Mr. CARTER. And how do you intend to deal with new developments to a particular antiterrorism technology that occur after it has received the designation to ensure that these developments are covered and can be deployed expeditiously?

Mr. ALBRIGHT. Well, there's two answers to that. Let me first start by saying that the SAFETY Act doesn't alter the competitive environment that the private industry operates in. So, for example, if you have a particular technology, and you have received SAFETY Act designation, and I have a technology that performs more or less

the same function but can do it better, then I ought to be encouraged by the fact that you have, in fact, already received SAFETY Act designation and will go out and develop that product and apply for SAFETY Act designation and will compete with you in the marketplace.

Mr. CARTER. That is not what I really intended. What I intended was, let's say I have a product that's been approved, and because my company does—continues, we come up with a better mouse trap, we've got a better idea, a way to improve what we've already had approved by you. Can you—is that going to be the—redo the whole process, or will there be a method where you can shorten the process to add the technology?

Mr. ALBRIGHT. No. In fact, we have in the rule in our implementation process—what we have done is we have set the system whereby any substantial change, a significant change or modification to the device—actually, we are requiring, much like the FDA does, that people who make substantial changes to a device or a technology come to us and tell us about it, and then we will issue a certificate that says that, in fact, this is OK, that you can do this. And so we see that there's a significant benefit to that, which is what you just articulated, and that is that it prevents the developer or the seller from having to go through the process all over again. They can just simply come in and say, "Hey, look, I've decided to quit making this out of plastic, I'm going to make it out of steel now," and we'll do a quick review of it to make sure there aren't any other changes and just simply issue them a certificate that allows them to keep their designation.

Mr. CARTER. Thank you. That answered my question.

Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much.

Mrs. Maloney, any questions?

Mrs. MALONEY. Thank you for having the hearing, and if I could place my opening comments in the record.

Chairman TOM DAVIS. Absolutely. Without objection.

[The prepared statement of Hon. Carolyn B. Maloney follows:]

COMMITTEE ON GOVERNMENT REFORM
OVERSIGHT HEARING

"Implementing the SAFETY Act: Advancing New Technologies for Homeland Security"

OCTOBER 17, 2003
ROOM 2154 RAYBURN HOUSE OFFICE BUILDING
10:00 a.m.

Statement of Congresswoman Carolyn Maloney

As Chair of the Democratic Caucus's Task Force on Homeland Security and as a Member who represents parts of New York City, homeland security is an issues that I care deeply about.

In fact, the safety and security of our homeland is something we can all agree on – it is truly a bipartisan issue. Because we are all advocates of tough homeland security, we should all celebrate our successes and work together to fix vulnerabilities.

I agree that the private sector is an important partner in developing technologies to enhance our security here and abroad.

We must make a number of efforts to ensure that we have created an environment where businesses are allowed to do their part to develop and produce potentially life-saving devises that we all can use during a terrorist attack or another homeland security event.

However we must also make sure that the American people are protected. We need to ensure that when they use a device that is supposed to protect them, it protects them. We need a system that provides a balance.

Some have argued that this balance has been created by a long standing law – Public Law 85-804 – which to my knowledge already protects sellers of anti-terrorism technology when they sell to the federal government.

As we all know, immediately following the passage of the bill that created the Department of Homeland Security, there was an uproar over an indemnity clause that was added for pharmaceutical companies.

My concern now is that we are acting in good faith to ensure that the SAFETY Act is used to promote businesses to use American ingenuity and all of our wonderful skills to develop the best technology and equipment to combat the war on terrorism and to promote a safe homeland rather than providing a level of protection that could only have harms on the individuals who use the products.

I look forward to hearing from our panel.

I am interested to learn more about the proposed rule on the SAFETY Act.

Mrs. MALONEY. I think this is a very serious issue and one that needs balance. Just from New York City, we're still reeling from some of the aftermath of really being supportive to the contractors who rushed to the scene to save the lives of others, and now they're facing certain liability issues, when all they were trying to do was save the lives of others selflessly. So it's a very important area and one that needs review, and I am glad that we're having it.

I'm interested in the new technologies you're seeing. In New York the telephones didn't work, the radios didn't work, and to this day they still don't work. Are you seeing new technologies on radios that could be implemented around the country for homeland security?

Being a New Yorker, I'm concerned about the power grid. We just had a power grid shortage, and fortunately it was in the middle of the summer so we didn't lose any lives. If it had happened in the middle of the winter, people would have frozen to death. And I'm wondering, are you seeing new technologies for a power grid, and how we can protect this?

Actually, Mr. Chairman, I think it might be interesting new technologies that we're seeing for homeland security, that you may be reviewing or seeing in the application process; it might be something that we might want to look at that we could take to our districts. And I would just like some comments on what new technologies are you seeing that you think would really be helpful to the country?

Chairman TOM DAVIS. Mrs. Maloney, I think one of the problems is a lot of these technologies are hesitant to come forward until we get these regulations nailed down in a way the companies are willing to come forward and not incur a lot of liability. I mean, that is the issue. There are a lot of them out there. I'm sure you've seen a part of it, but there are——

Mr. ALBRIGHT. We've seen an enormous flood of people with excellent ideas, and they come from not just the people you'd expect them to come from, the big companies, the Lockheed Martins, those sorts of people. We see them from people—inventors in garage shops, and there's been a flood of technology that has been coming at us over the past year and a half. I was at the Office of Homeland Security prior to my current position, and I saw a lot then, and I'm seeing a lot now.

With regard to communications, I'd be happy to arrange to have a briefing with this committee on Project SAFECOM, which is managed by the Science and Technology Directorate in the Department. It is focused entirely on developing and implementing new technologies and standards for those technologies, not just for interoperable communications, which, of course, was one of the big issues that you had in New York right after September 11. We're all familiar, for example, with the story that the police department couldn't warn the fire department to get out of the second building.

But also robust communications, your point is very well taken that when we talk to the user community, which we do spend a lot of time doing, their No. 1 priority is—obviously they're interested in interoperable communications, but they also want the communications that they have just within their own particular organization to work and continue to work in a robust fashion.

So, yes, the answer is there's lots of ideas out there. We have programs in place to develop them, and I would be happy at some point to brief you on them.

Mrs. MALONEY. I'd like to say that during September 11, not only could they not talk—the police talk to the fire, but the fire couldn't even talk to each other.

Mr. ALBRIGHT. Exactly.

Mrs. MALONEY. So they couldn't even warn people that they were getting calls in from people in the buildings that had phones or cells or Blackberries or whatever, and they couldn't communicate to the people on the site where to go.

And I want to share with my colleagues, when I went to the police station, they said the No. 1 thing they needed was radios. And so I thought, "Who's got radios?" The Defense Department. So I called Bill Young, and Bill Young organized a shipment of radios from the Defense Department to come into the fire and police so that they could communicate at Ground Zero. So that's one thing that this Congress organized the day after September 11.

But I'm told they still can't communicate, and I would like to ask if the chairman could arrange that for Members that might be interested in it. I feel that if you can't communicate with each other, how can you solve a problem, a crisis? And regrettably, that is the world we live in now, and I look forward to working with you and with the other members of the committee on coming forward with a balanced solution that protects the individuals and protects the companies. So I thank you for your work.

Chairman TOM DAVIS. Thank you very much.

Let me just ask one last question. Once a company's product or service receives SAFETY Act designation certification, it's conceivable that this company could then have a very competitive advantage in the marketplace. As you adopt the rules, how do you view that? Is that a concern? Is it just the way it happens? Are there any specific provisions you've included in the interim rule to guard against a potential competitive advantage?

Mr. ALBRIGHT. No. Well, we certainly have thought about that, but, again, the SAFETY Act is not designed—we're not going to try to necessarily level the playing field among various technologies. In other words, if you have a contractor that sells a particular technology for a particular threat environment fix, and they happen to hustle up there and apply for SAFETY Act designation and get SAFETY Act designation, and then another competitor who chose—who sells perhaps substantially the same technology in the same threat environment, they may be—but doesn't hustle to get that application, then they may be a bit behind the power curve.

However, having said that, we also in the regulation talked about the fact that we'll give great weight to what are called "substantially equivalent technologies." So if you have a technology that is basically the same as one that has already been approved, you will almost certainly get an expedited review.

Chairman TOM DAVIS. Mr. Schrock.

Mr. SCHROCK. Mr. Chairman, let me just ask one more thing. Can technology that already exists be designated as a qualified antiterrorism technology under the interim final rule? And can you explain the difference between technology that has been previously

sold versus technology that has been previously deployed? I think the commercial folks are asking that and want to know the answer to that.

Mr. ALBRIGHT. The term "deployment" in the SAFETY Act is a purely technical matter, and what it means, in effect, is that something that has been fielded proximate to an act of terrorism, either—so technologies that have been—technologies that receive anti—the SAFETY Act designation will only get that designation if they have been deployed prior to the term over which the designation applies, and there's an important reason for that. We do not want to go backward in time and unravel causes of action that may have already accrued, you know, due to a prior event, for example.

But having said that, we also understand that there are technologies that have been sold and fielded that pass all the technical criteria and meet all the various criteria associated with the SAFETY Act. And so the Under Secretary can, in fact, designate technologies that have been sold past a point, past a date of sale that is prior to when the designation is actually granted. And what that does is that relieves you of—let me give you an example of the situation where you could get an absurd result if you didn't do that. You may have technologies, for example, that are not widely deployed, they're extremely expensive, and the reason they're so expensive is because the cost of risk mitigation for them is very, very high. So you may have a jurisdiction, like, for example, Fairfax County, that can afford those technologies, and you may have other jurisdictions that cannot. And the Department of Homeland Security may decide that it's in the best interest of the Nation to assure a more wide deployment of that technology. OK. So that would then make that technology eligible for SAFETY Act protection. That would be if it passes all the other criteria. And we would so designate it. Having done that, the technologies that were sold in my example in Fairfax would fall into that category and would also receive the designation.

Mr. SCHROCK. So people who have technology already before the next attack comes, are you saying they need to get to DHS to get the DHS stamp of approval?

Mr. ALBRIGHT. You've got to be a little bit careful, because, for example, the purpose of the SAFETY Act, as the chairman, for example, pointed out, is to assure that the technologies that would not otherwise be deployed to the extent that they need to be deployed are deployed.

If we have technologies that are out there, and they are deployed to the extent they want to be deployed, and the insurance regime is acceptable to them, then it's hard to imagine that it was the intent of Congress to somehow indemnify them when, in fact, the purposes of the act have already been achieved, they have, in fact, been deployed.

Now, of course, insurance environments change. There's a lot of stuff that was out there before September 11 that now can't get insurance. They've had riders attached to their policies, for example, and so, yeah, under those circumstances we would have to go back in and look carefully at the technology, review it and see if it should, in fact, receive the designation.

Mr. SCHROCK. The premiums on these things, the insurance has to be out of sight.

Mr. ALBRIGHT. That's right. And so, again, prior deployment doesn't necessarily preclude designation. However, it doesn't form the decision.

Mr. SCHROCK. Thanks. Thank you.

Chairman TOM DAVIS. Mr. Carter, any additional questions?

Mr. CARTER. Thank you, Mr. Chairman.

You've indicated that the application process will be interactive between DHS and the applicant. What assurances can you give us that the applicants will not be faced with information requests that are burdensome and will delay the certification of the product?

Mr. ALBRIGHT. We have an application. It's available on the Web today. We don't think it's burdensome. It's been through the regulatory process at OMB. They don't think it's particularly burdensome.

I guess what I would say is that we have a set of criteria the statute requires us to evaluate, and that's our job to do what Congress told us to do in this case. We have asked for what was, in our view, the minimal amount of information needed in order to do what Congress told us to do. As I said in my opening statement, we are asking for whatever available data there may be to show that the technology is technically effective. We're asking contractors to tell us what the liability regime—what their risks are, what they feel their risks are, what the scenarios are that they think that this technology is going to be applicable for. And we're asking them to tell us something about what it takes to produce—what is the actual basis for the cost of the technology. After all, we are supposed to set the price of the liability risk—the risk insurance to be at a level that doesn't unnecessarily distort the price of the technology. To do that, we have to know the price of the technology, and so—and know the basis for that price.

As I said, we have a heavy burden here to bear. I mean, after all, at the end of the day we are granting designation and, in effect, limiting the liability for people who might want to recover damages at some point. That's a burden that we're bearing, and we have to, I think, be very diligent in our review of the data to—and our request for data to assure that we have the information we need to have to evaluate the criteria.

Mr. CARTER. Well, I understand that, and that's talking about your application. It's been estimated by someone that it would take about 108 hours to fill out that application, but in an interactive situation where the developer or applicant is dealing interactively with a member of your organization, which means that other requests could be made of him, we need additional information, I'm just asking that could easily become burdensome, especially if someone had just got up on the wrong side of the bed some morning. They can make that very burdensome.

Is there going to be some kind of criteria that keep that from being burdensome? And I can tell you from personal experience that I've dealt with Federal bureaucrats that if they got up on the wrong side of the bed could make life burdensome.

Mr. ALBRIGHT. Let me try and answer the question—maybe I can answer the question this way. Did you say someone told you it was 100 hours or days to fill out the application?

Mr. CARTER. They said hours. If it's days, that's pretty rough. Hours is rough.

Mr. ALBRIGHT. 100 hours is rough, but it's not overly rough, I would say. The way I would put it is that the Department of Homeland Security wants this legislation to succeed. We want this to work. As I've said, we've been very open. We've published this regulation with a comment period. We have, in fact, delayed release of the act from the date we originally said we would in order to assess those comments. We have an interim final rule where we are meeting for open comment. We've gone out on the road all over the country. I personally have done that with all of my staff to get input from the private sector, and we will continue to do that, because we really want this to work. And so if, in fact, it turns out to be the case that the balance between the burden on the seller and our ability to perform due diligence in the review of the application has gotten out of whack, then we will be the first people to try to go and fix that.

Mr. CARTER. And on the previous question, just out of curiosity for me, I'm making some assumptions, but I want to see if I've got them right. On a situation where there's existing technology that is deployed, the previous question that was asked, and they apply for the SAFETY Act, and the SAFETY Act assurances are granted, do you see that as grandfathering in all the previous implementation or not grandfathering it in?

Mr. ALBRIGHT. No, not grandfathering in all the previous implementation. For example, a lot of technologies have been deployed for purposes that have nothing to do with counterterrorism. Military technology is a perfect example of that. And the requirements threat, the set environment is very, very different. So, no, we're not going to grandfather things in.

However, having said that, you know, if the insurance regime has—if you have a bunch of technology that is already out there and has been deployed, it's even been deployed for counterterrorism purposes, and the insurance regime that they are operating in has changed dramatically, so now they're literally taking the technology off the street, for example, in order to protect themselves, then you can bet we're going to look at that and expeditiously review those applications and make sure that doesn't happen.

Mr. CARTER. Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much. I don't see any other questions at this point. Thank you very much for being with us. We'll continue the dialog. We will take just a 2-minute break while we get our next panel up here.

[Recess.]

Chairman TOM DAVIS. We are ready to start our second panel. We've got Harris Miller, the president of the Information Technology Association of America; Stan Soloway, the president of the Professional Services Council; and John Clerici, representing the U.S. Chamber.

It's the policy of the committee that we swear you in before you testify, so if you would rise with me and raise your hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you very much.

Harris, we will start with you; then Mr. Soloway; and then, John, you will be able to clean that up. Thank you all for being with us.

STATEMENTS OF HARRIS N. MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA; STAN Z. SOLOWAY, PRESIDENT, PROFESSIONAL SERVICES COUNCIL; AND JOHN M. CLERICI, ESQ., ON BEHALF OF THE U.S. CHAMBER OF COMMERCE

Mr. MILLER. Mr. Chairman, members of the committee, many thanks for having me here today to allow ITAA to testify on the implementation of the SAFETY Act. This important legislation, as you noted, Mr. Chairman, is intended to facilitate the rapid development and deployment of technologies and services that offer remarkable potential to improve homeland security.

I'm the ITAA president. ITAA is the Nation's leading and oldest trade association focusing on the diverse IT industry. It provides global public policy and national leadership to promote its continued rapid growth. We represent virtually every major Federal contractor and count among our membership a wide range of companies from the largest enterprise solutions providers to the smallest IT startups. We also serve as the co-sector coordinator for the ICT sector as designated by DHS. I submitted my program statement for the record, Mr. Chairman, and I assume it will be included in the hearing record. I would like to extend my appreciation, Mr. Chairman, for your holding this important hearing today, one that was postponed while DC grappled with something even the SAFETY Act could not prevent during Hurricane Isabel.

Let's be clear what this legislation is about. The citizens of this country look to government to protect our homeland. Government, in turn, wants to partner with industry to find the best technologies to fight terrorism. Effective implementation of the act is absolutely essential; on the other hand, poor implementation would inhibit access to great technologies.

In Spring 2002, soon after September 11, I began to hear extremely serious concerns from member companies, large and small, about some Federal agencies wanting successful bidders on key contracts to indemnify the government against the risk of loss if an unforeseen problem arose on an antiterrorism technology solution under consideration by DHS. Insurers did not know what to make of such requests and were not prepared to insure against such requests. These requests for indemnification made CEOs and our member companies stop in their tracks and ask themselves whether they were willing to literally bet the company on a decision to obtain a Federal contract. There had to be a better solution than having the private sector self-insure and indemnify the government against loss. Your leadership and that of Congressman Turner were instrumental in focusing attention on this important issue, and eventually led to implementation and passage of the SAFETY Act, which, as you've correctly pointed out, is meant to limit, but not eliminate, the insurance risk and litigation costs to companies that do have qualifying technologies.

ITAA has been very involved in the regulatory process to implement the SAFETY Act. We were one of the organizations that Dr. Albright referred to that provided extensive comments on the proposed rule, and we have been participating in the various parts of the road show that he described. We filed comments back in August. Frankly, we were pretty pleased with where DHS was heading, and we are still pleased with the overall positive approach. However, I would slightly disagree with something Dr. Albright said during his comments.

I think industry is pleased that DHS is doing it. I think the concerns we have are how DHS is doing it, and that's what we're going to focus on today. For example, we are concerned with how DHS is going to go about prioritizing the application process. Congressman Duncan asked about how many applications they are likely to receive. I agree with Dr. Albright, no one really knows. But we have seen a tremendous amount of interest among membership. Programs that ITAA has done, including the program with you, Mr. Chairman, and Congresswoman Maloney in New York City recently, a program I did as recently as yesterday, in which I, explaining opportunities at DHS, time and time again questions came up about liability concerns. So, certainly, there are a lot of companies out there, technology companies, that are concerned about how this act is going to be implemented. So, I suspect it's going to be very important that the DHS come up with a clear policy to prioritize the application process.

A second concern we have is that at times in the interim final rule, it suggests that the only group to benefit from this rule are going to be government contractors, rather than the American people. That is not true. Yes, it is true that getting the designation is a privilege, but the whole point of the act, as you pointed out, Mr. Chairman, and as DHS itself says, is to encourage a partnership; but you're not going to have a partnership if the partners do not start from the same premises.

Let me give you an example. The Department's proposed rule says that the insurance of critical technologies to aid the war on terrorism could end up actually coming full circle. We started down this legislative road because the government was asking private companies to indemnify and, if necessary, to self-insure to sell to the government. The SAFETY Act, as you pointed out, is meant to solve this problem, but what happens if insurance cannot be obtained for technology at any cost that does not distort the price of the technology in ways the act protects against? What happens if that uninsurable technology is still needed by the government? As outlined in the interim final rule, DHS still wants the company to self-insure, so it seems we are back to the same place.

A third concern has to do with the volume and kind of information that would be required. Congressmen in the last panel were asking about the number of hours that go into an application. DHS is estimating 180 hours, Congressman. Our companies looking at these applications think they may be closer to 1,000 hours. Now, that's an extremely heavy burden for a large company. It's a virtually impossible burden for a small to medium-sized company. We think we need to cut down this application process and make it much more manageable if we are really going to get the kind of ap-

plications we need to help protect the American people against terrorist attacks.

The last issue I want to mention, Mr. Chairman, is the issue of confidentiality. We respectfully disagreed with the assessment of DHS that the current FOIA legislation gives adequate protection to the extremely sensitive data companies are going to have to share, and we have devised specific suggestions to DHS as to how to provide adequate protection, including using the FOIA exemption that you helped to pass through the Congress last year, or 2 years ago rather, as part of the DHS legislation, so we think that this issue of providing information and giving adequate protection needs to be tightened.

Final point, Mr. Chairman: We don't think that DHS would further delay the implementation process, but the application kit which just became available yesterday is daunting. So basically what we are saying, Mr. Chairman, is, we hope DHS, on the one hand, will move ahead right away and begin accepting applications, but should it turn out that this application is too difficult to use, as we believe it is, we hope that DHS would quickly modify it down the road and not be locked into the application kit which was published yesterday.

Thank you very much, Mr. Chairman. I look forward to questions from you and your colleagues.

Chairman TOM DAVIS. Thank you very much.

[The prepared statement of Mr. Miller follows:]

STATEMENT

OF

HARRIS N. MILLER

President

Information Technology Association of America

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

CONCERNING THE IMPLEMENTATION OF THE "SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES ACT OF 2002"

ON BEHALF OF

INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

October 17, 2003

Introduction

Mr. Chairman and Members of the Committee. Thank you for inviting the Information Technology Association of America (ITAA) to testify today on the Department of Homeland Security's proposed and interim final regulations to implement the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), which was passed as part of last year's landmark legislation creating the new Department of Homeland Security ("DHS," or "the Department"). The SAFETY Act, as this portion of the legislation is known, is intended to facilitate the rapid development and deployment of technologies and services that offer remarkable potential to improve the security of the American people.

My name is Harris Miller, and I serve as President at ITAA. ITAA is the nation's leading and oldest trade association focused on the diverse information technology (IT) industry, and provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of more than 400 corporate members throughout the United States, and serves as the Secretariat for the World Information Technology and Services Alliance (WITSA), a global network of 50 countries' national IT trade associations. ITAA represents virtually every major federal contractor and many other public and private sector contractors, and counts among its membership a wide range of companies from the largest enterprise solutions providers to the smallest IT start-ups. The Association takes the leading role in major public policy issues of concern to the IT industry, including government IT procurement, homeland security, information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy protection, and e-commerce, among others. Of particular note to this hearing, ITAA also serves as the co-sector Coordinator for the ICT sector, as designated by DHS.

As the nation mobilizes to respond to new asymmetrical threats, the federal government has recognized the need to access America's technological resources to safeguard the homeland against future acts of terrorism. No one wants to wake up the day following another terrorist attack like the one our nation suffered on September 11, 2001 with the knowledge that we could have done more to prevent it. At the same time, the use of technology to secure the homeland carries with it significant risk of potentially unbounded and uninsurable

liability in the event of a terrorist attack where anti-terrorism technology was deployed to prevent such an event. The SAFETY Act seeks to strike a balance between the potential and the risk of deploying technology to defend against terrorism by establishing a regime to mitigate the technology providers' exposure to liability for potentially catastrophic losses resulting from acts of terrorism that could circumvent even the most innovative technology designed to prevent them. It is important to note that the SAFETY Act doesn't just protect sellers; entities that are mandated to implement anti-terrorism solutions also require protection, and the SAFETYT Act affords protection to those entities as well.

Passage of the SAFETY Act was a critical first step towards ensuring that U.S. citizens would have access to the benefits of the full range of technology solutions to aid in the war on terrorism. With passage of the statute, the focus necessarily shifted to implementation and ITAA began working with the Department and the Office of Management and Budget (OMB) to accomplish this objective as quickly as possible. I would like the record to show that ITAA strongly supports the Department's general approach to implementing the SAFETY Act that has been reflected in both the proposed regulations published on July 11, 2003 and in the interim final regulations that were published yesterday in the *Federal Register*. In particular, we are pleased that the Department's regulations carry out the statutory distinction between designation of products and services as qualified anti-terrorism technologies (QATT), and those QATT that are further certified as approved products for purposes of the government contractor defense. ITAA was also pleased to see that the Department interprets the statute to provide for a single federal cause of action that may only be brought against the "Seller" of the QATT. We also appreciate the Department's candid and open request for constructive suggestions about a range of significant policy issues.

Having said all that, ITAA does still have a number of both policy and process concerns that we raised first in response to the proposed regulations and that have carried over in reaction to the interim final regulations and the Department's implementation of the SAFETY Act more broadly. The remainder of our testimony today will focus on these concerns.

When the Department published it's NPRM in the *Federal Register* on July 11, it provided for a 30-day comment period for interested parties to respond. ITAA joined with several other leading trade associations in submitting extensive and detailed comments on the proposed regulations. At least forty-nine other entities submitted comments to the Department, many of which were equally detailed and also raised significant concerns with substantive issues that must be resolved prior to final implementation of the statute.

I provide for the record a copy of the comments ITAA submitted along with the Professional Services Council, the Aerospace Industries Association, and the National Association of Manufacturers. Because of the length and breadth of our

joint comments, our testimony today will focus more broadly on issues of concern to the IT community. I would refer you to our formal comments to the proposed regulations for our detailed analysis of the draft regulations. Our industry colleagues from the Professional Services Council (PSC) and U.S. Chamber of Commerce will address other areas of concern to the private sector.

In the initial "Regulatory Background and Analysis" section of the NPRM that prefaced the actual text of the proposed regulations (the "Preamble"), DHS indicated that the Department would begin accepting applications for QATT designation and approved product certification on September 1, and that the forms of application necessary to initiate these processes would be posted on the official DHS website. Many in industry were dubious of this timetable since the September 1 deadline – which was itself a federal holiday – allowed only **two weeks** from the expiration of the comment period for DHS to review and address comments on a major regulatory initiative. Moreover, in the absence of the application forms or any other information in the proposed regulations about the content of applications or the specific information required to be submitted, industry was left to respond in many ways in the abstract to the proposed rules. ITAA's comments in particular, though detailed as to the provisions outlined in the Preamble and proposed regulations, were hypothetical in nature since the application forms were not published.

On September 8, 2003, DHS published an emergency request for clearance of an information collection request to OMB in the *Federal Register*. This clearance request focused on what DHS is terming the "Application Kit" that interested vendors will use to apply for designation and/or certification under the terms of the SAFETY Act. ITAA obtained a copy of the supporting materials sent over to OMB—namely the application kit—and has been astounded at the kinds and scope of information to be required of applicants. We will discuss in more detail the concerns we have with the data being requested by DHS, but want to begin with an overview of the concerns industry has about the forms.

We cannot overemphasize the importance of the scope and content of the application forms. Until industry sees the actual final application forms the Department plans to use, we cannot be certain of the appropriateness of the information to be collected or the real burdens applying for designation and/or certification will that will be placed on companies seeking either approval from the Department. Industry needs to have input into the scope and form of the final applications, and we urge DHS to reach out to the industry community to seek input and comments on the draft applications as soon as possible. Now that the interim final rules have been published and the regulatory framework is effective, ITAA members want to know how and in what form they should submit applications to the Department for certification and/or designation. In the absence of an approved application kit, we believe there will be countless efforts undertaken by interested parties that may be rejected by the Department as a result of some gap in information contemplated in the proposed applications.

DHS's self-imposed deadline of September 1 has come and gone, and the Department has not yet released a draft of the application. Because of the nature and scope of information contemplated in the draft application submitted to OMB, ITAA believes it is critical for the Department to afford industry the opportunity to provide comments before using the proposed forms to process applications.

Yet even in the absence of the actual form, DHS has indicated to the vendor community in a variety of fora that it will accept submissions for certification and/or designation prior to the finalization of application kit. The Department recently posted a new SAFETY Act web page within its web site. The site notes in part that "Individuals may submit technologies for consideration to: Department of Homeland Security, Attn: SAFETY Act, 245 Murray Lane, Building 410, Washington, DC 20528." The site goes on further to indicate "at a future date, the Department will issue a formal application and submission criteria. Therefore, the Department reserves the right to request further information from submitters who request SAFETY Act consideration prior to the release of the formal application process."

This statement would seem to imply that companies seeking Departmental review of technologies may submit information to the Department prior to the release of the formal applications for designation and certification. ITAA is concerned that the language included on this website will lead to a flurry of submissions to the Department, and that in the absence of a formal process, DHS will be inundated with submissions that require formal evaluation criteria. Given that the regulatory framework is now effective as of yesterday, the lack of an approved application form is of even greater concern. We urge the Department to clarify the information on its website to assure that the designation and certification process works expeditiously for the benefit of both the government and its suppliers.

DHS just this week finished a series of informational "road shows" designed to educate the business community about the SAFETY Act and the specific application procedures for designation and certification under the Act. ITAA attended the first of these sessions on in late September in Dallas and had either staff or member representatives at each of the other forums held around the country, including the most recent event held in Washington on Tuesday of this week. Based upon the presentations given at the road shows and the supporting information in the application kit submitted to OMB, there are several concerns that we have about the Department's interpretation of the SAFETY Act statute and the amount and scope of information to be required for applications to the Department.

At the forums, DHS outlined significant data requirements for parties interested in receiving designation and/or certification of anti-terrorism technologies that quite

frankly were not even conceived of in the proposed regulations or enumerated in the interim final rule. ITAA is concerned that the massive scope of scientific, business, and insurance/risk data to be required on applications to the Department is so burdensome that even the largest information technology companies will need to assemble massive internal teams to comply with the requirements. While the scope and amount of data to be submitted to DHS may be assembled in large enterprises, we have significant concerns about the ability of smaller companies to comply with the information requirements outlined by the Department. Among other pieces of information, DHS envisions requiring applicants to submit information on the profitability of the technology, significant self-insurance data and virtually any conceivable technical data relating to a particular technology. ITAA will provide comments to the Department and to OMB on the burden estimates outlined in the interim final rules. Let me just state for this committee that based on feedback provided by ITAA members, we believe the Department has grossly underestimated the burdens applications will place on applicants.

We are concerned that the technical and business evaluation information requirements are so massive as to ignore the real-world business issues surrounding deployment of anti-terrorism technologies and urge the Department to rethink the scope of information to be required on applications. Based on the information presented at the forums, we are concerned that the regulations and information to be required on applications are so complex and so burdensome that they may themselves serve as a severe impediment to the deployment of anti-terrorism technologies and services. We are also concerned that the Department has not clearly identified how it specifically will protect this sensitive proprietary data from unauthorized disclosure or dissemination. At the SAFETY Act road shows, the Department indicated it's strong preference for electronic submission of applications and supporting data. While ITAA will certainly be the first to support and embrace the power of the internet to enhance and transform business processes, the Internet is still an open system and is vulnerable to breaches. We are concerned that there is no mention of a comprehensive management plan to secure the systems over which data will be transmitted, policies and procedures applicable to DHS personnel operating and having access to the system, or details on the technological approaches the Department will take to secure the data provided by applicants. We urge the Department to work with industry to develop and implement a comprehensive plan to secure the data and network over which this highly sensitive, proprietary information will flow.

Additionally, DHS outlined at the forums and has noted in its interim final rules the availability of an optional "pre-application" process whereby firms can submit condensed information to the Department to receive feedback on the likelihood of a full-blown application receiving certification and/or designation. ITAA understands and appreciates the spirit of this pre-application process, but is concerned that a pre-application program would further elongate an already

extensive review process. We are also concerned about the Department pre-judging technologies and services without full disclosure of information required in a full application.

DHS also maintains that SAFETY Act coverage is envisioned only for the narrowest of technologies specifically designed for anti-terrorism applications. The Department has also been quoted in recent news stories as interpreting the SAFETY Act to apply only to "new" technologies developed specifically for homeland security applications. While we understand that the Department has backed away from this interpretation of the statute, we are nevertheless extremely concerned that the Department interprets the SAFETY Act to apply to such a limited scope of technologies and services. The SAFETY Act statute makes no reference to technologies exclusively "designed" for anti-terrorism applications, but rather, references that coverage be extended to technologies and services "designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary." ITAA believes that a wide array of technologies not originally developed with specific anti-terrorism applications in mind will nevertheless have wide applicability in the homeland security arena, and we urge the department to clarify in its final regulations and application/briefing materials that the SAFETY Act applies to all manner of technologies that may be procured for homeland security purposes as the statute specifies. We address this issue in additional detail below.

Overview of ITAA Comments on the SAFETY Act Regulations

ITAA's comments to DHS on the proposed regulations address a wider range of issues than we can detail in this statement, and I would commend them to the Committee for a detailed position of ITAA on the changes needed to the proposed regulations. As noted earlier, they are attached.

Today I would like to focus our testimony on several broad issue areas that were addressed in our comments and remain of concern now that the interim final rule has been published. These concerns center around:

- The need for an expedited process for priority procurements;
- The time-frame for designation and certification of QATTs under the proposed regulatory framework;
- The need for sufficient flexibility in the scope of QATT designations and approved product certifications to ensure complex IT product and/or service offerings are properly addressed;
- Insurance provisions of the proposed rule;
- Issues associated with the single federal cause of action;

- Concerns with provisions dealing with post-designation and certification changes to approved products and services;
- Procedures to ensure the confidentiality of information submitted as part of applications for designation and/or certification;
- Appeal procedures for denials of applications for designation and certification; and
- The relationship between the SAFETY Act and indemnification under Public Law 85-804.

The Need for an Expedited Process for Priority Procurements

Whether and how quickly a technology is designated and/or certified under the SAFETY Act will have a profound impact on the acquisition of technology and services to fight the war on terrorism. While we are pleased that the Department indicates in the interim final rule that it will work to prioritize reviews, there is no clear standard outlined as to how the Department plans to accomplish this prioritization. There is also no clear framework for how DHS plans to prioritize reviews for technologies of interest to agencies other than DHS that have a need to acquire QATTs.

ITAA believes that the final regulations should be amended to expressly accommodate the needs of other agencies that will acquire technologies and services designed to fight the war on terror. Specifically, we believe that the regulations should provide that federal, state, and local agencies may notify offerors that a particular solicitation contemplates the acquisition of technology that will be recommended to DHS for designation as a QATT.

As noted above, while the Department has acknowledged that it intends to prioritize reviews based on the most immediate needs, we believe the final regulations should provide for an explicit mechanism to prioritize and expedite certain applications. ITAA strongly believes that what is most urgently needed right now is an appropriate process for expediting treatment of procurements that are ready to move forward and where the need for immediate deployment is urgent and compelling. This expedited process should apply not only to federal acquisitions of anti-terrorism technology, but to priority non-federal procurements as well – particularly, procurements by state and local authorities with frontline homeland security responsibilities for protecting critical infrastructure that is high on the Department's threat matrix. There are many procurements that have been awaiting resolution of liability concerns provided by the protections afforded under the SAFETY Act. Some of these procurements involve securing ports, bridges, mail services and other facilities critical to our nation's security. The expedited process should include a provision requiring that SAFETY Act review be performed in tandem with the agency's proposal evaluation process to the maximum extent possible.

In addition, the interim final regulations are silent on many other comments in the procurement arena that were provided by ITAA and other groups in response to the proposed regulations. Specifically, we believe the regulations should encourage agencies to allow the submission of (1) bids or proposals for which the price, contract performance, or other terms are conditioned upon QATT designation; (2) bids or proposals in which the bidder reserves the right to withdraw the bid or proposal if QATT designation is not received, or (3) bids or proposals which are conditioned upon a price renegotiation if QATT designation is not received or an insurance requirement is set at a higher cost than was set forth as a stated assumption in the bid or proposal. QATT designation will make a material difference in many procurement contexts and the issues surrounding it should be treated with this kind of flexibility. We believe that corresponding revisions to the FAR should be pursued to make this requirement binding upon other government agencies.
There is no clear discussion of these issues in the interim final rule and we urge the Department to amend the regulations to address these issues explicitly.

Marketplace pressures continue to mount against contractors with either existing technologies capable of contributing to the war on terrorism, or technologies in development, to deliver these products and services to the federal government. Absent the protections promised by the SAFETY Act, we are concerned that contractors will not be able to respond to critical needs. We appreciate the Department's acknowledgement that it will work to prioritize reviews and urge the Department to provide in the final rules the greatest flexibility necessary to prioritize the reviews required for designation and certification, both with respect to on-going or planned procurements, and to critical technology needs for which the Department requires innovative technologies and services.

Issues Concerning the Designation/Certification Timeframe

ITAA is still concerned that the interim final rules contemplate a minimum 150-day period for the designation/certification process to run its course. In light of the urgent needs that exist today, a lengthy approval process timeframe could complicate the rapid development and deployment of QATT. More importantly, it is critical that the final regulations provide for an expedited approval process for the review of technologies already in use or substantially equivalent to existing QATTs, changes and modifications to existing QATTs, technologies that are the subject of pending procurements for the protection of high-risk targets or critical infrastructure, technologies for which the cost of insurance has changed significantly, and in other appropriate circumstances.

The draft regulations proposed and the interim final rule maintains an across-the-board term of five to eight years on all designations of QATT. Because DHS does not explain its rationale for establishing a mandatory expiration date, it is difficult to weigh the pros and cons of such a requirement. ITAA believes that an

automatic expiration date for every designation, regardless of the circumstances, will tend to discourage the development of anti-terrorism technology because the seller would know that a designation, even if granted, would be effective only for a limited period of time. We are also concerned that an arbitrary timeframe for designation would needlessly increase costs for both sellers and the Department; sellers would have to build costs for renewal of designations into their cost structures, and the Department would have to review such applications every five to eight years, even when there have been no material changes to the technology or service.

The SAFETY Act, as passed by Congress and signed into law by the President, provides no term for a designation under the SAFETY Act. ITAA believes very strongly that the regulations should require that designations will apply for an indefinite period. Changes in technology that would require re-approval of the designation/certification are addressed in other areas of the proposed and interim final regulations, and absent any material changes in the technology or the insurance covering the technology or service, the approval should extend indefinitely.

If the final regulations are to require some term for an effective designation, we believe that DHS should explicitly substantiate why the 5 to 8 year period is needed absent a legislative requirement in this arena. In that case, we also believe that the timeframe should be extended to a minimum of 10 years—if not substantially longer—which is more consistent with the effective dates of long-term services agreements and more realistically reflects the length of time necessary to develop and implement complex systems and services.

ITAA also has concerns with the interim final rule's determination that designation/certification will be effective on the date of issuance by the Department. ITAA believes that the regulations should provide that a designation and/or certification should take effect retroactively to the earlier of the date of deployment or the date of sales. The regulations should also state that once designation/certification is obtained, the liability protections of the SAFETY Act will apply even if the facts of a particular claim are alleged to have occurred prior to the effective date of the designation/certification. By providing protection to a seller who elects to make its technology immediately available to the public pending the DHS approval process, retroactive designation and certification would encourage the deployment of a QATT at the earliest possible date.

At an absolute minimum, a designation/certification granted by the Department should be retroactive to the date of application. Moreover, any effective date should be outlined in the approval certificate issued by DHS rather than in the regulations themselves.

Need for Broad Scope of QATT Designations and Approved Product Certifications

Members of this Committee led the charge during consideration of the SAFETY Act to include anti-terrorism services in the scope of items to be covered by designation and/or certification. Anti-terrorism services are as critical to security as anti-terrorism technologies and devices, and, given the wide variations in the complexity of such services, are likely to require much more flexibility in the regulatory review process. We're happy that the services industry is also represented on this panel by the Professional Services Council. I am certain you will hear much more about the critical role services play in the anti-terrorism arena. On behalf of the information technology service providers, we stress that the regulations should clearly provide that designations and certifications of QATTs are sufficiently broad to include all elements of the component products and services, including systems design and customer-approved changes and related services, such as operations, maintenance, integration, and training. We are also concerned that the regulations do not adequately address the need to cover the range of deliverables across the entire spectrum of a procurement; complex system integration services, for example, could include a range of employee training, maintenance, and upgrade services might be offered that could be beyond the traditional scope of a technology designation or certification.

DHS maintains that services will be provided the same treatment as technologies in their reviews by the Department. The interim final regulations stipulate that the same seven criteria will be used to review applications for certification that cover services. As I'm sure our colleagues from the Professional Services Council will discuss, the nature of services is unique and requires greater flexibility in the review and evaluation process. The interim final rules do not adequately address the unique nature of services in this new arena.

We are pleased to see that the interim final rules acknowledge that the Department intends to apply the statute to a broad array of technologies and services, both those under development and already available. Previously, a DHS spokesperson was quoted as saying the protections of the SAFETY Act applied only to new technologies. ITAA strongly objected to this interpretation of the Act and is happy to see that the Department has backed away from this statement.

We are also pleased that the Department acknowledges in the interim final rule that the specific purpose for which technologies are designed does not imply an exclusive purpose. Many technologies with applicability in the war on terrorism may not have been developed with the exclusive purpose of thwarting terrorist attacks, and ITAA is pleased that the Department has recognized this issue.

Insurance Provisions in the Proposed and Interim Final Rule

As provided in the SAFETY Act, the Department's regulations require that the Department be able to certify that, in order to receive QATT designation, the seller has obtained and is maintaining adequate liability insurance for a single act of terrorism to satisfy third party claims where the technology has been deployed. The amount of insurance is not to exceed an amount reasonably available on the world market at prices and terms that would not unreasonably distort the price of the technology or service.

Given the fact that availability of and cost of insurance to satisfy the requirements of the SAFETY Act is uncertain, ITAA believes that the regulations should provide expressly that the Department has the authority to designate/certify technologies or services in the absence of an available policy.

Of particular concern in this area is the statement made by the Department in the interim final rules that in the absence of adequate insurance, the Department may require applicants to self-insure up to an appropriate level of liability determined by the Department. This assertion would seem to run completely contrary to the spirit and intent of the protections envisioned under the SAFETY Act. The genesis of the SAFETY Act began with a known problem of virtually unlimited risks confronting suppliers of anti-terrorism technologies and services. The Department has consistently implied that because the protections afforded under the act are voluntary industry should therefore view coverage as a privilege and accept risks and costs not conceived of in the statute. The reliance on requirements to self insure in the absence of adequate market coverage demonstrates a backwards philosophy within the Department that despite an intense interest by the government in acquiring innovative technologies from the private sector, industry should be willing to incur significant costs and assume incredible amounts of risk to support the war on terrorism. ITAA believes that the final regulations should remove the requirement to self insure and expressly provide that in the absence of available insurance on the open market, the Department will declare an applicant's liability to be zero.

ITAA also believes that given the probable high cost of such insurance coverage compared to current coverage, the costs incurred by a seller for SAFETY Act coverage should be treated as allowable costs under Federal Acquisition Regulation (FAR) § 31.205-28. To eliminate the risk of any dispute on this point, ITAA recommends that the regulations themselves (not the Preamble) be amended to recognize that insurance certified under this section, whether the costs are treated by the contractor as direct costs or indirect costs, shall be considered "insurance required or approved and maintained by the contractor" within the meaning of FAR § 31.205-28(a)(1).

Within the context of insurance, the regulations also require sellers to provide an annual certification to the Department that it has and will maintain the required

insurance, and that sellers notify the Undersecretary for Science & Technology of any changes in the type or amount of insurance coverage for a QATT. There is no such requirement in the statute passed by Congress, and ITAA is concerned that yet another certificate will unnecessarily burden both industry and government. As such, we would recommend that this requirement be deleted from the final regulations.

ITAA shares the concern noted in other comments made to the Department about liability issues surrounding potential terrorist events that occur outside the United States, but which may have economic or other consequences inside this country. We are concerned that the regulations as currently proposed do not address the circumstance in which an act of terrorism involving QATT technologies that take place outside the United States; if a terrorist attack were perpetrated on a target outside the United States despite deployment of designated QATT, it could result in serious economic harm to the United States. We urge the Department to clarify in its final rules that incidents of terrorism occurring outside the United States that involves a QATT technology expressly will receive the same protections envisioned for similar events occurring within our borders. By the same token, the Department's final regulations should make clear that QATT designation and certification is available equally to U.S. sellers and non-U.S. entities that otherwise qualify. The statute makes no distinction. We view this as vital because the fight against terrorism is global and the U.S. Government should extend the protection of the SAFETY Act to sellers to deploy their technology overseas to, either in whole or in part, protect the interest of the United States.

Comments on the Single Federal Cause of Action

The Safety Act states that the United States District Courts "shall have original and exclusive jurisdiction" over suits involving claims relating to acts of terrorism when designated anti-terrorism technology has been deployed, but does not state explicitly that federal actions will preempt litigation in state or local courts.

In the Preamble to the Department's proposed rules, the agency concludes that the "exclusive Federal cause of action" necessarily pre-empts such litigation in non-federal courts, and that such cause of action may be brought only against the seller of the QATT, and not against "arguably less culpable persons or entities, including...contractors, subcontractors, suppliers, vendors, and customers of the [s]eller...." ITAA is generally pleased with the discussion of the single federal cause of action in the preamble to the interim final rules.

The extent to which sellers of designated technologies and their customers and suppliers are kept from being subject to a plethora of lawsuits in various fora is a fundamental premise of the entire QATT program, including most obviously the efficacy of the liability cap keyed to the required level of liability insurance. Given

the importance of this issue, we strongly recommend that the Department codify in a "Findings and Purpose" section of the final regulations themselves the Secretary's understanding of Congressional intent in the SAFETY Act and its resulting overview of the operation of the SAFETY Act program for which the Secretary is responsible, including the inter-relationships among the various sections of the SAFETY Act. Leaving critical matters of interpretation to the Preamble to the rule, rather than codifying such interpretations in the regulations themselves, may lead to confusion among all interested parties. This is true with respect to various issues the Department addresses in the Preamble, but perhaps nowhere is it more important than in this area, which gets to the heart of the protections to be afforded to sellers whose technologies obtain QATT status.

Post-designation and Certification changes to Approved Products and Services

The interim final rule provides for automatic termination of a designation granted by the Department if the technology is significantly changed or modified, including changes in the design, material, manufacturing process or purpose for which a QATT is sold.

In response to the proposed rules published by the Department in July, ITAA noted that it was concerned that if the regulatory process for dealing with changes in qualified technology is overly burdensome it will serve as a disincentive for sellers to make improvements to approved technologies. ITAA believes that only changes that could have an adverse effect on the safety or effectiveness of a QATT would trigger a termination, and we believe the regulations should explicitly provide as such.

ITAA is pleased that the interim final rules have been amended to recognize that a change to an approved QATT will be considered significant only if the change materially affects the function or operation of the QATT, i.e., is detrimental to the safety of the technology or service. It is critical to define as precisely as possible in the final regulations when a change must be submitted to DHS; ITAA believes that the regulations should clarify that upgrades, enhancements, and other changes standard in the particular industry are not subject to additional review, and that the regulations provide for an expedited review of amendments to previously approved QATTs. Because the loss of a QATT designation/certification could be financially ruinous, any ambiguity in the proposed regulations on when a re-submittal is required might lead a seller to conclude that even the most minor changes trigger the requirement to supply additional information to the Department. This would impose significant administrative and financial burdens on the seller, and would result in significant delays in the re-approval of technologies as a result of what we perceive would be a flood of unnecessary filings.

One possible approach to resolving the problem of ambiguity is to provide that the designation for each QATT will be drafted in a way that includes changes approved by the customer and identifies the types of additional changes that will require re-application. As noted above, we believe the regulations should provide the greatest specificity possible on the kinds of changes that will require re-approval. Absent such specificity, ITAA is concerned that every lawsuit involving a QATT will include allegations that the technology was significantly changed and that the original designation was invalidated.

ITAA also believes that the procedures for modifications do not adequately address the nuances of the services environment. The nature and delivery of services may change on a much more frequent basis than the root technology, and the final regulations issued by the Department need to address the specific challenges with upgrades and modifications related to the delivery of services.

Procedures to Ensure the Confidentiality of Information Submitted as Part of Applications for Designation and/or Certification

A substantial portion of the data that a seller is required to disclose to DHS for designation/certification will constitute confidential and proprietary commercial and technical information, including trade secrets. The Department has recognized that "successful implementation of the Act requires that applicants' intellectual property interests and trade secrets remain protected in the application and beyond." The Preamble specifically recognizes the flexibility in the Freedom of Information Act ("FOIA"), but offers no guidance on how it will apply to information submitted in the application process. Id. The regulations also include little guidance for assuring the required protection beyond stating that the application and review process will maintain the confidentiality of an applicant's proprietary information. Section 25.8. We believe that significant modifications to the regulations are essential to assure the protection of proprietary data.

ITAA also believes that the regulations should include specific restrictions on disclosure of (a) information submitted in connection with an application for Designation or Certification, and (b) documents and other materials prepared by Government employees, representatives, or private contractors in connection with the evaluation of applications. The restrictions should explicitly state that the prohibitions in FAR § 3.104-4 are applicable to disclosure of such information if it constitutes "contractor bid or proposal information" or "source selection information" within the meaning of the Procurement Integrity Act, 41 U.S.C. § 423. For information that does not relate to a specific Federal agency procurement, the regulations should include disclosure prohibitions and procedures that are substantially the same as the provisions of FAR § 3.104-4.

Moreover, the regulations should include a rebuttable presumption that information submitted in the application and review process will be deemed to be privileged and confidential "trade secrets and commercial or financial information" exempt from disclosure under the Freedom of Information Act ("FOIA"), regardless of whether the information is marked with proprietary legends and limitations. See 5 U.S.C. § 552(b)(4).

The regulations should also provide that information submitted in the application and review process will be treated as information that "concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association" within the meaning of the Trade Secrets Act, 18 U.S.C. § 1905, regardless of whether the information is marked with proprietary legends and limitations.

The regulations should require DHS in every instance to provide advance notification to the submitter when considering whether to disclose SAFETY Act information to third parties, give the submitter the right to refuse to agree to disclosure of the information, and to seek judicial review of any decision to disclose the information before such disclosure is made.

The broader Homeland Security Act provides that "critical infrastructure information" submitted to DHS – information that is related to the security of critical infrastructure or protected systems -- will be exempt from disclosure under the FOIA. See Homeland Security Act, P.L. 107-296, Section 214(a)(1)(A); 6 U.S.C. 133 (2002). Because much of the information submitted by Sellers may constitute "critical infrastructure information," we suggest that the DHS regulation on confidentiality of information submitted as part of the consultation, Designation, and Certification processes include a cross-reference to the "critical infrastructure information" protections provided by the statute.

The concerns that ITAA has in this arena are magnified as a result of the incredible amounts of data the Department intends to require of applicants. We would note that on the issue of burdens outlined in the interim final rules, there is still a lack of information provided in the rules themselves as to the scope of information required of applicants. In the absence of a discussion of the kinds and amount of data to be required, we believe it will be difficult to provide precise responses to the Department's burden estimates. We urge the Department again to release the draft application kit in a formal way and solicit comments from industry before adopting the application as final.

The Regulations Need to Provide an Appeal Process for Denials of Applications for Designation and Certification

The proposed and interim final regulations provide that the Undersecretary's decisions on designation and certification are final and not subject to review. ITAA is confident that the vast majority of technologies submitted to the Department under these regulations will be highly complex and involve innovative approaches to deter a wide range of chemical, biological, nuclear, and other threats. Given the likely variety and sophistication of these technologies, ITAA believes there is a real risk that significant features may be overlooked or misunderstood during the review and evaluation process, particularly if DHS elects to undertake the review without meeting with the applicant. DHS notes in the preamble to the interim final rule that it believes the review process will be highly interactive, and thus, the need for an administrative review will be unnecessary.

We believe the interests of the government and the public would be best served by a process that builds in a method to resolve uncertainties and correct errors. While the regulations provide for delegation of the authorities afforded to the Secretary under the Act to the Undersecretary for Science & Technology, it would certainly seem appropriate for an applicant to have recourse to appeal to the entity assigned responsibility in the statute for the adoption and enforcement of the Act.

As such, we recommend that the final regulations explicitly provide that the applicant has a right to administrative review by the Secretary of a decision by the Undersecretary to deny or restrict the scope of a designation of technology as QATT or to deny certification of a QATT as an approved product for homeland security. There should be an opportunity for a second look at an application.

Relationship Between SAFETY Act Coverage and Indemnification Under Public Law 85-804

The Preamble to the rule notes that DHS believes "Congress intended that the SAFETY Act's liability protections would substantially reduce the need for the United States to provide indemnification under Public Law 85-804 to sellers of anti-terrorism technologies." At the same time, the Department recognizes that there may be certain circumstances in which SAFETY Act coverage and indemnification under Public Law 85-804 is warranted.

President Bush issued Executive Order 10789 on February 28, 2003, which grants the Secretary of DHS the authority to issue indemnification under Public Law 85-804 and also provides that federal agencies (other than an exception for the Department of Defense) cannot provide indemnification "with respect to any matter that has been, or could be, designated by the Secretary of Homeland Security as a qualified anti-terrorism technology" unless the Secretary of DHS had advised whether SAFETY Act coverage would be appropriate and the

Director of the Office of Management and Budget has approved the use of indemnification.

Both the Preamble and the regulations are silent as to circumstances when indemnification under Public Law 85-804 might be warranted, and the process by which the Secretary will review determinations of other federal agencies to issue indemnification for "any matter that has been, or could be . . . a qualified anti-terrorism technology." We believe that the regulations should include some clarification of these issues.

ITAA recommends that the final regulations provide that designation under the SAFETY Act "shall not" preclude the granting of indemnification under appropriate circumstances. For example, a seller might need indemnification under Public Law 85-804 to protect against damages that might occur if the technology is deployed and there is injury other than that arising from an act of terrorism.

Moreover, ITAA recommends that the regulations clarify that, as part of the process for determining whether SAFETY Act or indemnification under Public Law 85-804 is appropriate, the Secretary of DHS will consult with OMB and other agencies as appropriate but will not exercise a "veto" authority over the determinations of other agencies.

Conclusion

As noted at the beginning of our testimony today, ITAA generally supports the approach taken by the Department in issuing proposed regulations to implement the SAFETY Act. We stand ready to support the Department as it works through the changes suggested by ITAA and many other organizations to ensure that the final regulations provide the best possible framework to ensure the most cutting-edge technologies are available to the Department to support our overarching war on terrorism. Thank you for the opportunity to appear before the Committee today. I would be happy to answer any questions from the Committee.

Chairman TOM DAVIS. Stan, welcome.

Mr. SOLOWAY. Thank you, Mr. Chairman.

The professional Services Council is pleased to respond to your invitation to testify this morning on the SAFETY Act. PSC is the leading national trade association representing the professional and technical services companies doing business with the Federal Government, and our members are among the leaders in the provision of homeland security and national security technologies and related services.

As we know, effective prosecution of the war on terror requires that the U.S. Government and others have access to the full range of technologies and technology-based solutions. For many of these solutions, the potential for aiding in this crucial battle are quite significant, but so too are the liabilities. As such, providing an appropriate degree of protection against those liabilities is vital.

Such liability protection for other technology areas is both common and accepted; for example, the Defense Department has long had the authority to address extraordinary risks in its contracts. The security provided is essential to both contracting parties. These and related liability protections are not designed to protect companies from their day-to-day responsibility for performance. Rather, they exist to provide a reasonable degree of protection in the event of an occurrence that is anything but routine.

Our ability as a Nation to capture and utilize needed technology for homeland security requires us to understand and address this fundamental reality. As such, PSC and others have been actively involved in the discussions over the acquisition policy and liability protection provisions of the legislation creating the Department of Homeland Security and under the SAFETY Act.

Mr. Chairman, you and others on this committee immediately recognized the importance of this issue and proposed legislation to extend indemnification protections to antiterrorism technologies, similar to the "extraordinary relief" provisions afforded to defense technologies. We supported that proposal and continue to believe it is an important part of the solution. Others proposed a tort reform approach to strictly limit the liabilities that any one technology developer-owner would face. Each of these approaches has merit. Most importantly, Congress recognized the importance of providing such protections and, in the end, decided to enact a tort reform regime through the SAFETY Act. PSC strongly supports the act and compliments the Department for issuing its interim final rules this week.

The SAFETY Act represents an important step toward ensuring the government's ability to access the full scope of antiterrorism technologies and capabilities. However, from the perspective of the technology services base, PSC remains concerned that the regulations do not adequately address the critically important specifics relating to the act's application to services in particular. Since services will account for a substantial portion of the procurements of the antiterrorism technologies and solutions, this is an issue of significant importance.

The very nature of technology means that the provision of services differs in many critical respects from the provision of goods. It is important, for instance, to recognize that the services provider

might require qualification eligibility for a broad business area, rather than for a discrete technology use. The interim rule narrowly prescribes the scope of coverage by focusing on a deployed technology.

Similarly, the review and approval process must be sufficiently flexible to address the special characteristics of these services offerings. For example, many solutions evolve and cannot be completely defined or fixed in advance. It is therefore important to provide coverage when systems design, for instance, is part of the contract performance. The regulations seem to assume the opposite. In the absence of such protections, sellers may be unwilling to bring technologies to market.

On the positive side, we compliment the Department for outlining in the notice accompanying the proposed interim rules the Department's regulatory philosophy and interpretations. To add further clarity, we recommend that the Department incorporate these statements and views into the final regulations themselves. That way, all participants will have ready access to the information and be able to use that information directly in the application and interpretation of the specific provisions of the regulations.

We also support the strong statutory and regulatory statements of coverage regarding services. The law is also, properly, technology-neutral with respect to the scope of coverage and the protections offered. In our view, the regulations must be written in a neatly technology-neutral manner to the maximum extent practicable.

We support the broad definition of the term "qualified antiterrorism technologies" under the law and regulations. The categories of technologies that are available for designation must continue to be viewed broadly. This is particularly important in the services sector.

However, the interim rule states that a designation will only be valid for being 5 to 8 years. In our view, absent the change in circumstances initiated by the seller after the Department's approval of the designation, there is no public policy reason to impose any fixed period of time on the useful life of the designation period. Further, under the interim rule, a designation will terminate automatically and have no further force or effect if the solution is significantly changed or modified. We strongly oppose the automatic termination of the designation. We believe each case will have its own circumstances and should be treated as such, particularly in the services realm where the focus is on evolving solutions, rather than on static devices.

With respect to the certification of an application of a government contractor, we encourage the Department to use its rulemaking authority to recognize that some of the information to support applications for certification may be available and applicable to products but not for services.

With respect to the issue of proprietary information, the interim rule, while appropriately recognizing the importance of such protection, regrettably does not define the procedures that applicants should follow to ensure that their proprietary data and trade secrets are protected. We strongly recommended before and continue to recommend that the Department develop a proprietary data-

marking or other application notice by which applicants highlight or disclose those portions of the application that are proprietary.

Finally, with respect to the relationship between the SAFETY Act and Public Law 85–804, "Extraordinary Relief," we compliment the Department for acknowledging the interrelationship between these two important government contracting statutes and for recognizing that there are circumstances under which 85–804 relief will be appropriate. However, because there are some intrinsic and potentially unsolvable tensions associated with the SAFETY Act's effectiveness in the services sector, we continue to believe it important that the 85–804 authorities be clear and appropriately available. We recommend, therefore, that the Department create a new section in the regulations to specifically address this important matter.

Mr. Chairman, PSC supports the SAFETY Act and encourages the Department to move expeditiously with finalizing regulations, processing applications, and addressing the issues that we and others have raised. This law, in its implementing regulations, is designed to create an incentive for the deployment and development of technologies that will enhance our domestic security; and we hope these technologies work so well the United States never again faces a terrorist attack, but we must be prepared.

PSC would welcome the opportunity to work with you and the committee, the House Select Committee, and the Department on the further development of the regulations and in monitoring the implementation of the SAFETY Act. Thank you for the opportunity to testify today. I would be happy to answer any questions.

Chairman TOM DAVIS. Thank you very much.

[The prepared statement of Mr. Soloway follows:]

TESTIMONY

by Stan Soloway
President
Professional Services Council

before the

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

October 17, 2003

2101 Wilson Boulevard, Suite 750, Arlington, VA 22201-3009, 703/875-8059, Fax 703/875-8922, http://www.pscouncil.org

TESTIMONY OF

STAN SOLOWAY
PRESIDENT
PROFESSIONAL SERVICES COUNCIL

Before The

COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

OCTOBER 17, 2003

The Professional Services Council (PSC) is pleased to respond to your invitation to testify on the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act", or "the Act"). PSC is the leading national trade association representing the professional and technical services companies doing business with the federal government. PSC's approximately 155 member companies perform billions of dollars in contracts annually with the federal government, providing the full range of services, including information technology, high-end consulting, engineering, economic, international development, scientific and environmental and remediation services. Moreover, PSC's members are among the leaders in the provision of homeland security and national security services.

As part of the comprehensive congressional response to the tragic events of September 11, 2001, Congress passed the Homeland Security Act of 2002 and created the Department of Homeland Security. Congress also took a bold step to include the SAFETY Act within that comprehensive statute.

Chairman Davis, we appreciate your personal leadership on this issue, along with that of Congressman Jim Turner, the former Ranking member of your Subcommittee, and now the Ranking member on the House Select Committee on Homeland Security.

PSC was actively involved in the debate on the acquisition policy and liability provisions leading toward enactment. The SAFETY Act represents an important step toward assuring the market's (including federal and state governments) ability to access the full scope of anti-terror technologies and capabilities. PSC strongly supports the SAFETY Act, and compliments the Department for moving expeditiously to issue proposed regulations on July 11, 2003 and interim final regulations this week. In addition, the Department is conducting public seminars to share information on the Act and the application process.

Attached to my statement are two sets of comments that PSC submitted to the Department on their proposed rule. One set was submitted from PSC alone. In addition, PSC joined with other associations in submitting complementary additional comments on the proposed rule.

I would like to offer PSC's perspectives on both the broader issues associated with liability protection and indemnification for homeland security technologies, as well as the more specific issues associated with the SAFETY Act and the Department of Homeland Security's rules to implement that statute.

Effective execution of the war on terrorism requires that the U.S. Government and others have access to the full range of technologies and technology-based solutions, from sensors to aid in the detection of biological agents to information systems that enhance the ability of the nation to defend itself against, and respond to, acts of terrorism. For many of these solutions, the potential for aiding in this critical battle is quite significant, but so too are the liabilities that could arise in the case of an extraordinary occurrence that could not reasonably be anticipated or protected against. As such, providing an appropriate degree of protection against those liabilities is vital.

Such liability protection for other technology areas is both common and accepted. The Defense Department has long had the authority to address extraordinary risk in its contracts. Such clauses are reasonably common but have rarely been invoked. Yet the security they provide is essential to both contracting parties. Similarly, the nuclear industry participates in a special program under the Price-Anderson Act, and the government routinely provides needed assistance and relief in the case of natural or other extraordinary disasters. These liability protections are not designed to protect companies from the day-to-day responsibility associated with the normal performance of their work. Rather, they exist to provide a reasonable degree of protection in the event of an occurrence that is anything but routine. Perfection in technology is, after all, not 100%. And our ability as a nation to capture and utilize needed technologies requires us to understand and address this fundamental reality.

Mr. Chairman, you, Congressman Turner, and others on this Committee in the last Congress recognized this reality for homeland security and proposed legislation to extend indemnification protections to anti-terrorism technologies similar to the "extraordinary relief" provisions afforded to a select group of defense technologies for which similar risks exist. Others proposed to approach the issue from a tort reform perspective to strictly limit the liabilities that any one technology developer could face.

Each of these approaches has merit. In the end, Congress opted to enact a tort reform regime through the SAFETY Act. We are appreciative that both the Congress through this legislation and the Administration in their regulatory implementation have clearly and unequivocally recognized the importance of providing reasonable protections. At the same time, the President has extended to additional Executive Branch agencies the limited authority to utilize the extraordinary relief contract protections previously only available to the national defense agencies. These are both important, and positive, steps forward.

However, from the technology services base perspective, these protections may be inadequate to address the very real and legitimate concerns we face. The SAFETY Act, while appropriately covering services as well as products, presents a set of complications unique to services that I will discuss in more detail. Likewise, the authority granted by the President to agencies to utilize "extraordinary relief" provisions in conjunction with the SAFETY Act is extremely narrow and complex, and will likely be rarely applied.

For those reasons, Mr. Chairman, the Professional Services Council greatly appreciates your continued leadership in this area and your and the committee's continued commitment to ensuring that the laws and regulations in this area maximize the Nation's ability to access and utilize the many new and promising technologies that can substantially assist the global war on terrorism.

TREATMENT OF SERVICES

PSC remains concerned that the proposed implementing regulations do not adequately address the critically important specifics relating to the Act's application to services. We are mindful that the regulatory flexibility is limited by the inherent tensions created by the underlying statute. Nonetheless, since services will likely account for a significant portion of the procurements of anti-terror technologies and solutions, it is critical that the regulations provide as much detail and specificity as possible. Moreover, it is equally important that the regulations provide for broad coverage and clear instruction and guidance for balancing the statutory direction with sound business practices that will benefit the government and purchases. However, we are concerned about what we have seen of the application kit prepared by the Department.

We compliment the Department for including the extensive background information in the notice accompanying the proposed rule. Having the Department spell out its interpretations of the Act and its legislative history, and giving the public information on areas where the Department has made an initial determination of how to implement the Act and where additional comments from the public are requested, was extremely valuable in the formulation of our comments on the proposed rules. We recommend that the Department incorporate as part of the regulation (not merely in background or supplemental information) the Department's interpretations and regulatory philosophy. By making these views part of the regulations, all participants will have ready access to the information and be able to use that information directly in the application and interpretation of other specific provisions of the regulations.

We support the strong statements of coverage under the law and regulations for those companies offering services to address terrorism. The law is properly technology-neutral with respect to the scope of coverage and the protections offered. In our view, the regulations should be written in a technology-neutral manner to the maximum extent practicable, and only provide technology-specific guidance when such information would specifically address a unique application of the law to a given technology.

TIMING

PSC appreciates the Department's issuance of interim rules this week. We recognize the difficulty of developing rulemaking on each and every provision of the Act, and the importance of maintaining an important balance between the flexibility to address technologies and circumstances with the certainty in the application process and protections of the Act that Sellers and purchasers require. The interim rules, which closely mirror the proposed July 11 rules, offer further but still inadequate clarity and guidance.

Furthermore, on September 12, 2003 the Department sought an expedited OMB approval for the forms that interested applicants can use to apply for Designation or Certification. It is in the Department's and the potential Sellers' best interests to immediately commence the application process for both Designation and Certification. However, these applications appear to be overly complex and unnecessarily burdensome. We are concerned that this daunting process will dissuade applicants, or worse, dissuade companies from offering anti-terrorism technologies to the marketplace.

DESIGNATION AND CERTIFICATION OF QUALFIFIED ANTI-TERRORISM TECHNOLOGIES ("QATT")

We support the broad scope of the term "qualified anti-terrorism technologies" under the law and regulations. We recommend that the categories of technologies that are available for Designation continue to be viewed broadly; this is particularly important when evaluating the application of the Act and regulations to services.

PSC worked directly with the Congress last year to ensure that a wide range of services, including support services and information technology, were included in the definition of "qualified anti-terrorism technology"("QATT"). In our view, the types of services that may qualify as a QATT include, but are not limited to, training, maintenance, systems integration, testing, installation, repair, safety services, modeling, simulation, systems engineering, clean-up and remediation services, protective services, research and development, vulnerability studies, emergency preparedness planning and risk assessments. Information technology is also typically considered a service, although the Act separately identifies information technology as a "technology" under the Act.

We were pleased to see the Department's acknowledgement of this broad scope of coverage in the background section of the proposed and interim rules. In addition, recognizing that providing "services" differs in some respects from providing "goods," we further recommended that a Seller may seek qualification eligibility based on coverage for a business area and not only for a particular technology use (such as for "hazardous material remediation services," not merely for anthrax remediation). It does not appear that the Department is willing to go that far, yet.

Sales of services (or sales that include services) to prevent and respond to terrorist attacks are likely to be the subject of the majority of the applications for Designation and Certification, in part because, as a practical matter, anti-terrorism devices will be of little or no use unless there are people who can install, operate, maintain, and repair those devices, as well as people who can design and implement the complex systems necessary to deploy anti-terrorism solutions. The review and approval process for Designation and Certification of anti-terrorism technology must be sufficiently flexible to address the special characteristics of these services offerings. It is hard to tell from the first reviews of the application process whether that flexibility exists.

As such, although some proposals for services contracts may provide definite specifications that will allow Designation at, or shortly after, the time of the selection of the winning proposal and award of a contract, many professional services are not provided according to "specifications" that are determined in advance. For anti-terrorism activities that require sophisticated information technology, a "systems integrator" or "solutions provider" is likely to provide key services to implement the overall anti-terrorism system. For complex information technology systems, the design of the system is often one of the tasks performed under the contract. The regulations, however, appear to contemplate that specifications will be determined before the Seller begins work under the contract. It is important that the regulations provide for QATT protection when systems design is part of the required contract performance. In the absence of such protection, Sellers may be unwilling to proceed.

The regulations should also provide that in appropriate circumstances relating to an anti-terrorism procurement, systems design and other services themselves may be designated as QATT from the inception of performance.

With respect to the Designation to be made by the Under Secretary, the proposed rule provides that it is valid and effective for a term of five to eight years (as determined by the Under Secretary based on the technology) commencing on the date of issuance. In our view, absent a change in circumstances initiated by the Seller after the Department's initial approval of the Designation, there is no public policy reason to impose any fixed period of time on the useful life of the Designation period of a QATT. Indeed, in some cases, a contract performance period can extend beyond five or eight years. The Department has not accepted this recommendation.

We also encourage the Department to make the effective date of the Designation the date of the application for Designation. The Department has rejected retroactive application.

Further the rule provides that a Designation shall terminate automatically, and have no further force or effect, if the QATT is significantly changed or modified. The rule defines the term "significant change" as one that could significantly affect the safety or effectiveness of the device," including a significant change or modification. We strongly oppose the automatic termination of the QATT Designation, even where based on significant changes or modifications. This must be a case-by-case determination.

With respect to the Certification for and application of the government contractor defense, we have assumed that the title "approved product list" in the Act and the proposed regulations is not intended by Congress or the Department to exclude services. The Act and the regulations intentionally use the term "anti-terrorism technology" to refer to the source of approval, and that term is specifically defined in the Act and regulations to include services. We encourage the Department to use its rulemaking authority to recognize that different information to support the application for Certification may be available and applicable to products that may not be available or applicable to services. We believe the Department has adopted this approach.

PROPRIETARY DATA

With respect to the issue of protecting company proprietary information, we compliment the Department for recognizing the importance of protecting the confidentiality of an applicant's intellectual property, trade secrets and other confidential information. It is important to explicitly provide procedures that applicants should follow to ensure their information can be protected. For example, we strongly recommend that the Department develop a proprietary data marking or other application notice by which applicants highlight or disclose those portions of its application it considers to be proprietary. For example, the Department could draw easily from the marking and identification process used in the federal procurement system. While the Department continues to make strong statements recognizing the importance of protecting proprietary data, it remains to be seen how that protection will be provided.

RELATIONSHIP BETWEEN SAFETY ACT AND P.L. 85-804

Finally, with respect to the relationship between the SAFETY Act and P.L. 85-804, we compliment the Department for addressing coverage of the relationship between these two important government contracting statutes and acknowledging that there are circumstances under which these two acts can, and should, co-exist. We recommend that the Department create a new section in their regulations to address this important matter, including a recognition that a broader application of 85-804, particularly for services, may well be needed to ensure appropriate protection for Sellers and, in turn, for DHS's ability to access those solutions.

CONCLUSION

This law and its implementing regulations are designed to create an incentive for the development and the deployment of anti-terrorism technologies. We hope that these technologies work so well that the U.S. never again faces a terrorist attack. But we must be prepared. PSC fully supports the SAFETY Act, and we are encouraged that the Department is moving expeditiously with final regulations and in processing applications. We hope the application process does not become a barrier to implementation.

PSC would welcome any opportunity to work cooperatively with this Committee, the House Select Committee, and the Department on the further evaluation of the regulations and in monitoring the implementation of the Act and regulations.

Mr. Chairman, PSC appreciates the opportunity to appear today and share our support for the SAFETY Act and for the efforts to stop terrorism. I would be pleased to respond to any questions.

Chairman TOM DAVIS. Mr. Clerici, welcome.

Mr. CLERICI. Thank you, Mr. Chairman, and members of this committee. It's an honor for me to testify before you today regarding the SAFETY Act and its impact on deploying safe and effective antiterrorism technologies in the United States and abroad. I applaud the leadership that you, Mr. Chairman, and this committee have shown in the areas, of Federal procurement policy, national security and homeland security.

I appear before you today representing the Chamber of Commerce of the United States of America. The Chamber is the world's largest business federation, representing more than 3 million businesses and organizations of every size, sector and region. My testimony is based on over 24 months of direct experience advising large government contractors, pharmaceutical companies, biotech companies, and small businesses throughout America and, indeed, throughout the world, on how to bring the best possible homeland security and antiterrorism solutions to both government and private markets.

Let me begin by saying that the Chamber applauds the Department of Homeland Security in its effort to ensure that the SAFETY Act provides the full protections intended by Congress. Clearly, the interim regulations' dual goals of certainty and flexibility are in keeping with the spirit of the SAFETY Act. Most significantly, the Chamber wholly endorses the Department's proper interpretation of both the jurisdictional consequences of the statute—namely, that only the seller of designated and qualified antiterrorism technologies is a proper defendant in any action arising out of an act of terrorism—and the impact of the statutory "government contract or defense" as providing early dismissal from any tort suit involving a certified qualified antiterrorism technology following an act of terrorism.

The Chamber appreciates the Department's and this committee's recognition here today that there exist a number of antiterrorism technologies that have not and cannot be deployed by sellers unless and until they receive designation and/or certification under the SAFETY Act. The Chamber applauds this recognition and the Department's efforts to stimulate applications, including its innovative preapplication process. The Department also acknowledges that several technologies already have been deployed without protections of the SAFETY Act. However, while the interim rules attempt to address the issue of retroactive application of the protections of the SAFETY Act to such technologies, as we heard earlier today in response to Congressman Schrock's question, the Department appears to have too narrowly limited the possibility of such retroactive application. Clearly, Congress did not intend to limit the scope of the SAFETY Act only to newly developed technologies.

With respect to the retroactive application of the SAFETY Act, in the Chamber's view, so long as no cause of action has been accrued—that is, there has been no terrorist incident involving an antiterror technology resulting in a lawsuit against a seller—the Department may provide SAFETY Act protection retroactively to previously deployed technologies that are substantially identical to a qualified antiterrorism technology. Nothing in the statute limits such an action. The Chamber intends to provide additional com-

ments to urge clarification of this point and changes to the interim rule.

With respect to the precise types of technologies meriting protection of the SAFETY Act, Section 865(l) of the act notes that qualified antiterrorism technologies may include technologies deployed for the purpose of, "limiting the harm such acts [of terrorism] might otherwise cause." The "harm" that might be caused by an act of terrorism clearly goes beyond the immediate effects of the act itself. An act of terrorism such as the attacks of September 11 or the October 2001, anthrax attacks triggers a number of immediate remedial and emergency responses to limit the resulting harm and deter followup attacks. For example, immediately following the detection of anthrax in the offices of Senator Tom Daschle and Senator Patrick Leahy, Members of Congress and their staffs were treated with antibiotics and other prophylactic measures with the specific goal of limiting the harm that this act of terrorism could cause. Clearly, any injuries that might have been caused by the administration of these treatments, even though direct results of the act of terrorism itself, could be directly traced to the act and the objective of limiting the resulting harm. Moreover, any claims brought as a result of such injuries would clearly be arising out of, relating to, or resulting from an act of terrorism.

Congress recently acknowledged that technologies designed to limit the harm from an act of terrorism that may result in harm not directly caused by the act of terrorism are protected by the SAFETY Act. In the legislative history of the "Project Bioshield Act of 2002," Congress stated that the Secretary of Homeland Security is "encouraged to designate [biodefense] countermeasures as 'qualified antiterrorism technologies'." The Department should affirm this congressional statement that technologies deployed after a terrorist attack with the hope of limiting harm may receive such designation.

The Chamber appreciates that the Department has taken positive steps to more narrowly define the, "substantial modification" as one that significantly reduces safety and effectiveness and its willingness to promptly review notices of modification.

Unless the Department informs the seller otherwise, however, these designations should remain in force. Only upon a showing and a determination by the Department that there has been a significant change or modification should the Secretary be able to affirmatively terminate a designation. It should only take effect upon written notice to the seller.

The Chamber appreciates the opportunity to offer testimony on this very important statute. Achieving the objectives of certainty and flexibility in implementing the SAFETY Act are of the utmost importance to ensuring the homeland's protection and the protection of national security. We applaud your efforts and the efforts of the Department and look forward to the implementation of the act.

Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much.

[The prepared statement of Mr. Clerici follows:]

McKenna Long
& Aldridge LLP
Attorneys at Law

JOHN M. CLERICI, ESQUIRE
MCKENNA LONG & ALDRIDGE LLP
WASHINGTON, D.C.

TESTIFYING ON BEHALF OF
THE CHAMBER OF COMMERCE
OF THE UNITED STATES OF AMERICA

BEFORE THE HOUSE GOVERNMENT REFORM COMMITTEE

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

October 17, 2003

Mr. Chairman, Ranking Member Waxman, and Members of the Committee, it is an honor for me to testify before you today regarding the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act") and its likely impact in deploying safe and effective anti-terrorism technologies in the United States and abroad. I would like to recognize the commitment and leadership on the issue of homeland security from the Professional Services Council and the Information Technology Association of America. Finally, Mr. Chairman and Ranking Member Waxman, I applaud the leadership that both you and this Committee have shown in the areas of federal procurement policy, national security and homeland security.

I appear before you today representing the Chamber of Commerce of the United States of America. The Chamber is the world's largest business federation, representing more than three million businesses and organizations of every size, sector and region.

My testimony is based on over twenty-four months of direct experience advising large government contractors, pharmaceutical and bio-tech companies, and small businesses throughout America and throughout the world on how to bring the best possible homeland security and anti-terrorism solutions to both the government and private markets while ensuring these same companies fulfill their obligations to their owners - and in particular, their shareholders - by mitigating their risk of potential liability to the maximum extent possible. That effort culminated, in part, in the passage of the SAFETY Act in November 2002. Over the last two years, my firm has provided counsel to numerous companies selling anti-terrorism products and services, such as chemical/biological detection devices, perimeter security systems, biometric identity products, bio-defense vaccines, and airport security systems.

On July 11, 2003, the Department published in the Federal Register for notice and comment proposed implementing regulations for the SAFETY Act. On August 11, 2003, the Chamber filed comments regarding the proposed regulations. As you aware, final interim rules were published in the Federal Register just yesterday. While we are heartened that the Department has satisfactorily addressed a number of our concerns, several issues remain worthy of further comment.

Let me begin by saying that the Chamber applauds the Department of Homeland Security in its efforts to ensure that the SAFETY Act provides the full protections intended by Congress. Clearly, the interim regulations' dual goals of certainty and flexibility are in keeping with the spirit of the SAFETY Act. Most significant, the Chamber wholly endorses the Department's proper interpretation of both the jurisdictional consequences of the statute (namely, that only the Seller of designated qualified anti-terrorism technologies is a proper defendant in any action arising out of an act of terrorism when such technologies have been deployed) and

the impact of the statutory "government contract or defense" as providing early dismissal from any tort suit involving a certified qualified anti-terrorism technology following an act of terrorism.

The Chamber concurs with the Department's recognition that the "government contractor defense" referenced in the language of the SAFETY Act statutorily supplants the common law government contractor defense, thereby relieving the Seller of proving the common law elements of this defense in any tort suit filed against the Seller as a result of an act of terrorism. In such suits, the Seller would be required only to submit evidence that its qualified anti-terror technology has been "certified" by the Department under Section 863 of the Act, triggering a presumption of dismissal for the Seller and all other protections afforded by the SAFETY Act. If the SAFETY Act is to operate as Congress intends, the presumption of dismissal must not be subject to judicial permutations and interpretations of the common law government contractor defense.

We urge the Department to take appropriate actions in implementing the SAFETY Act in accordance with the interim rule to ensure that upon showing that a qualified anti-terrorism technology has been certified under Section 863 of the Act, the Seller is entitled to immediate dismissal of the action if the plaintiff fails to meet its burden to rebut this presumption.

The Chamber appreciates the Department's recognition that there exist today a number of anti-terrorism technologies that have not and cannot be deployed by Sellers unless and until they receive designation and/or certification under the SAFETY Act. The Chamber applauds this recognition and the Department's efforts to stimulate applications, including through its innovative pre-application process. The Department also acknowledges that several technologies already have been deployed without the protections of the SAFETY Act. However, while the interim rules attempt to address the issue of retroactive application of the protections of the SAFETY Act to such technologies, the Department appears to have too narrowly limited the possibility of such retroactive application. Clearly, Congress did not intend to limit the scope of the SAFETY Act to newly-developed technology.

With respect to retroactive application of the SAFETY Act, in the Chamber's view, so long as no cause of action has accrued (i.e., there has been no terrorist incident involving an anti-terror technology resulting in a lawsuit against a Seller), the Department may provide SAFETY Act protection, retroactively, to previously deployed technologies that are substantially identical to a qualified anti-terrorism technology. Nothing in the statute limits such an action. The Chamber intends to provide additional comments to urge clarification of this point in the interim rule.

With respect to the timeline for the application process itself, while the one-hundred-fifty (150) day time period provided by the interim regulations for both designation and certification under the SAFETY Act attempts to balance the need

for urgency with the requirements for certain reviews and evaluations of anti-terrorism technologies under the Act, we are concerned that this time frame is too lengthy and rigid. This is particularly true for those anti-terrorism technologies that are ready and urgently needed for deployment but which companies will not deploy until SAFETY Act coverage is provided. Early indications from the Department suggest that the application process may be unnecessarily burdensome, leading to both a lengthy review period post-application as well as extensive expenditures of Seller's resources during the application preparation process. This will, obviously, have a greater adverse impact upon small businesses where both time and money are scarce. In short, it appears the entire process - both pre and post application - may be open to further streamlining.

The interim rules note the need for the Department to retain discretion over the approval process and the Chamber, for the most part, agrees. However, the Chamber believes the decision whether to designate a technology as a qualified anti-terrorism technology and the decision whether to certify a technology as an "approved product" for purposes of the statutory government contractor defense should be subject to an internal appeal process similar to an agency-level bid protest. Under this process, the Chamber suggests that the Secretary of Homeland Security could review a decision by the Under Secretary to deny resignation and/or certification. The Chamber agrees that this decision by the Secretary should be final and not subject to further review.

Section 865(2) of the SAFETY Act defines an "act of terrorism" triggering coverage to include an act that "causes harm to a person, property, or entity, in the United States." We applaud the Department for clarifying in the interim rule that this definition does not require that the actual "act of terrorism" must occur within the boundaries of the United States, its territories or possessions. We believe that Congress intended the protections of the SAFETY Act to attach to the technology wherever deployed, so long as United States interests or citizens are harmed by an act of terrorism. Indeed, the Department itself has recognized the need to push the frontlines of protection for the homeland far beyond the natural borders of the United States by, for example, expanding U.S. Customs inspection responsibilities of sea cargo beyond domestic ports of destination to foreign ports of origin. Clearly, the providers of anti-terror technology supporting this mission are working to prevent harm to persons, property, and entities in the United States, albeit from foreign shores. Should an act of terrorism occur at a foreign port, these providers ought to enjoy the protection of the SAFETY Act.

With respect to the precise types of technologies meriting protection under the SAFETY Act, Section 865(1) of the Act notes that qualified anti-terrorism technologies may include technologies deployed for the purpose of "limiting the harm such acts [of terrorism] might otherwise cause." The "harm" that may be caused by an act of terrorism clearly goes beyond the immediate effects of the act itself. An act of terrorism such as the attacks of September 11th or the October 2001

anthrax attacks triggers a number of immediate remedial and emergency response to limit the resulting harm and deter follow-on attacks. For example, immediately following the detection of anthrax in the offices of Senator Tom Daschle and Senatc Patrick Leahy, Members of Congress and their staffs were treated with antibiotics and other prophylactic measures with the goal of limiting the harm that this act of terrorism could cause. Clearly, any injuries that might have been caused by the administration of these treatments, even though direct results of the act of terrorism itself could be directly traced to the act and the objective of limiting the resulting harm. Moreover, any claims brought as a result of such injuries would clearly be "arising out of, relating to, or resulting from an act of terrorism."

Congress recently acknowledged that technologies designed to limit the harn from an act of terrorism that may result in harm not directly caused by the act of terrorism are protected by the SAFETY Act. In the legislative history of the "Project Bioshield Act of 2002," (H.R. 2122), Congress stated that the Secretary of Homeland Security is "encouraged to designate [biodefense] countermeasures as 'qualified anti-terrorism technologies' as defined in section 862 of the Homeland Security Act." Report by Select Committee on Homeland Security to accompany H.R. 2122, July 8, 2003. Thus, the Department should affirm this Congressional statement that technologies deployed after a terrorist act with the hope of limiting resulting harm may receive designations and/or certification as qualified anti-terrorism technologies in keeping with the clear intentions of the law.

The interim rule correctly points to the intention of Congress that both the protections of the SAFETY Act and indemnification under Public Law 85-804 may, at times, be necessary for a given technology. We also note that 10 U.S.C. § 2354 provides the Department of Defense with the authority to offer indemnification for certain research and development activities. In fact, research and development institutions quite frequently engage in unusually hazardous activities related to th development of anti-terrorism technologies meriting indemnification under Public Law 85-804 and/or 10 U.S.C. § 2454.

We recommend that the Department clarify the occasions when these indemnification authorities will be used to complement the protections afforded by the SAFETY Act. For example, we suggest that Public Law 85-804 should be used on an interim basis for critical technologies that are awaiting designation and/or certification under the SAFETY Act. Otherwise, critical technologies that could protect the American people from terrorist attack or resulting harm may not be deployed solely because of liability concerns. Thus, it is important for the Department to provide further clarification on when indemnification may be appropriate in order to provide Sellers of anti-terrorism technology with the certainty the Department seeks to achieve.

We support the proposed regulations that allow the Department, in determining whether to grant the designation under Section 862, to consider

whether the proposed technology is substantially equivalent to previously designated technologies under the SAFETY Act. We urge the Department to use this concept expansively, where appropriate. For example, we suggest that the proposed regulations permit a class of services (e.g., port security) to be designated as a qualified anti-terrorism technology on the notion that substantially equivalent services that are provided at multiple locations should not be subject to multiple review processes. While the interim rule states that the Department recognizes it has the authority to grant such class designations, it appears that such class designations will not be offered immediately. We see no reason for delaying implementation of class designation as a way to streamline the process, reduce the burden on Sellers, and maximize the opportunity to bring anti-terrorism technologies to as broad a market as possible.

The Chamber appreciates that the Department has taken positive steps to more narrowly define a "substantial modification" as one that significantly reduces safety and effectiveness and its willingness to promptly review notices of modification. The interim regulations state that a "[d]esignation shall terminate automatically, and have no further force or effect, if the designated qualified anti-terrorism technology is significantly changed or modified." Given the seriousness of the loss of such designation, we strongly urge the Department to adopt a reasonable process by which it can assess whether such change has in fact occurred, with relevant input from the Seller. Unless the Department informs the Seller otherwise, the designation should remain in force, including for any changes made to the technology. Only upon a showing and a determination by the Department that there has been a significant change or modification will the Secretary be able affirmatively to terminate the designation and such termination should only take effect upon written notice to the Seller.

The interim rule requires the Secretary to establish "confidentiality protocols" with regard to the maintenance and use of information submitted to the Department by Sellers seeking designation and certification of their anti-terrorism technology under the SAFETY Act. Obviously, the information submitted to the agency will necessarily contain very sensitive confidential and proprietary commercial and technical information, including trade secrets. In addition, confidentiality is necessary to protect the information submitted from falling into the hands of potential terrorists. Moreover, such information may be sought by potential competitors to gain a competitive advantage or by the plaintiff's bar in lieu of, or as a supplement to, discovery in a tort action. Again, based upon initial indications from the Department regarding the application process, the Department appears ready to require Sellers to submit detailed financial information that goes well beyond what is required by any other government agencies. Without assurances of confidentiality, the need to supply this information alone will likely deter Sellers of qualified anti-terrorism technology from applying for SAFETY Act protections.

Finally, we are also somewhat concerned that the case law on the Freedom of Information Act ("FOIA") differentiates voluntary disclosures of information by contractors from statutorily mandated disclosures to the Federal government, and is more protective of disclosures that were not volitional. As such, applicants for designation and/or certification may be presumed to have voluntarily submitted their trade secret information and this submittal may be subject to a greater presumption toward release, even under 5 U.S.C. § 552(b)(4). Therefore, we recommend that the Department seek a specific FOIA exemption to be created for applications submitted under the SAFETY Act.

The Chamber appreciates the opportunity to offer testimony on this very important statute. Achieving the objectives of certainty and flexibility in implementing the SAFETY Act are of the utmost importance to ensuring homeland and national security. Again, we applaud your efforts, and the efforts of the Department, and look forward to full and immediate implementation of the Act.

I am happy to respond to any questions you may have.

Chairman TOM DAVIS. Let me ask each of you: Do you have suggestions for DHS to expedite the review process so that it is responsive to the need to deploy antiterrorist technologies?

Mr. MILLER. I think the first suggestion is prioritization, and we go back to work with DHS, but certainly some things they should look to are procurements that are actively under way; that would be one priority. They should look to prioritize applications related to procurement already under way.

The second principle they could look to for prioritization would be technologies that they've advanced as being priorities, and that's what Science and Technology does to some extent. They list out there for public consumption or, if not appropriate, for internal consumption, the types of technologies they believe are priorities. So if, as we expect, they get a flood of applications, we think it's going to be absolutely necessary that they come up with some way of prioritizing these applications; otherwise, some of the key technologies may fall into the bottom of the pile and not get designations early enough in meeting the needs of the American people so many will incorporate.

Another area that we touched on is the clarity of the regulations themselves. The process is going to be driven, by and large, by the degree the parties understand what the philosophy and interpretations of the Department are going to be and how it's going to work in critical areas, particularly when it comes to services and discrete products. That in itself will drive timelines for the application process and the discussions back and forth and trying to figure it all out.

Mr. CLERICI. Mr. Chairman, I think the proof is in the pudding how they interpret the responses to their application. If Dr. Albright's testimony of 100 hours is to be correct in the preparation, then hopefully DHS will not drill down to the extent that Congressman Carter mentioned and get these applications approved. The framework is there for them to do it expeditiously. It's just a question of whether they are going to be willing to do so.

Mr. MILLER. I don't mean to be cute, Mr. Chairman, but if they shorten the application, they shorten the review process, too.

Chairman TOM DAVIS. Absolutely. When we passed the bill, it was a matter of some urgency. The American people said it in the election. And the longer the bureaucratic process—and ultimately I can give my opinion, DHS can give their opinion—ultimately, the result is going to be the companies coming in and offering their services or their products—or not if they're deterred from doing it. That's why what industry thinks is far more important than what happens ordinarily, because if we can't get these products in the government marketplace, we are not going to be able to make use of the newest technologies.

We have a vote on. I am going to try to get our questions in, because we have about five votes, and let you all go. So I'm going to move quickly to Mr. Bell.

Mr. BELL. Thank you very much, Mr. Chairman.

Mr. Miller, I was fascinated by your testimony regarding the application process. The thousand hours, how do you calculate that?

Mr. MILLER. We did it informally, an unscientific poll with many of our member companies by e-mail, and we asked them the esti-

mates that they would fill out the application, based on the various drafts that are floating around even before they were published, and we got ranges. The lowest range we got was about 500 hours. We got some that estimated it would be 1,500, and we just averaged it out as 1,000 hours. This was based on asking government contractors who are used to filling out these kinds of applications.

What they particularly found daunting, Mr. Bell, was the incredibly extensive financial information, much of it extremely confidential and sensitive. But we don't really feel it's necessary for DHS to make the kind of judgments they need to make as to whether or not this technology does or does not have a place in the marketplace. We think we understand what DHS is trying to achieve. They're trying to understand whether this technology would otherwise go in the marketplace if they did not get the designation by DHS. We understand that, but the kind of information they requested would take a brilliant econometrician months to analyze, and it seems to me to be too academic an exercise.

Dr. Albright, to his credit, during his presentation to this committee, gave a couple simple rules of thumb. Why are they deployed already? Is there insurance in the marketplace? Those should be simple questions DHS should ask, not an incredible amount of financial information and then make some kind of a guess about whether this product will actually show in the marketplace in the absence of this designation.

Mr. BELL. Well, certainly the individuals who came up with an application that would take 1,000 hours would be up for some kind of bureaucratic award or high honor, I would think. It's an extraordinary accomplishment.

Chairman TOM DAVIS. The lawyers love it, don't they?

Mr. MILLER. That's why we poll our members and not our lawyer members.

Mr. BELL. What else can be changed about it, if any of the others would like to weigh in on this? The financial information, but what else would you recommend?

Mr. MILLER. From what we can tell, the scientific information we are requesting seems to be reasonable. I don't think our company would have objections to that, because obviously that's the information on which the Science and Technology Director is going to make his decisions. Most that we objected to was incredibly detailed and, as we saw it, basically irrelevant financial information.

Mr. SOLOWAY. I would also add that, in the area of protecting proprietary data and trade secrets, although I think the Department's intentions are correct there's a very unclear process as to how you get the protections you need; and as you can imagine, in the technology industry, that is something in terms of a company's capital. And so a clear process in the applications and in the regulations for getting that adequate protection is critical.

Mr. CLERICI. Congressman Bell, I think much of the information that's requested, safety and efficacy data, whether you've got the proper amount of insurance with the market, is something a responsible corporation has to do for its shareholders every day. The Department should rely, particularly with respect to public companies, on what is being done internally to mitigate risks, rather than trying to invent a separate scheme that is somehow codified in the

regulations. The parameters of the statute are quite clear, and you can round these bases not easily, but with a little bit of thought, in gathering the information that is usually already at the disposal of the company.

Mr. MILLER. This is the application, so just to give you some idea.

Chairman TOM DAVIS. We will put the application in the record.

Mr. MILLER. It's the form and the background material; 40-some pages, I believe.

[The information referred to follows:]

Department of Homeland Security
SAFETY Act Application Kit

October 2003

Registration
Pre-Application
Application for Designation as Qualified Anti-Terrorism Technology
Application for Certification as an Approved Product for Homeland Security

FOREWORD

We are pleased to release the October 2003 version of the *Department of Homeland Security SAFETY Act Application Kit*. The kit provides you with all of the necessary guidelines for developing and submitting an Application for a Designation or a Certification under the SAFETY Act.

As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the SAFETY Act to provide "risk management" and "litigation management" protections for Sellers of qualified anti-terrorism technologies and others in the supply and distribution chain. The aim of the Act is to encourage the development and deployment of anti-terrorism technologies that will substantially enhance the protection of the nation. Specifically, the SAFETY 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. It also confers other benefits. Although there are many technologies that are important to protecting our homeland, the SAFETY Act "Designation" and "Certification" are designed to support effective technologies aimed at preventing, detecting, identifying, or deterring acts of terrorism, or limiting the harm that such acts might otherwise cause, and which also meet other prescribed criteria.

If you are a Seller of a potential anti-terrorism technology and wish to be awarded SAFETY Act protections, you must formally apply to the Department using the forms provided by DHS, furnish all of the requisite supporting data and information, and successfully demonstrate compliance with the Act's specific criteria. DHS will perform a comprehensive evaluation to determine your eligibility for SAFETY Act Designation or Certification. The information required in the Application is necessary for the Department to implement this critical program.

Our entire process for making available, receiving, handling, and assessing SAFETY Act Applications is completely new. We encourage and welcome feedback that will improve our procedures and enhance our ability to conduct timely and thorough evaluations of Applications.

Dr. Holly A. Dockery
Director, SAFETY Act Office
Science and Technology Division
Department of Homeland Security

PAPERWORK REDUCTION ACT

OMB Number: 1640-0001

Expiration: March 31, 2004

Public reporting burden for this collection of information is estimated to average 36 – 180 hours per response (average = 108 hours per response), including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. This is required to obtain or retain a benefit as required by Public Law 107-296 Subtitle G of Title VIII of the Homeland Security Act of 2002.

The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies (ATTs) by creating a system of "risk management" and a system of "litigation management." The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or Sellers of ATTs from developing and commercializing technologies that could significantly reduce the risks or mitigate the effects of large-scale terrorist events. Without these protections, important technologies are not being deployed to counter harm resulting from a terrorist attack.

Send questions regarding any aspect of this collection of information to the Office of Science and Technology, U.S. Department of Homeland Security, 245 Murray Lane, Building 410, Washington, DC 20528 and to the Office of Management and Budget, Paperwork Reduction Project (1640-0001), Washington, D.C. 20503.

Persons are not required to respond to this collection of information unless it displays a currently valid OMB number.

TABLE OF CONTENTS

I. DESCRIPTION OF SAFETY ACT AND APPLICATION PROCESS 1

A. BACKGROUND 1

1. What is the purpose of the SAFETY Act? 1
2. What technology is covered under the SAFETY Act? 1
3. What protections does the SAFETY Act provide for the Sellers of ATTs? 2
4. How do I apply? 2
5. How does the evaluation process work? 3
6. What does a Designation include? 5
7. What does a Certification include? 5

B. SPECIFIC APPLICATION STEPS & TIMELINES 6

1. How do I obtain an Application Kit? 6
2. How do I fill out the SAFETY Act Application? 6
3. When and how do I submit my Application? 7
4. How long will it take for DHS to evaluate my Application? 8

II. COMPLETING SAFETY ACT APPLICATIONS – GENERAL INSTRUCTIONS 9

A. BEFORE STARTING 9
B. COMPLETING FORMS 9
C. SAVING COMPLETED FORMS 9

III. COMPLETING SAFETY ACT APPLICATIONS – ITEM-BY-ITEM INSTRUCTIONS ... 11

A. REGISTRATION 11
B. PRE-APPLICATION 12
C. DESIGNATION 18
D. CERTIFICATION 24
E. APPLICANT ACKOWLEDGMENTS 25

IV. APPLICATION FORMS 27

A. REGISTRATION 29
B. PRE-APPLICATION 30
C. DESIGNATION 35
D. CERTIFICATION 35
E. APPLICANT ACKOWLEDGMENTS 35

APPENDIX – PUBLIC LAW 107-296 "HOMELAND SECURITY ACT OF 2002" 39

I. DESCRIPTION OF SAFETY ACT AND APPLICATION PROCESS

This SAFETY Act Application Kit facilitates the Department of Homeland Security's (DHS') implementation of Subtitle G of Title VIII of the Homeland Security Act of 2002 – the Support Anti-terrorism by Fostering Effective Technologies Act ("SAFETY Act"; see Appendix A at the back of the Kit). The Kit presents the process by which a wide range of anti-terrorism technologies (ATTs) may apply to DHS for:

1. ***Designation*** as a Qualified Anti-Terrorism Technology (QATT), and/or
2. ***Certification*** as an Approved Product for Homeland Security.

Section A of this Chapter generally documents the SAFETY Act and DHS' implementation program. The *Regulations to Support Anti-Terrorism by Fostering Effective Technologies Act)*, 6 CFR Part 25 will be used to implement the SAFETY Act, once the Rule becomes final. At that time, the text of the Rule will be available at www.dhs.gov, from the U.S Government Printing Office (www.gpoaccess.gov), or at Federal Depository Libraries around the nation. Section A also introduces the concept of a **Pre-Application, a timely method for Applicants to receive DHS feedback and guidance prior to compiling all of the detailed supporting information required as part of a full Application for Designation and Certification**.

Section B describes the specific steps that comprise the Application process, and outlines the DHS timelines associated with the evaluation of and response to an Application.

A. BACKGROUND

1. What is the purpose of the SAFETY Act?

As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted several liability protections for providers of ATTs. The SAFETY Act provides incentives for the development and deployment of ATTs by creating a system of "risk management" and a system of "'litigation management." The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or Sellers of ATTs from developing and commercializing technologies that could significantly reduce the risks or mitigate the effects of large-scale terrorist events. The Act thus creates certain liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified ATTs have been deployed. The Act does not limit liability for harms caused by ATTs when no act of terrorism has occurred.

2. What technology is covered under the SAFETY Act?

The protections of the SAFETY Act can be extended by DHS to any qualifying product, equipment, service (including support services), device, or technology (including information technology) that is designed, developed, modified, or procured for the specific purpose of detecting, identifying, preventing, or deterring acts of terrorism, or limiting the harm that such acts might otherwise cause. This broad definition of "technology" encompasses tangible products, software, services and various forms of intellectual property.

3. What protections does the SAFETY Act provide for the Sellers of ATTs?

SAFETY Act protections available to Sellers of qualified ATTs include the following risk and litigation management provisions:

1. Exclusive jurisdiction in federal court for suits against the Sellers of "qualified anti-terrorism technologies" (Sec. 863(a)(2));
2. A limitation on the liability of Sellers of qualified ATTs to an amount of liability insurance coverage specified for each individual technology, provided that Sellers will not be required to obtain any more liability insurance coverage than is reasonably available "at prices and terms that will not unreasonably distort the sales price" of the technology (Sec. 864(a)(2));
3. A prohibition on joint and several liability for non-economic damages, so that Sellers can only be liable for that percentage of non-economic damages proportionate to their responsibility for the harm (Sec. 863(b)(2));
4. A complete bar on punitive damages and prejudgment interest (Sec. 863(b)(1));
5. A reduction of plaintiffs' recovery by amounts that plaintiffs received from "collateral sources", such as insurance benefits or other government benefits (Sec. 863(c)); and
6. A rebuttable presumption that the Seller is entitled to the "government contractor defense" (GCD) (Sec. 863(d)).

The first five provisions are conferred to Sellers of QATTs, whereas the last provision is conferred additionally to Sellers of technologies that have received a GCD Certification. A Certification can be applied for in conjunction with or subsequent to an Application for QATT Designation, as explained below.

4. How do I apply?

Sellers of ATTs must apply formally to DHS to receive SAFETY Act protections. (Application forms are given in Chapter IV.) All of these protections, with the exception of the GCD, would be conferred upon an Applicant (i.e., Seller) if DHS determines, after a comprehensive review of the Application, that the Applicant's ATT is a QATT. In this case, DHS will issue a Designation for the ATT to the Applicant. In order to be eligible for the GCD, DHS must conduct an additional level of review of the ATT. If the ATT successfully passes this review, DHS will issue a Certification of the Applicant's ATT as an Approved Product for Homeland Defense. Applicants may apply for a Designation and a Certification either simultaneously or in sequence. However, obtaining a Designation is prerequisite to obtaining a Certification.

The full Designation and Certification Applications ask Applicants to assemble and document detailed supporting information and evidence, which may involve an investment of substantial time and effort. To promote overall efficiency in this process, as an alternative to submitting a complete Application, ***Applicants are encouraged, but not required,*** to consider first submitting a condensed **Pre-Application form**. The Pre-Application form is designed to provide several benefits to the Applicant:

- Feedback from DHS will assist the Applicant in determining what to address and emphasize in a full Application.
- Feedback from DHS may identify potential limitations and shortfalls in the existing supporting data and evidence early in the process, which might prompt additional studies or testing.
- In some cases, the Pre-Application may serve to alert DHS to potentially important technologies that may warrant further attention.

Applicants are strongly encouraged to consider first submitting a separate Pre-Application form. The contents of the Pre-Application form are included wholly within the full Designation and Certification Applications. Consequently, the Pre-Application form questions will be required to be addressed by the Applicant regardless of whether an initial separate Pre-Application form is submitted or not. The only difference is whether the Applicant wishes to take advantage of the early DHS feedback provided by the Pre-Application process in order to guide the Applicant in generating and documenting the detailed supporting data and information required by the full Application. Applicants may, without prejudice, change their Pre-Application responses when submitting the full Application, or Applicants may, upon further reflection, resubmit a Pre-Application form with updated information.

Prior to deciding whether to submit an Pre-Application, potential Applicants are strongly encouraged to read the entirety of the Application forms and accompanying Instructions to familiarize themselves with the scope and requirements of a full formal Application and to aid them in deciding whether or not to submit a Pre-Application.

5. How does the evaluation process work?

Pre-Applications are reviewed expeditiously to provide informative feedback designed to facilitate future submissions. Applications for Designation and/or Certification are evaluated with respect to the statutory criteria prescribed by the SAFETY Act.

Although a Pre-Application does not constitute an official Application, DHS will review Pre-Application submissions and, within a nominal period of 21 days, provide explicit feedback to the Applicant, including, but not necessarily limited to:

1. Summary comments on the prospective significance of the ATT to homeland security.
2. Specific comments on the responses to selected questions indicating which are either highly valued areas of interest to DHS and may warrant emphasis and scrutiny in subsequent formal Applications; or which responses might disqualify an Application for Designation or Certification unless the issue is more adequately addressed by the Applicant.
3. An overall rating of the ATT's prospects for attaining Designation and/or Certification, in terms of three levels: *promising*, *doubtful*, or *uncertain*.

DHS response to the Pre-Application is not binding on DHS with respect to other or future Applications. The three levels of DHS ratings for Pre-applications can be interpreted as follows:

Promising: This is an ATT that appears to have the potential to satisfy the criteria for a Designation (and additional conditions for a Certification).

Doubtful: This is an ATT that apparently fails or is likely to fail to satisfy the criteria for a Designation (and additional conditions for a Certification).

Uncertain: This is an ATT that, based on the information available from the Pre-Application, cannot be readily categorized as either *Promising* or *Doubtful.*

The Application forms for Designation and/or Certification ask Applicants for detailed documentation that will be reviewed and studied by DHS to evaluate technologies with respect to the statutory criteria prescribed by the SAFETY Act and implemented through the Rule. To complement the sets of data and analyses provided as part of Application submissions, DHS may consult with the Applicants or pertinent subject matter experts in order to clarify evaluation issues and to solicit specific supplementary information. An iterative process of review, dialogue, and additional requests will be used; however, contact with the Applicant is at the sole discretion of DHS. All individuals involved in the processing and evaluation of Applications, including DHS personnel, supporting administrative contractors, and government and non-government evaluators, will be bound by appropriate nondisclosure and conflict of interest agreements.

In determining whether to grant a Designation, DHS will evaluate a proposed ATT using the following criteria:

(1) Prior U.S. Government use or demonstrated substantial utility and effectiveness.
(2) Availability of the ATT for immediate deployment in public and private settings.
(3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such ATT.
(4) Substantial likelihood that such ATT will not be deployed unless protections under the system of risk management provided under the SAFETY Act are extended.
(5) Magnitude of risk exposure to the public if such ATT is not deployed.
(6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.
(7) ATT that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.
(8) Any other factor that DHS may consider to be relevant to the determination or to the homeland security of the U.S.

In each case, DHS will exercise discretion and judgment in interpreting and weighting these criteria, and in determining their overall significance.

In determining whether an ATT qualifies for a GCD Certification, DHS will conduct a comprehensive review of the design of the ATT and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller will be required to provide safety and hazard analyses, and other relevant data and information regarding the ATT as determined by and requested by DHS.

6. What does a Designation include?

An Application for a Designation will culminate in either an approval or a rejection by DHS. During the review process, DHS may also reach an intermediate determination and notify the applicant that additional specified information from the Applicant is required to complete DHS' evaluation. An approval will contain an appropriate statement of Designation as a QATT, identifying the ATT and prescribing its scope of use, the term of coverage, and the liability insurance requirement. A rejection notice will describe the process the applicant must follow to obtain a detailed debriefing on the reasons for the rejection. A rejection by DHS is not subject to review, except at the discretion of DHS.

Sellers receiving a Designation must submit detailed information describing their insurance coverage as required by the terms of that Designation, and must demonstrate on an annual basis that the required insurance has been maintained. See Section 25.4 of the Rule for more details on the obligations of a Seller of a QATT.

A Designation will be valid for a prescribed period of time, varying between five to eight years, and will possibly include additional conditions explicitly imposed by DHS. Examples of potential limitations and restrictions include, but are not limited to:

- Authorized scope of applicability of the ATT, which may include the threats, targets, and other conditions of operation;
- Methods of monitoring effectiveness and responsibilities to ensure the appropriate level of effectiveness of the deployed QATT;
- Identification of critical dependencies on other technologies or capabilities in the operational environment for the QATT to be effective;
- Life cycle requirements, including but not limited to installation, training, operation, maintenance, updating, removal, or replacement the QATT;
- Critical operational specifications describing essential functions and how they will be employed in the operational setting; and
- Technical performance requirements specific to the QATT.

Sales of QATTs that are consummated during the term of the Designation will continue to benefit from SAFETY Act protections even after the expiration of the Designation. After the third anniversary of issuance of the Designation, the Seller may apply for renewal of the Designation beyond the original term. Details governing the transfer of a Designation, the extension of a Designation to licensees, and the termination of a Designation resulting from substantial modification of the QATT are described in Section 25.5 of the Rule.

7. What does a GCD Certification include?

An Application for a GCD Certification will culminate in either an approval or a rejection by DHS. During the review process, DHS may also reach an intermediate determination and notify the applicant that additional specified information from the Applicant is required to complete DHS' evaluation. An approval will contain an appropriate statement of Certification, identifying the ATT covered and prescribing any limitations or restrictions on the deployment and operation of the ATT. Additionally, the ATT will be placed on an Approved Product List for Homeland Security. A rejection notice will describe the process the applicant must follow to

obtain a detailed debriefing on the reasons for the rejection. A rejection by DHS is not subject to review, except at the discretion of DHS.

The Certification will be valid and effective for the same period of time for which the related Designation is issued, and will expire upon termination of the Designation. The Seller may apply for renewal of the Certification in connection with an Application for renewal of the related Designation. Additional details governing the transfer of Certification and the extension of Certification to licensees are covered in Section 25.7 of the Rule.

B. SPECIFIC APPLICATION STEPS & TIMELINES

There are four fundamental steps that comprise the Application process:

1. Obtain Application Kit,
2. Gather Application information and associated attachments,
3. Complete forms, and
4. Submit forms.

Applicants should note that DHS has an **Applicant Help Desk** to assist in the administrative process of obtaining an Application form, filling it out and submitting it, and to assist with the interpretation of the information requirements prescribed within the Application. Please contact 1-866-788-9318 for assistance. All of Help Desk assistance is *administrative only*; DHS employees cannot advise you on the content or substance of your Application.

1. How do I obtain an Application Kit?

The fastest way to get a copy of the SAFETY Act Application Kit, as well as to apply electronically, is via the dedicated web site at http://www.safetyact.gov. **The DHS web site is configured to accommodate the entire Application process, from Application form acquisition through Application submission**. Electronic Application submissions are encouraged but not required.

Application forms also are available by mail upon request sent to: Department of Homeland Security, ATTN: SAFETY Act, 245 Murray Lane, Building 410, Washington, DC 20528. Mail-in requests must be typewritten in English. Note that, as is the case for all mailings to DHS, mail requests for applications will be subjected to security checks and measures. Mail requests can be made for paper forms or for a CD format (with separate files for each section of the Application Kit). If ten business days have lapsed without a response from DHS, the Applicant should contact the DHS Applicant Help Desk to check on the status of the request.

2. How do I fill out the SAFETY Act Application?

Detailed Instructions for filling out the Application forms are provided in Chapters II and III. Again, the Applicant has the choice of electronic or paper filings; however electronic submissions are strongly encouraged in order to expedite the application process.

DHS has established protections for accepting, processing, evaluating, and reporting on technical, business and insurance data and information that are proprietary or sensitive. All Applications, whether paper or electronic, will be subject to these stringent safeguards. There is

no need for Applicants to be unduly apprehensive and to constrain the scope of the material offered to DHS as part of any Application. Limiting information in your Application may delay evaluation. Neither is there any need to identify and distinguish any specific data elements or segments of materials as being proprietary or sensitive – as everything in the Application will be accorded the same secure handling and treated as if it were proprietary.

Additionally, DHS has established protocols to ensure that the Department will utilize all appropriate exemptions from the Freedom Of Information Act.

Under no circumstances is *U.S. Government classified information* to be entered in or submitted as part of any Application. If the Applicant believes that classified materials are essential to answering an Application question or fully documenting the subject ATT's design, capabilities and demonstrated performance, a completely ***unclassified*** overview description of the information in question should be inserted as an attachment to the Application. If DHS evaluators subsequently concur that classified inputs are needed to support comprehensive assessments, DHS will identify specific classified information requirements and request that the Applicant forward the same to DHS as part of the extended Application review process. The precise means for accommodating the transmission of the classified inputs from the Applicant to DHS will be detailed in the formal request notice that DHS will send to the Applicant. DHS has established appropriate protocols for accepting, processing, evaluating, and reporting on classified material.

3. When and how do I submit my Application?

Application forms may be submitted to DHS either electronically via the dedicated web site http://www.safetyact.gov, or by mail sent to: Department of Homeland Security, ATTN: SAFETY Act, Washington, DC 20528. The web site and the electronic submission procedures can be accessed by Internet Explorer, Netscape, and other common browsers. Any problems or difficulties encountered should be reported to the Help Desk. To be accepted electronically, all attachments must be written in English and must be readable in one of the following formats: .PDF, .RTF, .CSV, .DOC, or .XLS.

Mail-in Applications, either paper or CD-ROM (with attachments adhering to .PDF, .RTF, .CSV, .DOC, or .XLS formats) must be typewritten in English. Again note that, as is the case for all mailings to DHS, mailed submissions will be subjected to security checks and measures. No hand deliveries, facsimile (fax) transmissions, or e-mail submissions will be accepted. Applicants can verify that their Application has been received by DHS, by checking the DHS web site or by contacting the DHS Applicant Help Desk.

All paper Applications will be converted to electronic format by DHS to facilitate subsequent processing, evaluation, tracking, and archiving. A paper copy of the reformatted Application will be forwarded by DHS to the Applicant in order to obtain formal verification that the reformatted Application is complete and accurate. If the Applicant has provided an e-mail address and if e-mail correspondence has been explicitly authorized, an electronic copy will be transmitted in lieu of a paper copy. The Applicant must review the information on the reformatted Application and formally transmit verification or corrections to DHS before the Application will be further processed. Instructions for how to respond with verification or

corrections will be supplied with the reformatted Application. The initial 30-day review for completeness will begin once DHS officially receives verification from the Applicant of correctness of the Application.

The first part of any initial Application for an ATT is the Registration by the Applicant, which must be submitted separately. Prompted by the Registration, DHS will assign to the Applicant a unique Applicant ID. This code is to be utilized by the Applicant in all subsequent Applications, possibly encompassing multiple ATTs.

As a precaution and to support future submissions and correspondences with DHS, the Applicant is encouraged to make and retain an electronic or paper copy of any submission.

4. How long will it take for DHS to evaluate my Application?

DHS will review Pre-Application submissions within a nominal period of 21 days.

DHS will review each Application for completeness and respond to the Applicant within 30 days with either a request for more information (for incomplete applications) or notification that the Application is complete and will be submitted for evaluation. Here and throughout the remainder of this subsection, "Application" refers to either an Application for Designation or an Application for Certification.

During the evaluation process, DHS may request that the Seller provide additional information, may consult with the Applicant and other government agencies or private entities, and may perform various studies. Within 90 days after receipt of a complete Application, the Assistant Secretary for Plans, Programs, and Budget of the Department of Homeland Security Directorate of Science and Technology ("the Assistant Secretary") will recommend to the DHS Under Secretary for Science and Technology ("the Under Secretary") whether the ATT should be approved or rejected for a Designation / Certification. The Assistant Secretary may also report to the Under Secretary that the ATT could potentially receive a Designation / Certification but that more information is needed to complete the evaluation. The Assistant Secretary may, without cause or explanation, extend the review period beyond 90 days upon notice to the Applicant.

Within 30 days after receiving a recommendation from the Assistant Secretary, the Under Secretary will approve or deny the Application, or notify the Seller that the ATT is potentially eligible for a Designation / Certification, but that more information is required to make a decision. The Under Secretary may, without cause or explanation, extend the review period beyond 30 days upon notice to the Applicant. The Under Secretary's decision to accept or reject the Application is final. It is not subject to review, except at the Under Secretary's discretion. Instructions for communications with DHS after your Application is either accepted or rejected will be provided at the time you are informed of the decision.

II. COMPLETING SAFETY ACT APPLICATIONS – GENERAL INSTRUCTIONS

A. BEFORE STARTING

Before initiating the filling out of any Application form, the Applicant is advised to first view the relevant portions of the form, determine in advance which entries will be checked and entered, and assemble all the requisite supporting material – in paper for a paper submission, and in an appropriate electronic form for electronic submission. Additional suggestions supporting electronic submission appear on the web site.

B. COMPLETING FORMS

The following requirements apply to both electronic and paper submissions:

1. Applications must be typed in English.
2. Use Times New Roman font (or comparable easy-to-read font), 12-point minimum.
3. Use normal default line spacing, i.e., a minimum of single space.
4. Adhere to the response and page limits stipulated in Chapter III.
5. Unless otherwise indicated, all requested data fields are mandatory and must be filled in ("N/A" for "not appropriate" or "not available" may be inserted).
6. Define any abbreviations that may be unfamiliar to readers.
7. Use either exclusively English units or exclusively metric / System International units.
8. All monetary values should be expressed in terms of then-year U.S. Dollars.
9. As appropriate and specifically identified, amplifying information should be included as attachments:
    a. Explicitly link each entry in all attachments to its corresponding Section and Item from the Application form.
    b. For any multi-page attachments in response to a single Application form Item:
        i. Use one-inch top, bottom, left, and right margins.
        ii. Number pages sequentially.

Additional requirements that apply to paper-based filings include:

- Use 21.6 x 27.9 cm (8½ x 11 in) paper.
- For the attached material only, print on both sides of the paper.
- If the originals of figures and drawings are in color but black and white copies are being submitted, ensure that the plots are still understandable; lines are identifiable and differentiable, etc.

C. SAVING COMPLETED FORMS

As a precaution and to facilitate future submissions and dialogue with DHS, the Applicant is encouraged to make and retain an electronic or paper copy of any submission.

III. COMPLETING SAFETY ACT APPLICATIONS – ITEM-BY-ITEM INSTRUCTIONS

These Instructions are divided into the five sections of the Application form:

A. REGISTRATION
B. PRE-APPLICATION
C. DESIGNATION
D. CERTIFICATION
E. APPLICANT ACKNOWLEGNENTS.

Here are four important notes to remember:

1. The first step for any Applicant is to fill out and submit a Registration.
2. Upon Registration, DHS will assign a unique Applicant ID to the Applicant, which the Applicant is required to enter in all subsequent Applications.
3. Updated Registrations are required whenever any of the information requested on the Registration form changes.
4. The first step for any Application is to complete Item 1 of the Pre-Application form.

A. REGISTRATION

Item 1. Check exactly one of the boxes in the first line. If this is the initial registration by the Applicant, check the first box and proceed to Items 2 and 3. If the Applicant has been registered previously but some of the relevant information on the Registration form has changed and requires revision, check the second box, enter the Applicant ID previously supplied by DHS, and proceed to enter all of the new or revised information into the appropriate lines in Items 2 and 3. The remainder of the lines, which involve no changes, should be left blank. It is important to update the Registration whenever any of the basic information called for in Section A changes.

Item 2. Item a and Items c – e are mandatory (except for "Line 2" in the Address); the remaining lines may be left blank. If the company has a nine-digit DUNS number, enter it at Item b. If the company does not have a DUNS number, it is unnecessary to obtain one. The Application will not be rejected due to lack of a DUNS number. NAICS Codes can be found in the official 2002 US NAICS Manual *North American Industry Classification System – United States, 2002* (available from the National Technical Information Service, (800) 553-6847 or (703) 605-6000) or directly from http://www.census.gov/. Include area codes and non-U.S. country codes with all telephone numbers.

Item 3. This information pertains to the initial principal Point Of Contact (POC). It is understood that, in support of the comprehensive DHS evaluation process, additional lines of communication may need to be established with other Seller representatives. Note that the items requested here ask only for office or business contact information, i.e., no personal or home contact information is being sought. Lines a – c are mandatory (except for "Line 2" in the Address); and the remaining lines may be left blank. Enter Name as Last, First, Middle Initial. Include area codes and non-U.S. country codes with all telephone numbers. If an e-mail address is provided in Line e, it is mandatory to check exactly one of the two boxes in Line f. Check the "Yes" box only if subsequent e-mail exchanges between DHS and Seller representatives are authorized to facilitate administrative communications and to reduce processing timelines.

Note: Once the Registration has been submitted and the acknowledgment and the Applicant ID from DHS have been received (this should be no more a few minutes for electronic submissions), the Applicant may proceed with the Application. All Applications must begin with Item 1 in Section B. Depending on the type of Application that is specified, the Applicant will be directed to particular portions of the Application form. A unique Application Number will be generated by DHS and reported to the Applicant. Past versions of any Application can be retrieved readily from the dedicated web site, and easily modified and re-submitted.

B. PRE-APPLICATION

Important: Chapter IV Section B, the "Pre-Application Form" must be filled out if you are submitting a Pre-Application only, or if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. Carefully read and adhere to Section B Item 1.b in the Instructions below.

This section is partitioned into groupings of Items associated first with a description and characterization of the subject ATT, and then with the specific SAFETY Act Evaluation Criteria prescribed within the Act and the Rule.

Item 1.a. Enter the Applicant ID (provided by DHS upon submission of the Registration, i.e., Section A). If all of the information from the last submitted Registration form remains valid, check the "Yes" box. If an update is required, stop filling out Section B. Instead, complete and re-submit Section A again, reflecting the changes, and await DHS acknowledgement before proceeding anew with Section B.

Item 1.b. Check exactly one box. Indicate which type of Application is being submitted: Pre-Application, Designation only, simultaneous Designation plus Certification, or Certification only (given previous Designation). If any one of the first three boxes is checked, complete the remainder of Section B and add attachments as indicated in the corresponding Instructions. If the "Designation" box is checked, also add the attachments prescribed in Section C below. If the "Designation + Certification" box is checked, add the attachments prescribed in Sections C and D below. If the last "Certification only" box is checked, provide the associated DHS Designation Number, and check each of the next two boxes if the particular indicated circumstances for the ATT have remained constant since Designation. The Application for Certification will not be processed unless these two boxes are checked or an appropriate explanatory narrative (no more than 5 sentences) is attached. All Applications except the informal Pre-Application require Section E, the Applicant Acknowledgments, to be completed. For electronic submissions, note that previous Applications can be retrieved, edited, and resubmitted.

Item 1.c. **REQUIRED**: As an attachment, provide a brief **completely non-proprietary** overview description of the ATT (no more than 20 lines of text), suitable for screening potential evaluators for conflict of interest. Identify explicitly any other known similar technologies or any other known substantially equivalent technologies – in concept phase, in development, available but not deployed, operationally deployed, DHS Designated / Certified, or other. Identify explicitly any corporate parent, partners, and related business affiliations – both for the company as a whole and for portions dedicated to the ATT.

Note: Items 2 – 5.a identify and characterize fundamental aspects of the ATT – supporting sorting into particular evaluation groupings (including the assignment of specific evaluators) and exploring whether the ATT warrants expedited processing as required by the Act and the Rule (Items 2.c, 2.d and 5.a). The links to similar technologies and any relevant historical usage identify specific sources of information that can facilitate the DHS evaluation process.

Item 2a. Enter the ATT name. Also, as appropriate, enter the ATT make and model descriptions to completely distinguish and identify the subject ATT. Otherwise, the make and/or model lines may be left blank.

Item 2.b. **REQUIRED:** Check "Yes" and, as an attachment, **provide a brief executive summary** (no more than one page) of the ATT describing: nature and characteristics of the technology, relevant threat scenarios (typical as well as a plausible high-loss scenario), demonstrated performance capabilities and limitations, potential safety issues, outline of business plan, and outline of insurance plan. Use the content of the remaining Items in Section B to help fashion this executive summary.

Item 2.c. Check exactly one box. If it is known that the subject ATT is substantially equivalent to another ATT that already has received DHS Designation / Certification, check the "Yes" box, and, if available, provide the corresponding DHS Designation / Certification number (to permit expediting the processing for and evaluation of the subject ATT). Note that a technology may be deemed to be substantially equivalent to a predicate technology if: (1) it has the same intended use as the predicate technology; and (2) it has the same or substantially similar technological characteristics as the predicate technology.

Item 2.d. Check exactly one box. If the ATT is being procured by a federal agency, either at present or anticipated in the near future, check "Yes" and supply the requested information. This will support expediting the processing for and evaluation of the subject ATT. Lines i – iv are mandatory (except "Line 2" in the Address); the remaining lines may be left blank. Enter Name as Last, First, Middle Initial. Include area codes and non-U.S. country codes with all telephone numbers.

Items 3.a & 3.b. Consider the following technological elements:

1. Hardware / equipment	2. Computer software	3. Bio-tech components
4. Personnel / operators	5. Skilled services	6. Mobile platforms
7. Logistics / supplies	8. Embedded intellectual property (including analyses)	
9. Networking	10. Other	11. None

Using the indicated enumeration to represent these elements, select and enter the most significant technological elements (at least one and up to three distinct entries) that comprise the ATT itself (e.g., "1, 2, 6"). Similarly, select and enter the most significant technological elements (up to three distinct entries; if "None" is appropriate enter "11" in the first fill-in box) that are external but essential to the ATT. Consider all interfaces with the ATT, including own company, other companies, public utilities, government, etc.

Item 4.a. Check exactly one box.

Item 4.b. Check all that apply. At least one box must be checked.

Item 4.c. Check all that apply, unless the specific threat information would be classified. In that case, see the discussion in Chapter I, Section B.2 that describes how classified information should be handled.

Item 4.d. From the list of enumerated potential terrorist targets provided below, choose from one to three that best represent the primary targets defended by the ATT (e.g., "P2, I5, V1"). Likewise, choose up to three distinct secondary targets; if "none" is appropriate enter "N" in the first fill-in box. For target type B7, "Non-profit" should be interpreted as "Non-Government, Non-Profit" organizations such as universities, science and technology centers, charities, etc.

People
P1. Crowds / special events
P2. General population dispersed nationwide
P3. General population in localized area
P4. Prominent individuals

Buildings / Facilities
B1. Large urban areas
B2. Nuclear power plants
B3. Airports
B4. Seaports / river & lake ports
B.5 Rail / subway terminals
B6. Warehouses, distribution centers & freight consolidation points
B7. Commercial & non-profit buildings /facilities
B8. Government buildings /facilities
B9. Residences
B10. National monuments / icons

O1. Other

Infrastructure Systems / Capabilities
I1. IT (databases, networks, computer &control systems)
I2. Telecommunications
I3. Defense industrial base
I4. Banking / finance
I5. Transportation (corridors, bridges, tunnels, locks)
I6. Energy (production, storage, distribution)
I7. Chemical / hazardous materials industry
I8. Agriculture / food
I9. Water (production, storage, distribution)
I10. Emergency services
I11. Public health
I12. Border check points (air, sea, road, rail)
I13. Postal/shipping

Vehicles
V1. Aircraft
V2. Ships / boats
V3. Trains
V4. Automobiles / Trucks

Item 5.a. Check all that apply; at least one box must be checked. Here "Non-profit" should be interpreted identically as in the preceding Item 4.d. The fifth category encompasses U.S. carriers at international destinations and along international travel routes.

Note: Item 5.b pertains directly to Evaluation Criterion 1:

- *Prior U.S. Government use or demonstrated substantial utility and effectiveness.*

Item 5.b. Check all that apply. The choices and their interpretations are identical to that described for the preceding Item 5.a.

Note: Item 6 pertains directly to Evaluation Criterion 2:

- *Availability of the ATT for immediate deployment in public and private settings.*

Item 6.a. Consider the following characterizations of the state of a technology's maturity:

1. Employed in military or counter-terrorism missions,
2. Production items available and mature concept of operations established,
3. Production items available,
4. Licensed producer exists,
5. Developmental units available and have passed operational tests,
6. Prototype units available,
7. Manufacturing specifications established, and
8. Conceptual phase.

Select the best characterization of the subject ATT and enter the associated number from above (e.g., "6").

Item 6.b. Check exactly one box. If the third box is checked, enter a projected availability date (month and year).

Item 6.c. Check exactly one box under "Entire", and Check exactly one box under "Limited". Assume that a go-ahead decision has been reached, that all requisite authorizations have been obtained, and that the only issue is how quickly the ATT can be produced, delivered, and deployed.

Note: Items 7 - 10 pertain directly to the inextricably related Evaluation Criteria 3 and 4:

- *Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such ATT, and*
- *Substantial likelihood that such ATT will not be deployed unless protections under the system of risk management provided under the SAFETY Act are extended.*

Item 7.a. If there is no current insurance coverage, check all of the boxes that apply (although logically not both of the first two boxes can be checked). Otherwise, enter all available values and information, using then-year U.S. Dollars for all monetary values. Blanks are permissible. Add attachments as needed to provide values, definitions, and other amplifying information. Limit each individual response (to a specific information query) to no more than two lines of text.

Item 7.b. If there are no additional insurance quotes, check either or both boxes, as appropriate. Otherwise, enter all available values and information, using then-year U.S. Dollars for all monetary values. Blanks are permissible. Add attachments as needed to provide values, definitions, and other amplifying information. Limit each individual response (to a specific information query) to no more than two lines of text.

Item 8.a. If no estimates are available, check the box and proceed to Item 9. Otherwise, proceed to Item 8.b.

Item 8.b. Check all boxes that apply. Blanks are permissible. For any checked box, also add any available dollar estimates or otherwise leave blank, considering separately typical and plausible high-loss scenarios.

Item 9.a. If no estimates are available, check the box and proceed to Item 10. Otherwise, proceed to Items 9.b and 9.c.

Items 9.b & 9.c. In each case, check all that apply. Blanks are permissible. If "Other" is checked, attach a short explanatory text (no more than three lines).
Item 10.a. If no business plan has been developed, check the box and proceed to Item 11. Otherwise, proceed to Items 10.b - 10.e.

Items 10.b & 10.c. If available, for each case estimate the size of the market (expressed in terms of millions of then-year U.S. Dollars) and the percentage share (integer between 0% and 100% inclusive) attributable to the Applicant.

Items 10.d & 10.e. Both Items refer to the timetables provided previously in the responses to Item 6.c. For each Item, check exactly one box. Item 10.d asks whether the business plan is consistent with the timetables presented in the response to Item 6.c. Item 10.e asks for the status of the expertise and resources required to execute those timetables, e.g., already in hand, or planning is underway, or no plans have been initiated.

Note: Items 11 - 13 pertain directly to Evaluation Criterion 5:

- *Magnitude of risk exposure to the public if such ATT is not deployed.*

Items 11.a & 11.b. For each Item, check "None" or all that apply. Here "risk exposure" includes considerations of both likelihood of attack and the impact of attacks.

Item 12.a. For each of the six categories of harm provided below, consider the typical-case terrorist act scenario articulated in response to Item 2.b, and in the top row enter the best estimate of harm from the tabled choices below (e.g., "F3."). If no estimate is available or appropriate, enter "N". There should be six entries, one per category of harm, and at least one should be a non-"N" other than "F0", "I0", "E0", "P0", "M0", or "S0". Proceed similarly for the plausible high-loss terrorist act scenario articulated in response to Item 2.b, and complete the second row.

Fatalities:	**Injuries:**	**Economic Losses (Then-Year U.S. $):**
Chose from: F0. None	Chose from: I0. None	Chose from: E0. None
F1. 1-10	I1. 1-10	E1. $0 to $100 million
F2.10-100	I2. 10-100	E2. $100 million - $10 billion
F3.100 – 1,000	I3. 100 – 1,000	E3. $10 billion - $1 trillion
F4. 1,000 – 10,000	I4. 1,000 – 10,000	E4. Over $1 trillion
F5. 10,000 – 100,000	I5. 10,000 – 100,000	
F6. 100,000 – 1,000,000	I6. 100,000 – 1,000,000	
F7. M ore than 1,000,000	I7. More than 1,000,000	

Physical Damage	**Mass Disruption (attacks on infrastructure or general fear)**	**Symbolic Damage (monuments, icons, cultural treasures or environment**
Chose from: P0: None	Chose from: M0. None	Choose from: S0. None
P1. Car/Truck	M1. Major organization	:S1. Known Locally
P2. Airplane/Ship	M2. Metropolitan area	S2. Known by major elite group
P3. Building	M3. State or region	S3. Known regionally
P4. Complex of structures	M4. All U.S.	S4. Known nationally
P5. Large neighborhood	M5. Global	S5. Known internationally
P6. City		
P7. Agriculture & Infrastructure		
P8. Multi-state region		

Item 12.b. For the same events entered in Item 12.a, indicate the estimated percentage reductions expressed in terms of integers between 0% and 100% (where 100% corresponds to completely reducing the potential harm).

Item 13. Check all that apply. At least one box must be checked.

Note: Items 14 - 20 pertain directly to the inextricably related Evaluation Criteria 6 and 7:

- *Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.*
- *ATT that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.*

Item 14. Check either "None" or all of the following that apply. There must be at least one checked box. Going from left to right, the non-"None" choices of analytical measures respectively denote broad performance statements ("Objectives"), lists of functional performance steps ("Functions"), measures of performance ("Metrics"), and measures augmented by associated quantitative or qualitative performance thresholds ("Metrics & specified criteria").

Item 15. Check either "None" or all of the following that apply. There must be at least one checked box. Here "Red team 'attacks'" denotes planned simulated attacks on the ATT that are unknown to the operators and users of the ATT.

Items 16.a – 16.c. For each row, assume a plausible high-loss event for harm potentially induced by the ATT itself. Then for each of the six damage categories, enter the estimate of harm using the codes provided above for Item 12.a. If no estimate is available or appropriate, enter "N". If there is no expectation of any possible harm attributable to the ATT, all of the entries would be comprised of some combination of "N", "F0", "I0", "E0", "P0", "M0", and "S0".

Items 17.a. Check either "None", or one or both of the following that apply. There must be at least one checked box. If "None" is checked, skip the remaining items and proceed directly to Item 18. If "None" is not checked, complete Items 17.b – 17.e.

Items 17.b –17.e. Check either "None", or all of the following that apply. There must be at least one checked box.

Items 18.a – 18.h. Consider the following hierarchy of potential types of evidence:

7. Operational deployment as an ATT,
6. Other operational deployment,
5. Independent operational tests,
4. Independent tests,
3. Company tests,
2. Independent studies and analyses,
1. Company studies and analyses, and
0. None

For each letter, respond by entering the one or two highest levels of supporting evidence (where "7" is the highest attainable) that apply, with the lower number entered first, e.g., "1 4". If there is only one type of available evidence, enter "0" in the first blank (to the left) and enter the other positive number in the rightmost blank. If there is no available evidence, enter " 0 0 ". For Items 18.c – 18.h, enter " N/A N/A " if the specified aspect of operational performance is inapplicable to the ATT.

Items 19.a – 19.f. For each Item, use the same hierarchy of potential types of evidence as in Item 18, except now exclude Categories 1 and 2 from the potential responses. Likewise, fill in each pair of blanks according to the exact procedures prescribed for Item 18. Note that the threat designations are shorthand representations of the more complete descriptions listed in Item 4.a. of the Pre-Application form.

Items 20.a – 20.d. Proceed as for Items 19.a – 19.f. Note that the asset designations are the target groupings listed in the Instructions for Item 4.d above.

Item 20.e. If additional classes of assets beyond those listed in Items 20.a – 20.d are required, fill in Item 20.e, check "Yes", and add a brief attachment (no more than two lines of text per additional class).

C. DESIGNATION

Important: Responses are required to Items 1 – 14 in this Section C if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. In either case, you must also complete the "Pre-Application Form" in Chapter IV, Section B.

For Items 1 – 10 below, a response will be provided as an attachment. Each response should consist of a short overview narrative, no more than 20 lines of text, followed by a summary-level compilation of appropriate supporting documentation comprised of dedicated sets of text and/or citations to and synapses of available complete reports. Each compilation will be limited to no more than five pages per numbered Item 1, 2, etc. For example, the compilation for all of Items 1.a – 1.f will encompass no more than five pages total. If subsequently deemed necessary, DHS will request complete reports at a later time. Note that responses appearing elsewhere in this Application or in other attachments should be cited only (e.g., "See Section X Item Y.Z") and not repeated verbatim. Instructions for Items 11 – 14 follow separately below. While certain Items below relate explicitly to specific identified criteria, a response to any Item may be used to evaluate any of the evaluation criteria.

1. **Provide a brief description of the technology – including the following items:**
   a. **Mission statement;**
   b. **Deployment history;**
   c. **Key subsystems;**
   d. **Functionality;**
   e. **Underlying scientific principles and unique technology attributes distinguishing the ATT from alternatives that could provide similar anti-terrorism capabilities; and**
   f. **Index of related intellectual property dispositions, i.e., patents, trademarks, copyrights, etc., either in the U.S. or internationally.**
2. **Describe the critical end-to-end steps / events that comprise the operating profile for the ATT, including all key subsystems, interfaces, and complementary systems:**
   a. **Under likely and extreme operating conditions, while countering specific types of actual terrorist attacks.**
   b. **Under likely and extreme operating conditions, in a readiness or standby mode awaiting a potential terrorist attack.**
   c. **Against plausible countermeasure tactics.**
   d. **Summarize the key operating profile differences between Items 3.a – 3.c.**
3. **Describe in detail the envisioned threat scenarios that the ATT is intended to counter. Focus on both typical and plausible high-loss threat scenarios.**
4. **Describe the complete steps and supporting activities required by the buyers and users of the technology to deploy, implement, and operate it as an ATT. Include projected timetables, manpower and training requirements, etc.** *(Relate explicitly to Evaluation Criterion 2 and Section B Item 6.)*
5. **Describe and document the studies and reports supporting your assessments of potential third party liability risks and other potential liability issues associated with the ATT. Focus on both typical and plausible high-loss scenarios.** *(Relate explicitly to Evaluation Criterion 3 and Section B Items 7 - 9. Include considerations of the impact of Quality Control / Quality Assurance programs.)*
6. **Describe and document the studies and reports supporting assessments of the likelihood that your technology would not be deployed as an ATT without the benefits of the SAFETY Act. Include the possible effects of the cost of insurance on the price of the product, and the possible consequences thereof on development, marketing, manufacture, qualification, sale, transportation, use, operation, support, and removal of the ATT.** *(Relate explicitly to Evaluation Criterion 4 and to Section B Items 7 – 10. Include considerations of the impact of Quality Control / Quality Assurance programs.)*
7. **Describe and document the studies and reports supporting assessments of the magnitude of risk exposure to the public, with and without the deployment of the ATT. Focus on both typical and plausible high-loss threat scenarios.** *(Relate explicitly to Evaluation Criterion 5 and Section B Items 11 - 13.)*

8. **Describe and document measures for evaluating the expected operational performance of the technology as an ATT, and the means for monitoring and assessing these measures post-deployment.** *(Relate explicitly to Evaluation Criteria 6 and 7and to Section B Items 14 and 15.)*

9. **Describe and document the scientific studies or other types of corroborative evidence that demonstrate that the technology has substantial utility and effectiveness as an ATT, or that otherwise would support an assessment of the capability of the technology to substantially reduce risks of harm.** *(Relate explicitly to Evaluation Criteria 6 and 7and to Section B Items 16 - 20.)*

10. **Document all known or suspected current hazards and safety issues associated with the ATT – covering the entire life cycle of development, marketing, manufacture, qualification, sale, transportation, use, operation, support, and removal. Summarize all related historical hazard concerns and safety incidents that were encountered in development, testing, and operational use, as well as all remedial actions taken.**

The remaining Items in this section request detailed insurance and financial information, in support of Section C Items 5 and 6. The provided responses will permit DHS evaluators to perform the independent assessments of maximum allowable liability insurance prescribed within the Act and the Rule. Document all responses as attachments – no more than 10 pages for Item 11, and sufficient pages for Items 12 – 14 to present the requested matrices. Note that all monetary values should be expressed in terms of then-year U.S. Dollars.

11. **Provide any risk management plan and risk analyses related to the ATT for the past three years. Enumerate potential liabilities relevant to the ATT and their probability and magnitude. Distinguish between risks related to a terrorist act and those unrelated. Distinguish among potential liabilities for economic damages, punitive damages and other non-economic damages. Focus on both typical and plausible high-loss scenarios.**
    a. **For the past three years, with respect to liability insurance purchased for the business as a whole and for the ATT specifically, or for other technologies, if applicable, provide the following:**
        i. **Name of insurer;**
        ii. **Types of coverage;**
        iii. **Annual premium and estimate:**
            1. **The amount of (or percentage of premium directly attributable to) protection against liability arising out of a terrorist act, and**
            2. **The amount of (or percentage of premium directly attributable to) protection associated with the ATT in an aggregate liability policy;**
        iv. **Amounts of coverage;**
        v. **Relevant terms of coverage;**
        vi. **Dollar limits for products and completed operations;**

vii. **Dollar limits per occurrence and annually, including applicable sub-limits;**

viii. **Any limitations on number of occurrences;**

ix. **Deductibles and/or self-insured retentions;**

x. **Exclusions or other restrictions or limitations on coverage;**

xi. **Whether the coverage includes contractors, subcontractors, suppliers, vendors, customers, or customers' contractors, subcontractors, suppliers, or vendors.**

b. **If applicant self-insures or plans to self-insure, submit all information described in 48 CFR 28.308(a)(1)-(a)(10).**

c. **Describe any unsuccessful attempts to purchase insurance coverage that would be applicable to third-party claims against the ATT.**

d. **Provide any benchmarking information used to arrive at applicant's level of liability insurance coverage or coverage specific to the ATT.**

e. **Provide information on the amount of liability insurance offered on the world market.**

f. **Provide data and history on mass casualty losses in situations comparable to those terrorist acts that the ATT is intended to counter.**

g. **Provide a point of contact (including phone number) that is authorized to discuss the Seller's insurance information.**

Same

12. Financial Information. In an attachment formatted like Table 12 below (a read/write downloadable format provided online at http://www.safetyact.gov), follow the subsequent directions. As appropriate, add more columns (years) or rows (cost/revenue/depreciation/etc. elements) in Table 12 (and for all subsequent tables), providing the complete table on an additional page(s). When using units, carefully define how "units" are measured with a footnote in the Table. Place all required footnotes at the outside base of the Table.

a. In Table 12 provide details of the existing ATT income statement (selling price, cost, and annual production volume) as currently marketed – on either a total cost basis or a per unit cost basis (cross-reference with the information in Section C Item 11 above). The indicated costs must be the costs that are used to measure and record any inventory of this ATT, i.e., exclude allocated central overhead costs such as R&D or headquarters staff that are not dependent on the product or service in question. Sales of this ATT may already be for "commercial" use in addition to government or military sales.

b. Indicate, using footnotes, when standard costs are being utilized and identify the variances from standard when used as a component of "Total technology cost" in the "other" cost category if they are not spread back to material, labor and overhead.

c. If the answer to Q1 in Table 12 is "No" for any year, explain the difference between the costs included in inventory and the costs noted above in a footnote.

d. If the answer to Q2 in Table 12 is "Yes" for any year, explain how the standards were adjusted for variances in a footnote.

e. Indicate the cost and revenue data provided in Table 12 that auditors could not trace in your records and explain how it was estimated in appropriate footnotes.

f. In a separate discussion associated with Table 12, not a footnote, identify the top five customers for this technology by sales dollars and indicate, if the selling price varies by customer, what the current selling price per unit of technology is by customer or explain why this cannot be provided.

Table 12. Technology Cost Data: Historical Costs (Then-Year U.S. Dollars)

Cost and Revenue data for technology as *currently marketed*			
	Indicate □ total costs or □ unit costs		
	2003E	**2002**	**2001**
Sales revenues – net	$		
Technology Costs:			
Direct Materials (Raw Material and Purchased Parts)	$		
Direct Labor	$		
Overhead (Describe cost components included))	$		
Other (describe cost components included)	$		
Total technology costs	$		
Gross Profit (Sales Revenue – Total Tech. Cost)	$		
Please break out the total technology costs above into variable and fixed costs:			
Variable *total technology costs* if known	$		
Fixed *total technology costs* if known	$		
Units of Production			
Units of Sales			
Q1. Is inventory cost made up of the costs above? Yes or No	□Y □N	□Y□N	□Y□N
Q2. Standard costs used? Yes or No	□Y □N	□Y□N	□Y□N
Q3. Indicate the % of commercial sales each year, if any.			

TOOK OUT OVERHEAD / DEPRECIATION TABLE

13. Prospective Data. In an attachment formatted like Tables 13-1 through 13-2 below (a read/write downloadable format provided online http://www.safetyact.gov), provide prospective data for the candidate ATT, on the same basis and comparable to the data in Table 12. If forecasts are available for different volumes of sales at different market prices, use column 2004ML to represent the most likely forecast, 2004H to be the highest volume (lowest price) forecast, and 2004L to be the lowest volume (highest price) forecast – all assuming that the ATT is approved under the SAFETY Act. Cross-reference with the information in Section C Item 11. If there is a risk premium for possible lawsuits in conjunction with the sale of this product built

in to its price in Table 13-1, indicate that value. If estimates exist for years beyond 2006, please add columns to Table 13-1 to show those estimates.

Line up the revenue and costs between the latest year in Table 12 and the first year in Table 13-1, and explain any variance in an attachment formatted like Table 13-2. With the exception of the risk premium associated with the new application of this ATT, the revenues, costs and profits of the ATT are expected to change on the basis of the traditional cost-volume-profit framework. To the extent that this traditional framework does not apply, explain in a footnote associated with Table 13-2. Describe the nature and cause of any changes in the costs or revenues between Tables 12 and Table 13-1 that are **not** related to pricing of additional risk (if any). These changes should be associated with the expanded application of this ATT to commercial customers (or to additional commercial customers if some commercial customers already exist).

Table 13-1. Technology Cost Data: Prospective Cost (Then-Year U.S. Dollars)

Cost and Revenue data for technology if certified as anti-terrorism device					
	Indicate total costs or unit costs				
	2004ML	**2004H**	**2004L**	**2005**	**2006**
Sales revenues – net					
Technology Costs:	$				
Direct Materials (Raw Material and Purchased Parts)	$				
Direct Labor	$				
Overhead (Describe cost components included)	$				
Other (describe cost components included)	$				
Total technology costs	$				
Gross Profit (Sales Revenue – Total Tech. Cost)	$				
Please break out the total technology costs above into variable and fixed costs:					
Variable *total technology costs* if known	$				
Fixed *total technology costs* if known	$				
Units of Production					
Units of Sales					

Table 13-2. Changes in Revenues and Costs (Then-Year U.S. Dollars)

Component	Explanation of Variance -Table 12 vs. Table 13-1		
	2003E	2004ML	Explanation of Change
Revenue	$		
Cost			
Direct Material	$		
Direct Labor	$		
Overhead	$		
Other	$		

DELETED "CAPITAL BUDGET" QUESTION / BUT SOME REMAINS

14. Product Related Spending. In an attachment (a read/write downloadable format is provided online at http://www.safetyact.gov), provide the capital and project-related spending (e.g. tooling, equipment, engineering, etc) required to deploy the anti-terrorism technology. Include spending already paid as well as estimates for future expenses. Break up the expense, in then-year US Dollars, into the years in which it was paid.

DELETED "CORPORATE FINANCIAL STATEMENTS" TABLE. EASIEST TO OBTAIN.

D. CERTIFICATION

Important: Responses are required to Items 1 – 3 in this Section D if you are applying simultaneously for Designation and Certification, or if you are applying for Certification only. In the former case, you must also complete the "Pre-Application Form" in Chapter IV, Section B, and provide the attachments described in Section C of this chapter. In the latter case, complete Item 1 of the "Pre-Application Form;" update, if required, the previous response to Section C Item 10 via an attachment; and comply with the Instructions below.

For every Item below, a response will be provided as an attachment. Each response should consist of a short overview narrative, no more than 20 lines of text, followed by a summary-level compilation of appropriate supporting documentation comprised of dedicated sets of text and/or citations to and synapses of available complete reports. Each compilation will be limited to no more than five pages per numbered Item 1, 2, or 3. For example, the compilation for all of Items 3.a – 3.f will encompass no more than five pages total. If subsequently deemed necessary, DHS will request complete reports at a later time. Note that responses appearing elsewhere in this Application or in other attachments should be cited only (e.g., "See Section X Item Y.Z") and not repeated verbatim.

Each of the Items here relates directly to the evaluation criteria for Certification prescribed in the Act (Sec. 863(d)(2)), *i.e., the ATT performs as intended, conforms to the Seller's specifications, and is safe for use as intended.*

1. **Document and provide all analyses / studies that establish the degree to which the ATT performs as intended:**
   a. **When countering an actual terrorist attack. Consider the spectrum of postulated threat scenarios, including both typical and plausible high-loss cases.**
   b. **When countering a falsely perceived terrorist attack, i.e., false positive.**
   c. **When employed or in standby mode in anticipation of a potential terrorist attack.**
2. **Document and provide all analyses / studies that establish the degree to which the ATT conforms to Seller specifications.**
3. **Document and provide all safety and hazard analyses / studies pertinent to the ATT:**
   a. **When used as intended, while countering an actual terrorist attack.**
   b. **When used as intended, while countering a falsely perceived terrorist attack, i.e., false positive.**
   c. **When used as intended, while employed or in standby mode in anticipation of a potential terrorist attack.**
   d. **When inadvertently used improperly, while countering an actual terrorist attack.**
   e. **When inadvertently used improperly, while countering a falsely perceived terrorist attack, i.e., false positive.**
   f. **When inadvertently used improperly, while employed or in standby mode in anticipation of a potential terrorist attack.**

E. APPLICANT ACKNOWLEDGEMENT

By signing the Application, the Seller's Authorized Representative certifies the Seller's commitment to provide any additional information requested by DHS to process and evaluate the Application. The Authorized Representative also attests to the completeness and accuracy of the Application and subsequent information supplied.

The following language from the Rule applies:

> "Fraud or willful misconduct in the submission of information to the Department in connection with an application under the Act may result not only in rebuttal of the presumed application of the government contractor defense, but may also prompt the Department to refer the matter to the Department of Justice for pursuit of criminal or civil penalties."

IV. APPLICATION FORMS

A. REGISTRATION

Important: Read carefully and comply precisely with the related Instructions in Chapter III, Section A.

1. ☐ INITIAL REGISTRATION ☐ UPDATED REGISTRATION

Assigned "SAFETY Act Applicant ID": _____

2. APPLICANT (i.e., SELLER / COMPANY) INFORMATION

a. NAME _____
b. DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER _____
c. NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM (NAICS) CODE _____
d. ADDRESS: Line 1: _____
Line 2: _____
State / Province: _____ Country: _____ Zip Code / Mail Code: _____
e. TELEPHONE NUMBER _____
f. FACSIMILE NUMBER _____
g. E-MAIL ADDRESS _____
h. WEB SITE URL _____

3. PRINCIPAL POC INFORMATION

a. NAME _____
b. ADDRESS: Line 1: _____
Line 2: _____
State / Province: _____ Country: _____ Zip Code / Mail Code: _____
c. TELEPHONE NUMBER _____
d. FACSIMILE NUMBER _____
e. E-MAIL ADDRESS _____
f. E-mail Communication Authorization: ☐ Yes ☐ No

B. PRE-APPLICATION

Important: This "Pre-Application Form" must be filled out if you are submitting a Pre-Application only, or if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. Carefully read and adhere to Section B Item 1.b in the Instructions presented in Chapter III.

Important: Read carefully and comply precisely with all of the related Instructions in Chapter III, Section B.

---

1. a. APPLICANT ID: _____ REGISTRATION INFO REMAINS VALID? ☐ Yes

b. APPLICATION TYPE

☐ Pre-application
☐ Designation as Qualified Anti-Terrorism Technology
☐ Designation + Certification as an Approved Product for Homeland Security
☐ Certification only; DHS Designation Number _____
  ☐ ATT, specifications, level of effectiveness, and use have not changed since Designation
  ☐ Insurance premium and coverage have not changed since Designation

c. Brief non-proprietary description of ATT is attached? ☐ Yes

---

2. ATT DESCRIPTION

a. NAME _____ **MAKE** _____ **MODEL** _____

b. Brief Executive Summary of ATT is attached? ☐ Yes

c. Similar to another QATT? ☐ No ☐ Yes
DHS Designation/Certification Number _____

d. BEING PROCURED BY A FEDERAL AGENCY? ☐ No ☐ Yes

i. FEDERAL AGENCY _____
ii. POC NAME _____
iii. ADDRESS: Line 1: _____
Line 2: _____
State / Province: _____ Country: _____ Zip Code / Mail Code: _____
iv. TELEPHONE NUMBER _____
v. FACSIMILE NUMBER _____
vi. E-MAIL ADDRESS _____

3. a. What technological elements comprise the ATT? _____ _____ _____

b. What external technological elements are essential? _____ _____ _____

4. a. What is the primary means of terrorist attack that the ATT counters?

☐ Radiation / nuclear ☐ Chemical Warfare ☐ Humans, e.g., suicide bombers
☐ Conventional explosives or incendiary weapons to include improvised explosives
☐ Biological against people, livestock, or agriculture
☐ Cyber / information technology, especially Information Assurance

b. By what means does the ATT defend against terrorism?

☐ Deter terrorism ☐ Detect activity ☐ Identify activity ☐ Interdict before attack
☐ Defeat attack ☐ Reduce effects ☐ Recover following attack ☐ Forensic / investigative

c. What are the most relevant means that terrorists could employ to counter the ATT?

☐ Inspection or familiarity ☐ Trial & error ☐ Insider information or action ☐ None

d. What are the targets of the terrorist attacks that the ATT defends against?

Primary: _____ _____ _____ **Secondary:** _____ _____ _____

5. a. Select all potential users of the technology, as an ATT or otherwise.

☐ Federal Government ☐ State/Local Government ☐ Non-profit ☐ Commercial
☐ International border / air & sea travel ☐ Other

b. Select all current or past users of the technology, as an ATT or otherwise.

☐ Federal Government ☐ State/Local Government ☐ Non-profit ☐ Commercial
☐ International border / air & sea travel ☐ Other ☐ None

6. a. What is the ATT's current state of maturity? _____

b. What is the status of the least mature of any external but essential elements?

☐ Currently widely deployed or available ☐ Limited current deployment or availability
☐ Unavailable, Projected availability date: _____ ☐ No external essential elements

c. How quickly could the ATT, including external elements, be deployed throughout the entire identified market in defense of the U.S.? In a limited few select situations?

Entire:	Limited:
☐ 0 – 4 months	☐ 0 – 4 months
☐ 5 – 12 months	☐ 5 – 12 months
☐ 1 – 2 years	☐ 1 – 2 years
☐ More than 2 years	☐ More than 2 years

7. Characterize any insurance coverage of the Applicant (i.e., Seller) that might apply in the event of a terrorist action where the technology is (or is to be) deployed:

a. Current: ☐ Past coverage, but none presently
☐ No past and no present coverage
☐ Actively seeking but cannot acquire coverage

Insurer: _____ Occurrence & Annual Aggregate Limits: _____
Annual premium: _____ Deductible/Retention: _____ Exclusions: _____

b. Additional Quotes: ☐ None ☐ Actively seeking but cannot acquire quotes

Insurer: _____ Occurrence & Annual Aggregate Limits: _____
Annual premium: _____ Deductible/Retention: _____ Exclusions: _____

8. Characterize any estimates of the potential liability faced by the Applicant (i.e., Seller) if the ATT were to be marketed without SAFETY Act protections.

a. ☐ None available

b. Estimated Liabilities (Then-Year U.S. Dollars):

☐ Economic damages	Typical: $_____	Plausible High-Loss: $_____
☐ Punitive damages	Typical: $_____	Plausible High-Loss: $_____
☐ Other damages	Typical: $_____	Plausible High-Loss: $_____

9. How are any available estimates of the effect of liability limitations on the profitability of the ATT expressed?

a. ☐ None available

b. If the ATT were to be marketed without SAFETY Act protections?

☐ Internal rate of return ☐ Dollar cost per unit sold ☐ Risk-adjusted rate of return ☐ Other

c. If the ATT were to be marketed with SAFETY Act protections?

☐ Internal rate of return ☐ Dollar cost per unit sold ☐ Risk-adjusted rate of return ☐ Other

10. Characterize the business plan elements that have been established for the ATT.

a. ☐ None established

b. Current market: Size (Then-year U.S. $M) $_____M Applicant's share _____%

c. Potential market: Size (Then-year U.S. $M) $_____M Applicant's share _____%

d. Support deployment expectations presented in Item 6.c? ☐ Yes ☐ No

e. Sufficient supporting expertise/resources for expectations presented in Item 6.c?

☐ Existing ☐ Planned ☐ Unplanned

---

11. Indicate the source of any studies that assess, either quantitatively or qualitatively, the magnitude of risk exposure to the public if the technology:

a. Were not to be deployed as an ATT.

☐ None ☐ Own company ☐ Independent insurance or risk analysis organizations

b. Were to be deployed as an ATT.

☐ None ☐ Own company ☐ Independent insurance or risk analysis organizations

12. a. Indicate the estimated potential magnitude of harm to the public if the technology were not deployed as an ATT and there was a terrorist attack.

	Fatalities	Injuries	Economic Losses	Physical Damage	Mass Disruption	Symbolic Damage
Typical Case	_____	_____	_____	_____	_____	_____
High-Loss Case	_____	_____	_____	_____	_____	_____

b. Indicate the percentage decrease in the potential magnitude of harm to the public if the ATT were deployed and there was a terrorist attack.

	Fatalities	Injuries	Economic Losses	Physical Damage	Mass Disruption	Symbolic Damage
Typical Case	_____	_____	_____	_____	_____	_____
High-Loss Case	_____	_____	_____	_____	_____	_____

13. Select the psychological impacts that might well arise from a serious terrorist attack against targets defended by the ATT.

☐ Regional/national drop in economic activity or property values
☐ Regional/national drop in social activity sectors, e.g., enjoying public areas, entertainment events, or travel
☐ Undermining trust in availability or safety of essential infrastructures, social services, or people
☐ Dread of exposure to a severe hazard, e.g., disease or nuclear radiation
☐ Loss of something of irreplaceable symbolic or natural value
☐ Widespread personal fear of potential harm
☐ Other significant psychological impacts on a large segment of society
☐ None

---

14. Indicate the analytical measures that have been established for evaluating the expected operational performance of the ATT.

☐ None ☐ Objectives ☐ Functions ☐ Metrics ☐ Metrics & specific criteria

15. Indicate the means that have been established for monitoring and assessing the performance of the technology after it were to be deployed as an ATT?

☐ None ☐ Periodic inspections ☐ Periodic tests or exercises ☐ Red team 'attacks'
☐ Built-in diagnostics / reporting systems ☐ Analytical or indirect indicators

16. Indicate the estimated potential magnitude of harm to the public that the ATT by itself could be responsible for were it to be employed: (a) in response to a terrorist attack; (b) against a falsely perceived terrorist attack, i.e., false positive; and (c) in a standby or alert mode in anticipation of a potential terrorist attack.

	Fatalities	Injuries	Economic Losses	Physical Damage	Mass Disruption	Symbolic Damage
a.	____	____	____	____	____	____
b.	____	____	____	____	____	____
c.	____	____	____	____	____	____

17. Characterize the scientific studies or other corroborative evidence that demonstrate that the technology has substantial utility and effectiveness as an ATT, or that otherwise would support an assessment of the capability of the technology to substantially reduce risks of harm.

a. Reports of analyses or test results
☐ None ☐ Own company ☐ Independent organizations

b. Addressing utility and effectiveness
☐ None ☐ While countering a terrorist attack ☐ In the absence of a terrorist attack

c. Addressing safety
☐ None ☐ While countering a terrorist attack ☐ In the absence of a terrorist attack

d. Addressing other specific performance metrics

☐ None ☐ Success probability / Expected degree of success
☐ False positive/negative rates ☐ Sensitivity to user error
☐ Reliability ☐ Availability
☐ Maintainability ☐ Robustness
☐ Interoperability ☐ Learning curve and retention
☐ Quality control/assurance ☐ Countermeasures

e. Demonstrating compliance with specific design or performance standards
☐ None ☐ Industry ☐ Government ☐ DHS ☐ Other

18. Characterize the existing evidence that demonstrates that the ATT has substantial utility and effectiveness in specific aspects of operational performance:

a. Mission success in representative operational settings ____ ____

b. System reliability and availability in representative settings ____ ____

c. Safety for operators, support personnel, or other parties ____ ____

d. Maintenance, calibration, fault detection / warning / diagnostics, and general sustainability in operational settings ____ ____

e. Likely countermeasures to be employed by terrorists ____ ____

f. Adequacy of the concept of operations for use as intended ____ ____

g. Ability to upgrade or remove a deployed technology ____ ____

h. Availability and training of operational and support personnel ____ ____

19. Characterize the actual use or testing evidence that demonstrates that the ATT has substantial utility and effectiveness against specific terrorist threats:

a. Radiation / nuclear ____ ____ **b. Chemical** ____ ____

c. Conventional explosives ____ ____ **d. Biological** ____ ____

e. Cyber/Information Technology ____ ____ **f. Human** ____ ____

20. Characterize the actual use or testing evidence that demonstrates that the ATT has substantial utility and effectiveness in defending specific assets:

a. People ____ ____ **b. Infrastructure/Capabilities** ____ ____

c. Buildings/Facilities ____ ____ **d. Vehicles** ____ ____

e. Other ____ ____ **Explanatory attachment added?** ☐ Yes

C. DESIGNATION

Important: This section is pertinent if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. In either case, you must also complete the preceding "Pre-Application Form" in Section B of this chapter.

Add appropriate attachments that are explicitly linked to each of the individual Items 1 – 14 in Section C of Chapter III.

D. CERTIFICATION

Important: This section is pertinent if you are applying simultaneously for Designation and Certification, or if you are applying for Certification only. In the former case, you must also complete the preceding "Pre-Application Form" in Section B of this chapter, and provide the attachments required for Section C of this chapter. In the latter case, complete Item 1 of the "Pre-Application Form;" update, if required, the previous response to Section C Item 10 via an attachment; and comply with the Instructions below.

Add appropriate attachments that are explicitly linked to each of the individual Items 1 – 3 in Section D of Chapter III.

E. APPLICANT ACKNOWLEDGMENTS

Under penalty of perjury, I declare, to the best of my knowledge and belief, that all statements made and information provided in this Application and any accompanying documents are true, correct, and complete.

Prepared By: _____

Title (if applicable): _____

Signature: _____

Date: _____

The signature of the preparer must be notarized below:

APPENDIX – PUBLIC LAW 107-296 "HOMELAND SECURITY ACT OF 2002"

Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002
SEC. 861. SHORT TITLE.
This subtitle may be cited as the "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" or the "SAFETY Act".

SEC. 862. ADMINISTRATION.
(a) IN GENERAL.—The Secretary shall be responsible for the administration of this subtitle.
(b) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES.
—The Secretary may designate anti-terrorism technologies that qualify for protection under the system of risk management set forth in this subtitle in accordance with criteria that shall include, but not be limited to, the following:
(1) Prior United States Government use or demonstrated substantial utility and effectiveness.
(2) Availability of the technology for immediate deployment in public and private settings.
(3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism technology.
(4) Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this subtitle are extended.
(5) Magnitude of risk exposure to the public if such antiterrorism technology is not deployed.
(6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.
(7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.
(c) REGULATIONS.—The Secretary may issue such regulations, after notice and comment in accordance with section 553 of title 5, United States Code, as may be necessary to carry out this subtitle.
SEC. 863. LITIGATION MANAGEMENT.
(a) FEDERAL CAUSE OF ACTION.—
(1) IN GENERAL.—There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism occurred, unless such law is inconsistent with or preempted by Federal law. Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers.
(2) JURISDICTION.—Such appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.
(b) SPECIAL RULES.—In an action brought under this section for damages the following provisions apply:
(1) PUNITIVE DAMAGES.—No punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses may be awarded, nor shall any party be liable for interest prior to the judgment.
(2) NONECONOMIC DAMAGES.—

(A) IN GENERAL.—Noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.
(B) DEFINITION.—For purposes of subparagraph (A), the term ''noneconomic damages'' means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.
(c) COLLATERAL SOURCES.—Any recovery by a plaintiff in an action under this section shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of such acts of terrorism that result or may result in loss to the Seller.
(d) GOVERNMENT CONTRACTOR DEFENSE.—
(1) IN GENERAL.—Should a product liability or other lawsuit be filed for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in paragraphs (2) and (3) of this subsection, have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, there shall be a rebuttable presumption that the government contractor defense applies in such lawsuit. This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary's consideration of such technology under this subsection. This presumption of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.
(2) EXCLUSIVE RESPONSIBILITY.—The Secretary will be exclusively responsible for the review and approval of antiterrorism technology for purposes of establishing a government contractor defense in any product liability lawsuit for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in this paragraph and paragraph (3), have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. Upon the Seller's submission to the Secretary for approval of anti-terrorism technology, the Secretary will conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller will conduct safety and hazard analyses on such technology and will supply the Secretary with all such information.
(3) CERTIFICATE.—For anti-terrorism technology reviewed and approved by the Secretary, the Secretary will issue a certificate of conformance to the Seller and place the antiterrorism technology on an Approved Product List for Homeland Security.
(e) EXCLUSION.—Nothing in this section shall in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that—(1) attempts to commit, knowingly participates in, aids and abets, or commits any act of terrorism, or any criminal act related to or resulting from such act of terrorism; or (2) participates in a conspiracy to commit any such act of terrorism or any such criminal act.

SEC. 864. RISK MANAGEMENT.
(a) IN GENERAL.—
(1) LIABILITY INSURANCE REQUIRED.—Any person or entity that sells or otherwise provides a qualified anti-terrorism technology to Federal and non-Federal Government customers (''Seller'') shall obtain liability insurance of such types and in such amounts as shall be required in accordance with this section and certified by the Secretary to satisfy otherwise compensable third-party claims arising out of,

relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.
(2) MAXIMUM AMOUNT.—For the total claims related to 1 such act of terrorism, the Seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies.
(3) SCOPE OF COVERAGE.—Liability insurance obtained pursuant to this subsection shall, in addition to the Seller, protect the following, to the extent of their potential liability or involvement in the manufacture, qualification, sale, use, or operation of qualified anti-terrorism technologies deployed n defense against or response or recovery from an act of terrorism:
(A) Contractors, subcontractors, suppliers, vendors and customers of the Seller.
(B) Contractors, subcontractors, suppliers, and vendors of the customer.
(4) THIRD PARTY CLAIMS.—Such liability insurance under his section shall provide coverage against third party claims arising out of, relating to, or resulting from the sale or use of anti-terrorism technologies.
(b) RECIPROCAL WAIVER OF CLAIMS.—The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers, involved in the manufacture, sale, use or operation of qualified anti-terrorism technologies, under which each party to the waiver agrees to be responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.
(c) EXTENT OF LIABILITY.—Notwithstanding any other provision of law, liability for all claims against a Seller arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.

SEC. 865. DEFINITIONS.

For purposes of this subtitle, the following definitions apply:
(1) QUALIFIED ANTI-TERRORISM TECHNOLOGY.—For purposes of this subtitle, the term ''qualified anti-terrorism technology'' means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary.
(2) ACT OF TERRORISM.—(A) The term ''act of terrorism'' means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.
(B) REQUIREMENTS.—An act meets the requirements of this subparagraph if the act—
(i) is unlawful;
(ii) causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel) based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and
(iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

(3) INSURANCE CARRIER.—The term ''insurance carrier'' means any corporation, association, society, order, firm, company, mutual, partnership, individual aggregation of individuals, or any other legal entity that provides commercial property and casualty insurance. Such term includes any affiliates of a commercial insurance carrier.

(4) LIABILITY INSURANCE.—

(A) IN GENERAL.—The term ''liability insurance'' means insurance for legal liabilities incurred by the insured resulting from—

(i) loss of or damage to property of others;

(ii) ensuing loss of income or extra expense incurred because of loss of or damage to property of others;

(iii) bodily injury (including) to persons other than the insured or its employees; or

(iv) loss resulting from debt or default of another.

(5) LOSS.—The term ''loss'' means death, bodily injury, or loss of or damage to property, including business interruption loss.

(6) NON-FEDERAL GOVERNMENT CUSTOMERS.—The term ''non-Federal Government customers'' means any customer of a Seller that is not an agency or instrumentality of the United States Government with authority under Public Law 85–804 to provide for indemnification under certain circumstances for third-party claims against its contractors, including but not limited to State and local authorities and commercial entities.

Mr. BELL. What is the normal response?

Mr. MILLER. Well, you're talking about people supplying notebooks of financial and scientific information to back up their application and response. That's why we came up with the estimate of approximately 1,000 hours, which goes to the Congressman's earlier question.

Mr. BELL. On the liability, I will be clear on that from where you all are. Is there a misunderstanding in the industry about the limitations on liability, or is it your suggestion to suggest we go further in limiting the liability?

Mr. MILLER. We didn't respond to this hearing in terms of suggested changes to the legislation. We were just commenting specifically on the regulations.

Mr. BELL. You mention in your testimony that the liability questions are causing a lot of problems.

Mr. MILLER. Oh, just generally because the SAFETY Act has not been implemented. I think I was trying to make the point, Mr. Bell, maybe not eloquently, that exactly as Chairman Davis said, I've rarely had an occurrence where CEOs and member companies call me at night because a regulation was published.

But I can tell you that, looking back to March 2002 when one of the first requests for proposal came out that had this self-insurance requirement, I literally had CEOs finding me at home at night saying, "ITAA has to make this their No. 1 priority; we cannot bid in good conscience on these Department of Homeland Security contracts, when we're literally betting the company." And these were company CEOs of, in some cases, multibillion-dollar companies. That's how negative the initial reaction was and why the legislation that was enacted was so important and how the implementation of it was critically important.

Mr. SOLOWAY. Let me just second Harris' comments, that we've had dozens of company executives talking to us about this issue, even before the passage of the legislation. It's not a question of the extension or extent of liability. It's a question of how you can obtain appropriate protection and the interplay between this act, Public Law 85–804 for extraordinary relief, and the different tools that are available to make sure the government can get what it needs and provides the protections. So it's really a question of bringing it together in a clear way, and I think there is a lot of work to do in that area.

Mr. CLERICI. And I can say in my personal experience in the past few years, there has been an entire division of a company depending on whether risk mitigation could be accomplished. In one instance, the division suffered because the SAFETY Act was not in place and those jobs were lost; in the next one, hopefully we'll have the SAFETY Act up and running.

Mr. BELL. Thanks a lot.

Thanks, Mr. Chairman.

Chairman TOM DAVIS. Mr. Schrock.

Mr. SCHROCK. I'll be very brief because we have six votes, and we're not professors, so you're not required to stay in class past 20 minutes.

Mr. Miller, you talked about Isabel. I represent Virginia Beach and Norfolk where there's massive amounts of military, maybe 125

ships in a massive commercial port. What a perfect opportunity for the terrorists to get in there, and to get in here too.

You talked about protecting the IT companies. Is it a "hold harmless" agreement? We used to have people sign "hold harmless" things, so that if something happened to them the Navy couldn't be held accountable. Is that an answer to this? The lawyers wouldn't like it; and the chairman is right, he is one, so he knows what he talks about. Is that an answer?

Mr. MILLER. Industry is not saying there should not be liability whatsoever. There is an industry that will offer certain-level protections.

The world has changed since September 11. As Mr. Soloway pointed out in his testimony, the idea between the Congress and the government saying to government contractors, "In extreme situations when insurance is not available in the marketplace, we are going to offer you some protections," is not new. It goes back almost 50 years, Mr. Schrock, in the Department of Defense. It's used in the nuclear industry; it's used in the space launch industry. It was used at the time of development of Cipro in order to respond to the anthrax scare in this country. Those were situations where they said, "We can't deal with this situation. There were no actuarial tables that gave us the ability to insure, so that's why the SAFETY Act is so critical.

Not to say that the companies have zero liability, not to say they should be able to commit fraud, but in these extreme situations, if they don't have some limitation of liability, particularly when DHS reviews and approves their technology and services as Mr. Soloway pointed out, that's the only way to get these products to the public and ultimately to protect the American people.

Chairman TOM DAVIS. There's got to be some limit somewhere, some reasonable limits.

Mr. SCHROCK. It seems like there's a real disconnect between what the three of you say and what our previous person who testified said. It's like you're worlds apart. Have you all sat down with the DHS? You all have done that?

Mr. MILLER. We've had extensive discussions with DHS, collectively and independently. I think each of us, independently and collectively. In fact, ITAA and PSC worked very closely together on comments on the rule and so forth, so we've worked very closely with the Department and actually think the Department has made significant progress here. We don't want to be overly negative.

What we're concerned about is, if there's a perception that the job is now completed and executed and we've got significant hurdles to overcome in bringing these products and services to the market, there are some realities that have to be addressed, issues of clarity, as I said earlier; and I don't want to harp on it again.

There is a vast difference in buying a product or device and buying an evolving service which could be developed over time and constantly upgraded. A lot of discussion around the rule seems to focus more on the presumption of product than a service, and there are big differences that have to be overcome.

Chairman TOM DAVIS. We want to make the vote and I don't want to keep you. We will be probably close to an hour over there voting.

I want to allow you to supplement over the next 5 days, anything you want to add on this. We've had other questions, but we've been obviously in constant dialog. I appreciate your being here, and I hope that the Department understands this continues to be an ongoing discussion, that the interim regulations are really not where we need to be.

At the end of this—I think you've articulated this—at the end of the day, the question is, "are we getting the products in or aren't we?" And there are still a lot of concerns, but I appreciate your being here and I'm going to adjourn the meeting. Thank you.

[Whereupon, at 11:30 a.m., the committee was adjourned.]

[The prepared statement of Hon. Elijah E. Cummings and additional information submitted for the hearing record follows:]

Statement of Congressman Elijah E. Cummings
Government Reform Hearing
On
"Implementing the SAFETY Act: Advancing New Technologies for Homeland Security"
October 17, 2003 at 10:00 a.m.

Thank you, Mr. Chairman for holding this important hearing.

The "Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002," which was included as part of the Homeland Security Act of 2002, was established in an effort to promote the development of anti-terrorism technologies and services, by extending liability protections to the providers of Qualified Anti-Terrorism Technologies (QATTs). The Department of Homeland Security published proposed regulations to implement the SAFETY Act on July 11, and just yesterday issued an interim rule, effective immediately, stating that although it will continue to consider the rule, it believes that the rule is in the public's best interest, as it will encourage the development and distribution of anti-terrorism technologies.

Because the SAFETY Act extends several protections to the providers of QATTs (Qualified Anti-Terrorism Technologies), we must be very detailed

and not hasty in our understanding of the implications this ruling has, not only for the sellers of these technologies, but also for the purchasers and citizens. This rule will in effect limit legal liability for personal injury and other lawsuits, while failing to provide an alternate form of compensation or safeguards for the general public. The need for qualified anti-terrorism technologies is no doubt pressing. As we consider the safety of the United States and its citizens, and as we move forward in our effort to secure this country from acts of terrorism, we must very carefully consider the rights and protections our citizens deserve. By hastily taking away or capping injury compensation in an effort to quickly qualify anti-terrorism technologies, we are doing an injustice to our citizens.

This hearing today is timely, because it will help to shed light on several pressing issues surrounding the SAFETY Act (Support Anti-Terrorism by Fostering Effective Technologies Act of 2002). Because the Department of Homeland Security is continuing to consider this issue and may issue new regulations in the future, it is my hope that this discussion today will lead to further clarification and modification of the rule in an effort to improve it for both the providers of QATTs (Qualified Anti-Terrorism Technologies) and the citizens these technologies will protect.

Again, thank you for holding today's hearing. I look forward to hearing from Today's witnesses as we discuss the current implementation of the SAFETY Act and its impact on both the sellers and the purchasers of Qualified Anti-Terrorism Technologies.

August 11, 2003

Docket Management Facility
U.S. Department of Transportation
400 Seventh Street, S.W.
Washington, DC 20590-0001

Re: Comments on DHS Draft Rules Implementing SAFETY Act
Docket No. USCG-2003-15425

Dear Sir or Madam:

This is to provide comments on the referenced draft regulations on behalf of the undersigned associations.

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 400 corporate members throughout the U.S., and a global network of 50 countries' IT associations. The Association plays the leading role in issues of IT industry concern including information security, homeland security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA also serves as the IT sector coordinator for IT-ISAC. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields.

The Professional Services Council (PSC) is the leading national trade association representing professional and technical services companies doing

business with the federal government. PSC's approximately 155 member companies perform billions in contracts annually with the federal government, from information technology to high-end consulting, engineering, scientific, and environmental and remediation services. Many of PSC's members also provide homeland security and national security services to the federal government.

The Aerospace Industries Association (AIA) represents the nation's major manufacturers of commercial, military, and business aircraft, helicopters, aircraft engines, missiles, spacecraft, material, ground- and sea-based military hardware, and related components and equipment. Together, AIA's membership represent every facet of the aerospace industry and deliver highly complex systems to the federal government.

The National Association of Manufacturers (NAM) is the nation's largest industrial trade association. The NAM represents 14,000 members (including 10,000 small and medium companies) and 350 member associations serving manufacturers and employees in every industrial sector and all 50 states. Headquartered in Washington, D.C., the NAM has 10 additional offices across the country.

Several of these associations will be submitting their own comments in addition to the joint comments in this letter.

I. Introduction

The signatory associations strongly support the Department's general approach in the proposed regulations and believe the proposed regulations will achieve many of the goals of the SAFETY Act. In particular, we are pleased that the proposed procedures reflect the statutory distinction between products and services that are designated as qualified anti-terrorism technologies and those technologies that are further certified as Approved Products for Homeland Security. The statute expressly provides that the Secretary's consideration of the two levels of protection will involve different criteria and different kinds of review. Although we recognize, and strongly urge, that the two reviews can and frequently will take place concurrently, we believe that by establishing separate procedures for Designation and Certification the Department can expeditiously designate important anti-terrorism technologies as qualified anti-terrorism technology ("QATT"), without any delay that might attend the more extensive design review required for Section 863(d) ("government contractor defense") immunity.

We are also pleased that the Department has interpreted the statute to provide for a single federal cause of action, and that such action may only be brought against the Seller of the QATT. These principles are critical to effective QATT protection. It is also critical that the regulations expressly provide that the protections of the statute apply in perpetuity to QATTs covered by the Designation.

We also appreciate the Department's candid and open request for constructive suggestions about such difficult and important issues as the method by which the Secretary will evaluate what level of insurance will "unreasonably distort" prices and the manner in which the Department will assure that trade secrets and other confidential information will be fully protected during the review process.

We emphasize, however, that the proposed regulations do not address in detail two critically important issues: (1) the form or content of applications for Designation or Certification; and (2) guidance and procedures for the Designation and Certification of anti-terrorism technologies consisting in whole or in part of services.

With regard to the first issue, in some respects our comments are, by necessity, somewhat hypothetical in nature because the proposed regulations do not include any details about the form or content of the applications for Designation or Certification. We encourage DHS to be as open and receptive to comments on the proposed application form and related instructions as it has been to date in the rulemaking process.

With regard to the second issue, sales of services (or sales that include services) to prevent and respond to terrorist attacks are likely to be the subject of the majority of all applications for Designation and Certification, in part because, as a practical matter, virtually all anti-terrorism devices will be of little or no use unless there are people who can install, operate, maintain, and repair those devices, as well as people who can design and implement the complex systems necessary to deploy many anti-terrorism solutions. For reasons that are described more fully below, we believe that the review and approval process for Designation and Certification of anti-terrorism technology must be sufficiently flexible to address the special characteristics of services offerings. We also believe that Sellers and others involved in the development of QATT would greatly benefit from more extensive guidance on this subject.

We hope that these comments are helpful to the Department as it proceeds with the rulemaking process. We fully support the Department's issuance of

interim final regulations as soon as possible to get the QATT program started while the Department further elaborates and refines the regulations in certain areas.

II. Executive Summary

Our comments below address a wide range of issues organized under the following topics: Designation of qualified anti-terrorism technology ("QATT"); Certification of a QATT as an Approved Product for Homeland Security; additional regulatory guidance for qualification of services; the single federal cause of action; insurance; post-designation and certification changes; relationship of SAFETY Act procedures to ongoing procurements; protection of confidential information; definitions; the relationship of the SAFETY Act to indemnification under Public Law 85-804; and administrative review.

Although we urge DHS to give careful consideration to all of the comments discussed below, we believe that several of our recommendations are of critical importance to successful implementation of the SAFETY Act.

First, the proposed regulations impose an across-the-board term of five to eight years on all Designations of QATT. We believe that an automatic expiration of every Designation, regardless of the circumstances, will tend to discourage the development of anti-terrorism technology and needlessly increase costs for both Sellers and the Department. We recommend that the proposed regulations be amended to presume that Designations will apply for an indefinite period. If the Department determines that some term is necessary, the period should be extended to 10 years at a minimum.

Second, the proposed regulations provide that Designation of a technology as QATT and Certification of a QATT will be effective beginning on the date of issuance. We believe that the regulations should provide for the Designation and/or Certification, once granted, to take effect retroactively to the earlier of the date of deployment or date of the sale. The regulations should also state that, once Designation and/or Certification is granted, the liability protections of the Act will apply even if the facts of a particular claim are alleged to have occurred prior to the effective date of Designation and/or Certification. By providing protection to a Seller who elects to make its technology immediately available to the public pending the DHS approval process, retroactive Designation and Certification would encourage the deployment of a QATT at the earliest possible date. At a minimum, the Designation and Certification should be effective as of the date of the application.

Third, the proposed rules contemplate a 150-day period for the Designation process, which, in light of the urgent needs that exist today, could complicate the rapid implementation of QATT. More importantly, however, it is critical that the regulations provide for an expedited approval process for the review of technologies already in use or substantially equivalent to existing QATTs, changes and modifications to existing QATTs, technologies that are the subject of pending procurements for the protection of high-risk targets or critical infrastructure, technologies for which the cost of insurance coverage has significantly changed, and in other appropriate circumstances.

Fourth, although the statutory immunity provided by the SAFETY Act is modeled after the judicially-created doctrine of the government contractor defense, it is significantly different from, and much broader than, that doctrine. We therefore recommend that both the implementing text and the preamble of the final regulations state that the government contractor defense affords complete immunity from all claims in lawsuits subject to the SAFETY Act.

Fifth, anti-terrorism services are as critical to security as anti-terrorism devices, and, given the wide variations in complexity of such services, are likely to require much more flexibility in the regulatory review process. The regulations should clearly provide that Designations of qualified anti-terrorism technologies are sufficiently broad to include all elements of the component products *and* services, including systems design and customer-approved changes and related services, such as operations, maintenance, integration, and training.

Sixth, the regulations should provide that the Designation and Certification of QATT will not automatically terminate upon the cancellation or reduction of insurance coverage through no fault of the Seller.

Seventh, the procedure for reviewing changes in a technology designated a QATT should not deter Sellers from making improvements. The regulations should expressly provide that a change or modification to a QATT will be considered "significant" only if the change *materially* affects the function or operation of the QATT. The regulations and the Designation should identify the kinds of changes that would require re-designation or re-certification. The regulations should also provide for the Secretary to grant retroactive approval as of the date of the modification or application for modification.

Eighth, the regulations should encourage close consultation between DHS and federal, state, and local procuring agencies, and provide for SAFETY Act review to be performed in parallel with a procuring agency's evaluation process, to the maximum extent possible. The regulations should also encourage agencies to allow

the submission of bids or proposals for which the price or other terms are conditioned in some way upon QATT Designation or Certification. Education and guidance to procuring agencies and other customers of QATT should be one of the Department's most important goals.

Ninth, the regulations should include detailed procedures, similar to those provisions in the Federal Acquisition Regulation governing bid and proposal information and source selection information, to assure the confidentiality of proprietary commercial and technical information submitted by Sellers in the Designation and Certification approval process. The regulations should also require DHS to provide advance notification to the submitter when considering whether to disclose SAFETY Act information to third parties.

Tenth, the proposed regulations provide that the Under Secretary's Designation and Certification decisions are final and not subject to review. In light of the variety and sophistication of the technologies submitted to DHS, we believe that there is a real risk that significant features may be overlooked or misunderstood during the initial review and evaluation process. Accordingly, we recommend that the regulations provide for an administrative procedure in which an applicant may seek review of a decision by the Under Secretary to deny an application for Designation or Certification.

III. Discussion

A. Designation of a Qualified Anti-Terrorism Technology ("QATT")

1. Term of Designation

Proposed Section 25.5(f) provides that, although the protections conferred by a Designation extend indefinitely to all sales of the QATT made during the term of the Designation, the Designation itself will have a term of only five to eight years, to commence on the date of issuance.

The purpose of the SAFETY Act is to assure that potential manufacturers and sellers of anti-terrorism technologies are not deterred from providing QATT because of the threat of potential liability. This purpose can be achieved only if sales once made are forever subject to the statutory protections. We interpret Section 25.5(f) to provide such permanent protection, and agree that this should be stated explicitly.

In light of what we view as the intent of the SAFETY Act, we are concerned that the regulations propose that every Designation should expire automatically at some fixed date in the future regardless of the circumstances. The statute itself does not provide for a fixed Designation term. Because the proposed regulations do not explain the Department's rationale for establishing a mandatory expiration date, it is difficult to weigh the pros and cons of such a requirement. In our view, rather than furthering the purpose of the statute, the five-to-eight-year term provision would tend to discourage the innovative and rapid development of improved, and more cost-efficient, anti-terrorism technologies because the Seller will know that a Designation, even if granted, will be effective for only a limited period of time. An automatic expiration would also increase costs for contractors, by building into their business plans the need to apply for renewal every 5-8 years regardless of any changes in the QATT or other circumstances, and for the Government, by guaranteeing that DHS will have to process renewal applications even where there have been no changes in the technology or other relevant circumstances. Finally, the automatic expiration provision unnecessarily restricts the Department's flexibility "to address the specific circumstances of each particular request for SAFETY Act coverage," contrary to the stated purpose of the regulations. *See* 68 Fed. Reg. 41420 (July 11, 2003).

Accordingly, we recommend that any interim or final regulations be amended to presume that a Designation applies indefinitely in the absence of unique circumstances presented by a particular technology. Changes in the technology or in the insurance situation can and should be addressed through requirements for new submissions to DHS, as has generally been proposed, rather than through an automatic expiration of the Designation.

In the alternative, if DHS determines that some term must be established in advance for all QATT Designations, we strongly recommend that the period be extended to a minimum of ten years, a period that is more consistent with the effective dates of long-term services agreements and more realistically reflects the length of time necessary to develop and implement complex systems and services. In addition, if the Designation is to have a fixed term, the regulations should clarify that the Designation (and Certification if one exists) continues in effect for all deliveries of products or services made pursuant to contracts entered into during the term of the Designation, including all option periods if those options are exercised. Renewal of a QATT Designation should be automatic upon request, or based on a limited and expedited review to confirm that the original Designation remains valid. If DHS adopts this alternative, the regulations should also provide that the same criteria will be used for making the renewal determination as for the original Designation, and that the renewal period will be for a period at least as

long as the original period. Regardless of the sunset date of Designation and/or Certification, sales made during the effective period are covered in perpetuity.

2. Effective Date of the Designation

Proposed Section 25.5(f) provides that a Designation will be effective beginning on the date of issuance. We recommend that this provision be modified so that Designation will be effective retroactively to the earlier of the date of deployment or date of the sale, and, in appropriate circumstances, should apply to technology that is substantially the same but was deployed or sold prior to the Seller's application.[1] Although many Sellers will choose to await QATT Designation, and perhaps Certification as well, before offering their anti-terrorism technology, this change would provide protection to Sellers and their customers who, eager to fulfill urgent needs and anticipating Designation, elect to make technology immediately available to the public pending Designation and/or Certification. Failure to adopt a retroactive effective date would discourage the deployment of a QATT at the earliest possible date and could cause such technologies to be unavailable for a pending procurement. The availability of retroactive Designation would also help to address the competitive imbalance that arises in favor of a Seller whose specific technology happens to be designated as QATT first, a potentially critically important issue.

Retroactive Designation could also be appropriate to protect Sellers in the event that a technology, *e.g.,* a vaccine, was originally used for routine protection against disease purposes but is now used for protection against terrorist acts, or in circumstances in which technology has been resold and is now used for anti-terrorism purposes not contemplated by the Seller.

Because in many instances the need for and the extent of retroactive Designation will vary depending upon the particular circumstances, we recommend that the effective date be specified in the Designation document rather than prescribed in the regulations. We also recommend that the regulations clarify that,

---

[1] At an absolute minimum, the Designation should be effective retroactive to the date the Seller's application is filed with DHS. This principle of retroactive effectiveness to the earlier of the date of the sale or date of the deployment should also apply to the Certification of a QATT once that determination has been made by DHS. The applicant can ask for a date certain and supply information on the importance of that date.

once effective, Designation and/or Certification will apply even if the facts of particular claims are alleged to have occurred prior to the effective date of Designation or Certification.

3. Timeframe for Designation Process

The proposed rules contemplate a 150-day period for the Designation process, from the date of application to issuance, with allowance for DHS to extend this period in its discretion. *See* Section 25.5(a)-(e). As a threshold matter, we believe that in most circumstances a 150-day processing period impedes the goal of deploying QATT as quickly as possible. We recommend that, at a minimum, the regulations provide that the 30-day notification period will run concurrently with the period for review by the Assistant Secretary.

Even more important, however, the regulations should explicitly provide for an expedited approval process in appropriate circumstances. Expedited procedures would be appropriate, and often essential, for review of the following:

- Technologies that are already in use and therefore have an established record of safety and effectiveness;
- Technologies that build upon, improve, or maintain already designated QATTs;
- Technologies that are substantially equivalent to existing QATTs;
- Changes/modifications to existing QATTs;
- Technologies that are the subject of pending procurements by an agency with "frontline" anti-terrorism responsibility or in other urgent circumstances, such as to acquire technologies to protect known high-risk targets or critical infrastructure;
- Technologies for which the procuring agency has already completed its assessment of the technology's safety and effectiveness;
- Technologies for which the level or cost of available insurance coverage has significantly changed; and
- Renewal applications if such applications are required.

There are certain to be other situations that would warrant expedited review in addition to these examples, and we believe it is critical for the regulations to be flexible while providing for such a procedure.

4. "Multi-Use" Technologies and Services

As defined in the statute and regulations, a technology may be considered a QATT if it is "designed, developed, modified, or procured for the *specific* purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause . . . ." (Emphasis added.) Certain types of technologies, however, such as security systems and services, will have broad application to protect against a wide range of criminal activity in addition to terrorist acts. In order to clarify this situation, and consistent with the expressed purpose of covering a broad range of technology, the regulations should make clear that so long as customers may procure such technology for the identified purposes regarding acts of terrorism, such technology may be designated as a QATT and certified as subject to the Section 863(d) immunity.

5. Use of Standards

Proposed Section 25.3(c) permits the Under Secretary to issue safety and effectiveness standards for categories of anti-terrorism technologies and consider compliance with those standards in determining whether to grant a Designation. The notice of proposed rulemaking specifically asks for comments on how the Department can best develop standards and implement the SAFETY Act provisions to provide the appropriate market and industry incentives for the development and deployment of anti-terrorism technologies.

Although we agree that the Under Secretary clearly has the authority to establish procedures that would make the review and processing of QATT more effective and efficient, we distinguish "development" of new standards by the Department from "identification" of existing standards created by private sector Standards Organizations, the compliance with which may help to speed a determination of whether to grant a Designation.

Identification of applicable existing standards, as well as new standards that are established in the future, may simplify and shorten the approval process. For example, the fact that a technology meets an established standard may supplement or substitute for examination of scientific studies or extended DHS reviews of the technology's effectiveness. The Department could begin by adopting some of the basic standards that already exist in the commercial world, such as professional

engineering standards for certain products and professional licensing standards for the performance of certain services.

Standard-setting, however, should be independent of Designation and Certification, and should not delay Designation or Certification, or divert DHS resources from the review process. We are also concerned that standards could, unintentionally, chill innovation or inhibit creativity. Because many applications will involve highly advanced, cutting-edge technology, identifying important standards necessarily will be an ongoing process reflecting advancements in and experience with that technology, and use of standards as a "filter" for QATT Designation may involve a serious risk of unintended adverse consequences.

Moreover, because many of the products and services that will be deployed as QATT will be either substantial adaptations or modifications of existing technology, or designed anew for QATT purposes, it is crucial that potentially applicable standards not be set arbitrarily without meaningful input from the contracting community. For example, it is unclear whether and how compliance with standards would be applied to existing technology, and whether it is even practical to identify standards for many types of services. If DHS decides to identify or develop standards to help make the Designation or Certification processes more efficient, the process should require prior consultation with scientific and industry representatives, and standards should be identified only after being subject to the normal administrative notice and comment rulemaking procedures.

Regardless of whether DHS eventually identifies or develops standards in the future that could be useful in helping to determine qualification, the regulations governing Designation as QATT should expressly permit and encourage the submission of safety and other test information developed by the applicant as part of the qualification process. Such a provision would be consistent with similar language in proposed Section 25.6, which requires the Seller to "provide safety and hazard analyses and other relevant data and information regarding such technology," and which permits the Under Secretary to "consider test results produced by an independent laboratory or other person or entity engaged by the Seller" when deciding whether to certify qualified technology as an Approved Product for Homeland Security.

6. Multiple Sellers

Development of complex systems integration technologies frequently involves several different Sellers of multiple component products and services. The regulations should be sufficiently flexible so that in such circumstances DHS could

Designate and Certify the entire system, for which the prime contractor would be considered the Seller, or, in the alternative, issue multiple Designations and Certifications to multiple Sellers of the components of that system.

7. Other Clarifying Regulatory Changes

Proposed Section 25.3 (a) includes in the definition of QATT products or services designed for the purpose of "limiting the harm such acts might otherwise cause." We believe that this term is sufficiently broad to include much of the emergency response equipment currently in use or available to first responders. Accordingly, we recommend that this subsection include criteria to identify the types of products or services that may be designated as a QATT, *e.g.,* language such as "designed, developed, modified, adapted, produced, or procured to limit, mitigate, and/or reduce the effects of a terrorist event." The regulations might also provide a nonexclusive list of examples, such as search and rescue equipment, communication services and equipment, services related to the operation of critical infrastructure, and systems integration services.

Proposed Section 25.4 (e) requires the Seller to enter into a reciprocal waiver of claims with its contractors and subcontractors, suppliers, vendors, and customers, and contractors and subcontractors of the customers, for losses including those "resulting from an activity resulting from an act of terrorism when a QATT has been deployed in defense against, response to or recovery from such act." Sellers clearly will have an incentive to negotiate such reciprocal waivers. Nevertheless, because such waivers are not standard industry practice, we believe that the regulations need to address those circumstances in which a Seller is unable to convince one or more of its subcontractors or vendors to execute such a waiver. We recommend that this section be amended to provide that Sellers are required to use commercially reasonable efforts to negotiate such reciprocal waivers, but that failure to achieve a reciprocal waiver will neither preclude the granting of a Designation or Certification nor terminate a Designation or Certification once issued.

B. Certification of QATT As An Approved Product for Homeland Security

Proposed Sections 25.6 and 25.7 address the proposed procedures for the Secretary to certify that a technology designated as QATT is also an Approved Product for Homeland Security presumptively entitled to the immunity from liabilities provided by Section 863(d) of the SAFETY Act. The preamble to the proposed regulations also includes several additional important interpretations of

the immunity available under the Act that we believe should be included in the regulations in the appropriate fashion.

1. Scope of the "Government Contractor Defense"

In addition to the liability limitations provided to Sellers of QATTs receiving a Designation based on the criteria set forth in Section 862(b) of the Act and Section 25.3(b) of the proposed regulations, the SAFETY Act also provides immunity for Sellers from liability for claims brought in a "product liability or other lawsuit" "arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies . . . have been deployed" if the QATT receiving the Designation has also been evaluated and certified as an Approved Product for Homeland Security based on the factors set forth in Section 863(d) of the Act and Section 25.6 of the proposed regulations.

While the statutory immunity provided by the Act is modeled after the judicially-created doctrine of the government contractor defense, it is significantly different from, and much broader than, that doctrine. For example, the preamble to the proposed regulations properly recognizes that the SAFETY Act immunity would apply to defeat a "failure to warn" case given the broad statutory definition of the lawsuits subject to the immunity as quoted above (*see* 68 Fed. Reg. at 41422). In addition, one of the basic predicates for the judicially-created government contractor defense, government-defined specifications, is replaced in the SAFETY Act by the Seller's own specifications; and the limitation to sales to the Federal government under the judicial doctrine is replaced in the SAFETY Act by coverage for *all* sales, including sales to State and local governments and commercial customers as well as sales to the Federal government. We therefore recommend that both the text and the preamble of the final regulations focus on these statutory provisions and highlight the limited significance of the government contractor defense doctrine as based in common law to the interpretation or application of the SAFETY Act.[2] The substance of the statement in the preamble that "[t]his express statutory framework thus governs in lieu of the requirements developed in the case law for

---

[2] In particular, the final rule and any accompanying preamble should clarify that the statement in the proposed preamble that Congress incorporated the *Boyle* line of cases as it existed rather than incorporating future judicial developments was not intended to restrict the plain meaning or scope of the broad immunity provisions of the SAFETY Act as available in product liability and other lawsuits.

application of the government contractor defense" (68 Fed. Reg. at 41422) should be incorporated into the final regulations.

2. Other Recommended Regulatory Changes

To minimize potential confusion and uncertainty, we recommend that the regulations be further amended in several ways to clarify the nature and scope of the Section 863(d) immunity.

First, the regulations should state clearly that immunity under the SAFETY Act relieves Sellers of any potential liability arising out of design defects, manufacturing defects, failure to warn, and all other lawsuits arising or resulting from, or relating to an act of terrorism where a QATT that has received a Certification has been deployed.

Second, the regulations should state clearly that (1) the presumption of immunity can be rebutted only if the Under Secretary determines that there is clear and convincing evidence of fraud or willful misconduct in submitting information in connection with the review process; and (2) evidence of negligence in the performance of safety and hazard tests would not be sufficient to rebut the presumption. This is consistent with the preamble to the proposed rule, which acknowledges that, under § 863(d)(1) of the SAFETY Act, the presumption of the statutory immunity can be rebutted *only* by a showing that the "Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary's consideration of such technology." 68 Fed. Reg. at 41422.

Third, the text of the regulations should include specific language applying the protection of SAFETY Act immunity to those "who sell to state and local governments and to the private sector." This is consistent with the language in the preamble, which recognizes that the SAFETY Act makes the statutory immunity available not only to federal government contractors, "but also to those who sell to state and local governments and the private sector." *See* Act § 863(d)(1); 68 Fed. Reg. at 41422. Thus, the SAFETY Act's statutory Certification grant provides much broader immunity than the judicially-created government contractor defense.

Finally, the rebuttable presumption should apply even if the technology is misused or is not used for the intended purpose identified in the Certification process. Once the sale of a product is complete, the Seller has very little control over how it is used. If the purchaser fails to follow the Seller's operating instructions or uses the product for a purpose for which it was not designed and

loss or damage results from an act of terrorism, the rebuttable presumption should still be applicable to the Seller. We believe that the Congress intended such broad application of the Act and the broad application of the statutory government contractor defense.

C. Additional Regulatory Guidance for Qualification of Services

The Act and the proposed regulations provide that services as well as products will qualify for the SAFETY Act protections, reflecting the fact that anti-terrorism services are as critical to security as anti-terrorism devices. The regulations should make clear that Designations of qualified anti-terrorism technologies are sufficiently broad to include all elements of the products and services that form a part of the technologies, as well as solutions that combine them. The regulations should also clearly state that Designations should be broad enough to include customer-approved changes and related services, such as operations, maintenance, integration, and training. The regulations should provide detailed guidance regarding the Designation and Certification of services in a manner that allows interactive dialogue with the applicants.

There are a number of ways in which the regulations could specifically address Designation and Certification of anti-terrorism technology consisting wholly of services or comprising a hybrid of services and products. First, the regulations should provide that a services offering may be designated as a QATT and certified as an Approved Product/Service for Homeland Security. Sales of such services would be subject to the protections of the SAFETY Act without the need to re-apply if the Seller will provide only minimal customization of the services for a particular buyer.

Second, although some proposals for services contracts may provide definite specifications that will allow at least Designation at, or shortly after, the time of the selection of the winning proposal and award of the contract, many professional services are not provided according to "specifications" that are determined in advance. For anti-terrorism initiatives that require sophisticated information technology, a "systems integrator" or "solutions provider" is likely to provide key services to implement the overall anti-terrorism system. For complex information technology systems, the design of the system is often one of the tasks performed under the contract. The proposed regulations, however, appear to contemplate that specifications will be determined before the Seller begins work under the contract. It is important that the regulations provide for QATT protection when systems design is part of the required contract performance. In the absence of such protection, Sellers may be unwilling to proceed.

The special issues for service contractors in this context can be illustrated by a real-life example. The Department of Homeland Security has announced plans to contract for the U.S. Visitor and Immigrant Status Indication Technology (U.S. VISIT) system. Although the specific capabilities and functionalities of the system have not been fully determined, the goal is to improve the entry-exit process for non-U.S. citizens passing through U.S. borders. The contractor will be providing a multi-faceted "system," which is likely to require a combination of products and services.

The products would include, for example, items such as biometric devices and scanners. These products would be designed and manufactured to particular specifications that can be reviewed and independently approved for Designation and Certification as QATT. The services, however, would include a variety of activities, including data integration, database management, and training. The services would be provided, in part, in accordance with the device provider's requirements or design document or the operating procedures of the repairer or trainer. The requirements document can be independently validated before implementation, although often not before the contract work actually begins. Actual performance of the services would be provided in accordance with an established performance framework, including metrics, which could be used to evaluate effectiveness.

In this type of situation, we suggest that the regulations provide that federal agencies (and other purchasers, including state and local agencies seeking to coordinate with the Department to obtain the benefits of SAFETY Act protections for vendors) could include as an acceptable method of verification a requirement (1) to specify in their solicitations a method for demonstrating that the solution proposed and delivered meets the requirements of the contract (*e.g.*, completion of a live test demonstration, first article testing, or acceptance testing), and (2) to identify any other safety or hazard analyses that must be submitted to the agency and/or the Secretary. In addition, the solicitation and resulting contract could state that, upon successful completion of the specified demonstration or testing, the Secretary will provide an expedited review of the services component for Designation as QATT and Certification as an Approved Product/Service for Homeland Security.

Third, the regulations should provide that in appropriate circumstances, relating to an anti-terrorism procurement, professional systems design and other services themselves may be Designated as QATT from the inception of performance.

Fourth, in circumstance where there will be a delay in the Department's SAFETY Act approval process until some portion of the contract work has been

initiated, the decision of whether the products and/or services will be designated as QATT and certified as an approved Product for Homeland Security will likely have a significant impact on the price. The regulations should specifically provide for an equitable adjustment in the contract price if (1) the products and/or services are priced based on the assumption that they would receive SAFETY Act approval but the Secretary declines to designate and/or certify those services, or (2) if the Secretary establishes a required amount of liability insurance that imposes a cost on the Seller in excess of an assumed insurance cost stated in the proposal. Upon mutual agreement of the contractor and the government, the contractor also should be allowed to cease performance of the contract without penalty or make its performance expressly contingent upon Designation and/or Certification.

Fifth, it is important that the regulations recognize that products and services are not static. In particular, the nature of the technology required for the defense against terrorism, or to respond to a terrorist attack, may vary as the program is implemented and becomes operational. The proposed regulations, however, arguably would require termination of QATT Designation if the technology was significantly changed or modified in a way that could significantly affect the safety or effectiveness of a device. *See* Section A.1. of these comments. It is completely impractical for technology providers – particularly providers of complex systems design and integration services, or other service providers -- to reapply to DHS every time such a change is required to comply with evolving customer requirements under a performance-based contract.

With respect to technology sold to federal and state agencies, there is generally an established process for incorporating changes, sometimes at the unilateral direction of the government agency, to contract documents. This process could be used as a baseline for acceptance of changes to the requirements document or performance framework. We recommend that, for systems sold to governments, any changes to the provider's requirements document or performance framework that are approved by the customer be considered within the scope of the QATT Designation and not automatically terminate or require reapplication.

Sixth, the regulations should provide for sufficient flexibility in evaluating and certifying services that involve operation or support of a previously-designated QATT. If a Seller applies for SAFETY Act coverage for services involved in operating and maintaining a qualified anti-terrorism device, the scope of the evaluation process would be different depending upon the nature of the service. For example, different factors would be involved in evaluating (a) operation of a QATT device that requires some human manipulation (*e.g.*, wiping a swab on luggage for detection of explosives at airports); (b) operation of a QATT device such as an X-ray

machine that requires some degree of skill on the part of the operator; and (c) performing passenger screening services involving the use of one or more QATTs (*e.g.*, metal detecting wand or sophisticated imaging) at the discretion of the contractor performing the service. These services obviously involve very different levels of capability on the part of the service provider. The regulations should be sufficiently broad so that the Department may request commensurately different information to be submitted to support the application for Designation and Certification. For example, for services that are necessary simply to operate an already Designated and/or Certified QATT, such as those described in example (a), the regulations should provide a simplified application procedure under which Designation and Certification would be effective immediately upon the filing of an application by the service provider.

Seventh, the regulations should expressly state that services may be Designated as QATT and Certified for Section 863(d) immunity even if the services themselves would not be considered intellectual property *per se*, and even if the services involve the operation of devices that may not be QATT.

D. Single Federal Cause of Action

The SAFETY Act (§ 863(a)(2)) states that United States district courts "shall have original and exclusive jurisdiction" over suits involving claims relating to acts of terrorism when designated anti-terrorism technology has been deployed, but does not explicitly state that federal actions preempt litigation in state or local courts.

In the preamble, the Department concludes that the "exclusive Federal cause of action" necessarily preempts such litigation in non-federal courts, and that such cause of action may be brought only against the seller of the QATT, and not against "arguably less culpable persons or entities, including . . . contractors, subcontractors, suppliers, vendors, and customers of the [s]eller. . . ." 68 Fed. Reg. at 41424. The extent to which Sellers of designated technologies and their customers and suppliers are potentially subject to a plethora of lawsuits in various fora is a fundamental promise of the entire QATT program, including most obviously the efficacy of the liability cap keyed to the required level of liability insurance. Given the importance of this issue, we strongly recommend that the Department codify in a "Findings and Purpose" section of the regulations themselves the Secretary's understanding of Congressional intent in the SAFETY Act and its resulting overview of the operation of SAFETY Act program for which the Secretary is responsible, including the inter-relationships among the various sections of the SAFETY Act.

E. Insurance

As provided in the SAFETY Act, the proposed regulations require that the Department certify, and require the seller of a QATT to obtain and maintain, an amount of liability insurance for a single act of terrorism appropriate to satisfy third-party claims arising from such act of terrorism where the QATT has been deployed. Proposed Section 25.4(a). The certified amount (which may include self-insurance) is not to exceed an amount reasonably available on world markets at prices and terms that will not unreasonably distort the price to be charged for the QATT. Proposed Section 25.4(b). The Department has specifically requested comments on the appropriate interpretation of "prices and terms that will not unreasonably distort sales prices," and the factors that should be used in determining the appropriate amount of insurance. 68 Fed. Reg. at 41425.

In determining whether an insurance premium will "unreasonably distort" the price of the product or service, we recommend that the Secretary consider factors including the following: (a) the percent by which the sales price of a pre-existing product or service would increase if it were deployed for an anti-terrorism purpose; (b) the percent by which the Seller's indirect cost rates would increase if the insurance were purchased; and (c) the Seller's cost of liability insurance for QATTs as a percentage of the total price of the QATTs as compared with the Seller's cost for liability insurance as a percentage of the total price of non-QATT goods or services.

We also recommend several modifications to the insurance-related provisions.

First, the regulations should provide expressly that, if the Department determines that no liability insurance meeting the statutory requirement is "reasonably available" that does not "unreasonably distort" the price of the technology, the Under Secretary nevertheless has the authority to designate the technology as a QATT, certify the QATT as an Approved Product/Service for Homeland Security eligible for the Section 863(d) immunity, and determine that the Seller's maximum liability is zero because there is no amount of reasonably available insurance.

Second, the regulations should state that the "reasonably available" standard permits the Department to accept the Seller's existing general liability coverage as sufficient for purposes of the SAFETY Act, at least in the short term, and that the SAFETY Act insurance need not be a specific stand-alone policy.

Third, most general liability policies do not cover the acts of third parties, and it is unclear to what extent, if at all, such coverage will become available in the

future. The regulations should clarify that, as an alternative to the "zero liability" determination, the Department may certify as appropriate an amount of insurance that does not contain upstream/downstream protection if the Department determines that that is the only insurance "reasonably available."

Fourth, given the nature of the post-September 11 insurance market, the cost of war and terrorism risk insurance (if available at all) may be extremely high compared to current and past costs of general liability insurance. We believe it is clear that the costs of insurance certified under this section are allowable costs on federal government contracts under FAR § 31.205-28. To eliminate the risk of any dispute on this issue, however, we recommend that the regulations be amended to recognize expressly that insurance certified under this section, whether the costs are treated by the contractor as direct costs or indirect costs, shall be considered "insurance required or approved and maintained by the contractor" within the meaning of FAR § 31.205-28(a)(1).

Fifth, the regulations provide for an annual certification by the Seller that it has maintained the required insurance. It is unclear whether a separate certification for each QATT is contemplated when a Seller is providing more than one such technology. The regulations also require the Seller to notify the Under Secretary of any changes in types or amounts of liability insurance coverage for any QATT. *See* Proposed Section 25.4(g). There is no statutory requirement for such a certification,[3] and the requirement for yet another certificate is unnecessarily

---

[3] Although the SAFETY Act regulations are arguably not "procurement regulations," the certification requirement would be a condition of selling QATT to the federal government. As such, the requirement is inconsistent with the Federal Acquisition Reform Act ("FARA"), which provides, in part, as follows:

> A requirement for a certification by a contractor or offeror may not be included in a procurement regulation of an executive agency unless--
>
> (i) the certification requirement is specifically imposed by statute; or
>
> (ii) written justification for such certification requirement is provided to the head of the executive agency by the senior procurement executive of the agency, and the head

(continued...)

burdensome for both industry and the Government, particularly in light of the separate requirement for Sellers to notify the Government of any changes to their insurance coverage. Accordingly, we recommend that the annual certification requirement be deleted from the regulations.

Sixth, the regulations should expressly provide that the Designation and Certification of QATT shall not automatically terminate upon the cancellation or reduction of insurance coverage through no fault of the Seller. The regulations should provide for an expedited review process to determine the availability of other sources of insurance, or to set a reduced amount of required insurance if that reduced amount is all that is available without distorting the price of the QATT. During this review process, the QATT should continue to be subject to the SAFETY Act protections. In addition, the regulations should specify that the Seller will not be penalized in connection with existing QATT Designations or future applications if its coverage is reduced, or eliminated entirely, because insurance at a reasonable cost is no longer available on the world market.

Seventh, proposed Section 25.4(b)(6) could be interpreted to require the applicant to disclose information regarding mass casualty losses. The terms of the settlement of mass tort claims are often subject to strict confidentiality agreements. In those cases where the information is not publicly available, disclosure could be seriously disadvantageous to a Seller. Accordingly, we recommend that any company-specific data, other than aggregated information available from insurance industry associations and research institutions, be subject to the same restrictions on disclosure as those that apply to other proprietary or confidential information, as discussed in Section H below.

Finally, to minimize duplicative or overlapping insurance policies, we recommend that, as part of the application process, the regulations permit coordination in obtaining insurance for projects in which there are multiple Sellers.

(...continued)

> of the executive agency approves in writing the inclusion of such certification requirement.

41 U.S.C. § 425(c)(2)(A).

F. Post-Designation and Certification Changes

The proposed rules provide for automatic termination of a Designation if the technology "is significantly changed or modified," including the design, material, manufacturing process or purpose for which the QATT is sold. A significant change is one that "could significantly affect the safety or effectiveness of the device." Proposed Section 25(i).

The regulatory process for dealing with changes in qualified technology should not be so burdensome or risky that there is a disincentive for making improvements. For example, we assume only changes that could *adversely* affect the safety or effectiveness of the QATT would trigger the automatic termination of the Designation. The regulations should explicitly so provide. Also, the regulations seem to assume that the prior Designation will be modified, but that is not necessarily the case. A Seller might wish to retain the original Designation and continue to make sales of that original version of the technology even though a significantly improved version of the technology is now available. The regulation should be clarified to address this point.

We strongly recommend that the regulations expressly provide that a change will be considered "significant" only if the change materially affects the function or operation of the QATT. In this regard, it is critical to define as precisely as possible when a change must be submitted, clarify that upgrades, enhancements, and other changes standard in the particular industry are not subject to additional review, and provide for an expedited review of changes to QATTs already designated (and perhaps certified). As proposed, the review procedure would require Sellers to make a judgment call as to whether a change is "significant" so as to require re-designation and re-certification. DHS has recognized the difficulty in predicting the types of terrorist threats that may emerge and the types of technologies that may be required to respond to those threats. Adding to the difficulty is the possibility that terrorist threats may evolve rapidly, necessitating numerous changes in QATT to keep pace with those threats. Because the loss of a QATT Designation or Certification could be financially ruinous, to the extent that there is ambiguity, a prudent Seller might conclude that even relatively minor changes should trigger a revised filing, causing administrative burdens and delays arising from a veritable flood of unnecessary filings. The mere act of filing might also be construed as an implied admission that the change was significant.

One possible approach to the problem of ambiguity is to provide that the Designation for each QATT will be drafted in a way that includes changes approved by the customer and identifies the types of additional changes that will require

submittal for re-designation. For example, the provision in Proposed Section 25.5(i) that "changes or modifications will be evaluated at a minimum with reference to"....should be revised to delete "at a minimum." The regulations should set forth with the greatest specificity possible the kinds of changes the Secretary would consider to be sufficiently significant to trigger a termination of Designation and/or Certification unless a new application is filed. Absent such specificity, we are concerned that every lawsuit involving a QATT will include an allegation that the technology was significantly changed and the Designation/Certification had therefore been automatically terminated. The issue of whether a change in a QATT was "significant" should be determined in the first instance by the Secretary, not by a court.

We also strongly recommend that the regulations provide for a separate, expedited process for reviewing changes to QATTs. DHS personnel will already be familiar with the underlying technology and should be able to determine promptly if the change requires full-blown re-analysis. The regulations should require that the process be completed as quickly as possible, but, except in extraordinary circumstances, should not take more than 60 days.

Finally, as part of the process for reviewing changes, the proposed regulations should provide for the Secretary to determine, retroactive to the date of the submission of a proposed modification to a QATT, that (a) the proposed modification was not "significant," or (b) alternatively, that the proposed change was "significant" but that the QATT should retain its Designated and Certified status. A retroactive approval provision would minimize the risk that, during the period in which the Secretary is evaluating the modification, a Seller will refuse to sell a previously-designated/certified QATT or will continue to sell the original QATT rather than the modified – and presumably improved – version of the technology. As in the case of initial applications, this change would provide protection to a Seller who elects to make its modified technology or service immediately available to the public and thereby encourage the deployment of an improved QATT at the earliest possible date.

G. Relationship to Procurements

Whether and how quickly a technology is designated and certified under the SAFETY Act will have a profound impact on the Government's acquisition of products and services intended to provide protection against terrorist acts. Although DHS has the ultimate responsibility for the Designation and Certification decisions, as a practical matter other federal agencies that are acquiring those products and services must be included in the process. We recommend the following

modifications to the regulations to accommodate the needs of acquiring agencies, Federal, State and local.

First, the regulations should expressly state that federal, state, and local government agencies may notify offerors that a particular solicitation contemplates the acquisition of technology that will be recommended to DHS for Designation as QATT.

Second, the regulations should establish an expedited review process for any technology in a proposal submitted in response to such a solicitation issued by a federal, state, or local government agency. The expedited process would include provision for SAFETY Act review to be performed in parallel with the agency's evaluation process, to the maximum extent possible.

Third, the regulations should specifically authorize the Under Secretary to consult with representatives of any federal, state, and local government agency seeking to acquire technology for purposes of assessing the timing or approval of an application submitted for Designation as QATT or for Certification.

Fourth, the regulations should encourage agencies to allow the submission of bids or proposals for which the price, contract performance, or other terms are conditioned upon QATT Designation, in which the bidder reserves the right to withdraw the bid or proposal if QATT Designation is denied, or in which the bid or proposal is conditioned upon a price renegotiation if QATT Designation is not provided or an insurance requirement is set at a higher cost than was set forth as a stated assumption in the proposal. DHS should pursue corresponding revisions to the Federal Acquisition Regulation that would be binding on other agencies.

H. Protection of Intellectual Property, Trade Secrets, and Other Confidential Information

A substantial portion of the data that the Seller is required to disclose to the Secretary and Under Secretary will constitute confidential and proprietary commercial and technical information, including trade secrets. The Department recognizes that "successful implementation of the Act requires that applicants' intellectual property interests and trade secrets remain protected in the application and beyond." 68 Fed. Reg. at 41423. The preamble specifically recognizes the flexibility in the Freedom of Information Act ("FOIA"), but offers no guidance on how it will apply to information submitted in the application process. *Id.* The regulations also include little guidance for assuring the required protection beyond stating that the application and review process will maintain the confidentiality of

an applicant's proprietary information. Section 25.8. We believe that significant modifications to the regulations are essential to assure the protection of proprietary data.

First, the regulations should include specific restrictions on disclosure of (a) information submitted in connection with an application for Designation or Certification, and (b) documents and other materials prepared by Government employees, representatives, or private contractors in connection with the evaluation of applications. The restrictions should explicitly state that the prohibitions in FAR § 3.104-4 are applicable to disclosure of such information if it constitutes "contractor bid or proposal information" or "source selection information" within the meaning of the Procurement Integrity Act, 41 U.S.C. § 423. For information that does not relate to a specific Federal agency procurement, the regulations should include disclosure prohibitions and procedures that are substantially the same as the provisions of FAR § 3.104-4. For example, Section 25.8 of the regulations might include language such as the following:

> (a) For purposes of this section, the term "SAFETY Act information" means any information that is (1) submitted in connection with an application for Designation of technology as QATT or for Certification of technology as an Approved Product for Homeland Security; or (2) prepared by Government employees, representatives, or other individuals or entities in connection with the evaluation of applications.
>
> (b) Except as specifically provided for in this subsection, no person or other entity may disclose SAFETY Act information to any person other than a person authorized by law or the Secretary or Under Secretary to receive such information.
>
> (c) SAFETY Act information must be protected from unauthorized disclosure in accordance with applicable law and agency regulations.
>
> (d) Individuals unsure if particular information is SAFETY Act information should consult with agency officials as necessary. Individuals responsible for preparing material that may be SAFETY Act information must mark the cover page and each page that the individual believes contains SAFETY Act information

> with the legend "SAFETY Act information – See Section 25.8." Although the information in paragraph (a) of this section is considered to be SAFETY Act information whether or not marked, all reasonable efforts must be made to mark such material with the same legend.
>
> (e) Except as otherwise provided by law, the Under Secretary must notify the applicant in writing if the Under Secretary believes that proprietary information or other information marked in accordance with paragraph (d) herein has been inappropriately marked. The person or entity that has affixed the marking shall be given a reasonable period of time to justify any challenged marking.

Second, the regulations should include a rebuttable presumption that information submitted in the application and review process will be deemed to be privileged and confidential "trade secrets and commercial or financial information" exempt from disclosure under the Freedom of Information Act ("FOIA"), regardless of whether the information is marked with proprietary legends and limitations. *See* 5 U.S.C. § 552(b)(4).

Third, the regulations should provide that information submitted in the application and review process will be treated as information that "concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association" within the meaning of the Trade Secrets Act, 19 U.S.C. § 1905, regardless of whether the information is marked with proprietary legends and limitations.

Fourth, the regulations should require DHS in every instance to provide advance notification to the submitter when considering whether to disclose SAFETY Act information to third parties, give the submitter the right to refuse to agree to disclosure of the information, and to seek judicial review of any decision to disclose the information before such disclosure is made.

Finally, the broader Homeland Security Act provides that all "critical infrastructure information" submitted to DHS will be exempt from FOIA. *See* Homeland Security Act, Section 214(a)(1)(A). Because much of the information submitted by Sellers may constitute "critical infrastructure information," we suggest that the DHS regulation on confidentiality of information submitted as part of the consultation, Designation, and Certification processes include a

cross-reference to the "critical infrastructure information" protections provided by the statute.

I. Definitions

The definition of "act of terrorism" should clearly state that an act is "unlawful" if it violates any federal, state, or local law.

The Department should also revise the definition of "Seller" to mean "any person or entity that sells or otherwise provides anti-terrorism technology to Federal or non-Federal Government customers to whom the Department has issued a Designation for such technology under this Part." Our proposed revision would recognize as a Seller both the prime contractor who obtains a Designation for an overall anti-terrorism solution, and its subcontractors who either contribute components for which they have already received a Designation or who affirmatively seek to be designated as a Seller along with the prime contractor. Moreover, this change clarifies that no one else is a Seller for purposes of the Act. In contrast, under the broadly-worded definition in Proposed Section 25.9, the prime contractor and all of its subcontractors and suppliers could potentially be the Seller – irrespective of whether these entities affirmatively applied to be a Seller. The Department should revise the definition as suggested above to avoid this interpretation.

J. Relationship to Indemnification under P.L. 85-804

Although the proposed regulations themselves are silent about indemnification under Public Law 85-804, in the preamble the Department "recognizes" that "Congress intended that the SAFETY Act's liability protections would substantially reduce the need for the United States to provide indemnification under Public Law 85-804 to sellers of anti-terrorism technologies." The Department also "recognizes" that "there might be, in some limited circumstances, technologies or services with respect to which both SAFETY Act coverage and indemnification might be warranted." 68 Fed. Reg. at 41425.

The proposed balance in favor of immunity under the SAFETY Act rather than indemnification under Public Law 85-804 appears to reflect the February 28, 2003, amendment to the Executive Order on indemnification, Executive Order 10789 (Nov. 18, 1958, as amended). The revised Executive Order grants the Secretary the authority to issue indemnification under Public Law 85-804 and also provides that federal agencies (other than an exception for the Department of Defense) cannot provide indemnification "with respect to any matter that has been,

or could be, designated by the Secretary of Homeland Security as a qualified anti-terrorism technology" unless the Secretary of DHS had advised whether SAFETY Act coverage would be appropriate and the Director of the Office of Management and Budget has approved the use of indemnification.

Both the preamble and the proposed regulations are silent as to circumstances when indemnification under Public Law 85-804 might be warranted, and the process by which the Secretary will review determinations of other federal agencies to issue indemnification for "any matter that has been, or could be . . . a qualified anti-terrorism technology." We believe that the regulations should include some clarification of these issues.

First, we recommend that the regulations provide that Designation under the SAFETY Act shall not preclude the granting of indemnification under appropriate circumstances. For example, such indemnification might be necessary to protect Seller against damages that might occur if the technology is deployed and there is injury other than injury arising from an act of terrorism.

Second, we recommend that the regulations clarify that, as part of the process for determining whether SAFETY Act protection or indemnification is appropriate, the Secretary will consult with OMB and other agencies as appropriate but will not exercise a "veto" authority over the determinations of other agencies.

K. Review of the Under Secretary's Decision

The proposed regulations provide that the Under Secretary's decisions on Designation and Certification are final and not subject to review. Sections 25.5(e), 25.7(e). The vast majority of technologies submitted under these regulations will be highly complex and involve innovative approaches to deter a wide range of chemical, biological, nuclear, and other threats. Given the likely variety and sophistication of these technologies, we believe that there is a real risk that significant features may be overlooked or misunderstood during the review and evaluation process, particularly if DHS elects to undertake the review without meeting with the applicant. The interests of the Government and the public would be served best by a process that builds in a method to resolve uncertainties and correct errors. Accordingly, we strongly recommend that the regulations specifically provide the applicant a right to administrative review of a decision by the Under Secretary to deny or restrict the scope of a Designation of technology as QATT or to deny Certification of a QATT as an Approved Product for Homeland Security.

* * *

Thank you for the opportunity to submit comments on the proposed regulations. Please contact us if we can answer any questions or provide additional information. Our points of contact are as follows: ITAA, Brendan Peter (703-284-5337) and Joe Tasker (703-284-5331); PSC, Alan Chvotkin (703-875-8059); AIA, Jason Cervenak (703-358-1044); and NAM, Quentin Riegel (202-637-3058).

Respectfully submitted,

Information Technology Association of America
Professional Services Council
Aerospace Industries Association
National Association of Manufacturers

August 11, 2003

Docket Management Facility
U.S. Department of Transportation
400 Seventh Street, S.W.
Washington, D.C. 20590-0001

By e-mail: http://dms.dot.gov

Re: Docket USCG-2003-15425; July 11 Department of Homeland Security Proposed Regulations Implementing the SAFETY Act

To Whom It May Concern:

The Professional Services Council (PSC) is pleased to submit these comments on the July 11 proposed regulations (68 F.R. 41420) issued by the Department of Homeland Security to implement the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act", or "the Act"). PSC is the leading national trade association representing the professional and technical services companies doing business with the federal government. PSC's approximately 155 member companies perform billions of dollars in contracts annually with the federal government, providing the full range of services, including information technology, high-end consulting, engineering, economic, international development, scientific and environmental and remediation services. Moreover, PSC's members are among the leaders in the provision of homeland security and national security services.

PSC strongly supports the SAFETY Act, and compliments the Department for moving expeditiously to issue proposed regulations. The SAFETY Act represents an important step toward assuring the government's ability to access the full scope of anti-terror technologies and capabilities.

However, PSC remains concerned that the regulations do not adequately address the critically important specifics relating to the Act's application to services vice products. We are mindful that the regulatory flexibility is limited by the inherent tensions created by the underlying statute. Nonetheless, since services will likely account for half or more of the federal government's procurements of anti-terror technologies and solutions, it is critical that the regulations provide as much detail and specificity as possible. Moreover, it is critically important that the regulations provide for robust application and that they provide clear instruction and guidance for balancing the statutory direction with sound business practices that will benefit the government. As noted later in these comments, PSC thus believes this must be an iterative regulatory policy and that, as a result of the comments received, the Department should seriously consider both a public meeting and additional rulemaking activities.

In addition, PSC has joined with other associations in separately submitting complementary additional comments on the proposed rule.

2101 Wilson Boulevard, Suite 750, Arlington, VA 22201-3009, 703/875-8059, Fax 703/875-8922, http://www.pscouncil.org

I. SUMMARY OF COMMENTS

1. We support the strong statements of coverage under the law and regulations for those companies offering services to address terrorism. The law is technology-neutral with respect to the scope of coverage and the protections offered. In our view, the regulations should be written in a technology-neutral manner to the maximum extent practicable, and only provide technology-specific guidance when such information would specifically address a unique application of the law to a given technology.

2. We compliment the Department for including the extensive background information included in the notice accompanying the proposed rule. Having the Department spell out its interpretations of the Act and its legislative history, and giving the public information on areas where the Department has made an initial determination of how to implement the Act and where additional comments from the public are requested, was extremely valuable in the formulation of our comments. As noted below, we recommend that the Department incorporate as part of the regulation (not merely in background or supplemental information) the Department's interpretations and regulatory philosophy. By making these views part of the regulations, all participants will have ready access to the information and be able to use that information directly in the application and interpretation of other specific provisions of the regulations.

3. PSC supports the Department promptly issuing any interim rule or rules to implement the Act. We recognize the difficulty of developing rulemaking on each and every provision of the Act, and the importance of maintaining an importance balance between the flexibility to address technologies and circumstances with the certainty in the application process and protections of the Act that Sellers and purchasers require. In our view, certain aspects of the regulations (such as the issues of the termination of a Designation or the transfer of a certification) can be deferred for subsequent rulemaking in favor of promptly publishing interim regulations addressing the application process for both Designation and certification, the procedures for protecting company proprietary information, and the insurance requirements.

4. Without regard to the timing of issuing any interim or final rules, we urge the Department to promptly (and if necessary separately) publish the application forms that interested applicants can use to apply for Designation or Certification and not wait until all application forms are complete. It is in the Department's and the potential Sellers' best interests to immediately commence the application process for both Designation and Certification. Other application forms discussed in the proposed rules (such as the application for transfer of Designation), while important, can be issued administratively in the next few weeks without jeopardizing the implementation of the Act or awaiting comprehensive interim or final regulations.

5. We support the broad scope of the term "qualified anti-terrorism technologies" under the law and proposed regulations, including the creation of an eighth evaluation criterion for Designation. We recommend that the categories of technologies that are available for Designation continue to be viewed broadly; this is particularly important when evaluating the application of the Act and regulations to services.

6. Proposed Section 25.5(f) provides that a Designation made by the Under Secretary shall be valid and effective for a term of five to eight years (as determined by the Under Secretary based upon the technology) commencing on the date of issuance. In our view, absent a change in

circumstances initiated by the Seller after the Department's initial approval of the Designation, there is no public policy reason to impose any fixed period of time on the useful life of the Designation period of a Qualified Anti-Terrorism Technology ("QATT"). We also encourage the Department to make the effective date of the Designation the date of the application for Designation.

7. Proposed Section 25.5(i) provides that a Designation shall terminate automatically, and have no further force or effect, if the QATT is significantly changed or modified. The proposal defined the term "significant change" as one that could significantly affect the safety or effectiveness of the device," including a significant change or modification. We strongly oppose the automatic termination of the QATT Designation even where based on significant changes or modifications.

8. With respect to the Certification for, and application of the government contractor defense, we assume that the title "approved product list" in the Act and the proposed regulations is not intended by Congress or the Department to exclude services. The Act and the regulations intentionally use the term "anti-terrorism technology" to refer to the source of approval, and that term is specifically defined in the Act and regulations to include services. We encourage the Department to use its rulemaking authority to recognize that different information to support the application for Certification may be available and applicable to products that may not be available or applicable to services.

9. With respect to the issue of protecting company proprietary information, we compliment the Department for recognizing the importance of protecting the confidentiality of an applicant's intellectual property, trade secrets and other confidential information. Any interim or final rule should explicitly provide procedures that applicants should follow to ensure their information can be protected. For example, we strongly recommend that the Department develop a proprietary data marking or other application notice by which applicants highlight or disclose those portions of its application it considers to be proprietary.

10. Finally, with respect to the relationship between the SAFETY Act and P.L 85-804, we compliment the Department for acknowledging both the Congressional and Departmental coverage of the relationship between these two important government contracting statutes and that there are circumstances under which these two acts can, and should, co-exist. We recommend that the Department create a new part to these regulations to address this important matter.

II. REQUEST FOR PUBLIC MEETING

1. The notice of proposed rulemaking requests comments on the desirability of holding a public meeting on the regulations.[1] We believe a public meeting that provides for an exchange of views between the Department (and other appropriate government officials) and interested members of the public on key aspects of this regulation would be beneficial. We do not see any value to such a meeting if the Department would only repeat the elements of the proposed rule or if the public would only be permitted to make oral presentations that could be appropriately included in written comments.

---

[1] 68 F.R. 41420 (July 11, 2002)

2. However, following the formal submission of all comments on this proposed rule, Department representatives may find helpful the opportunity to raise questions to the public about any comments submitted, and for Department representatives to address any significant conflicts raised in the comments. The public would similarly benefit from such a public meeting. However, we do not recommend that the rulemaking process be delayed simply to hold such a meeting; we believe the Department's highest priority should be to provide interim or final guidance on the application process and the key elements of the qualification standards for those companies interested in seeking Designation as a qualified anti-terrorism technology and certification for the government contractor defense.

III. ITERATIVE RULEMAKING WILL FURTHER THE TIMELY IMPLEMENTATION OF THE ACT

1. PSC supports the Department promptly issuing any interim rule or rules to implement the Act. We recognize that the SAFETY Act regime is a series of inter-related provisions. But as the Department notes in the Regulatory Background and Analysis Section of the proposed rules, the "Department will begin implementation of the SAFETY Act immediately with regard to federal acquisitions of anti-terrorism technologies and will begin accepting other SAFETY Act applications on September 1, 2003."[2] We strongly support the prompt implementation of the Act and urge the Department to move expeditiously to issue interim final regulations on the essential opening aspects of coverage, such as the application process, the insurance requirements, and the treatment of company proprietary information. Other aspects of the regulations (such as addressing the issues of the termination of a Designation or the transfer of a Certification) can be deferred for subsequent rulemaking over the next several weeks.

2. We recognize the difficulty of developing rulemaking on each and every provision of the Act, and the importance of maintaining an important balance between the flexibility to address technologies and circumstances with the certainty in the application process and protections of the Act. We do not believe in a "static" set of regulations that is unrelated to the changing threat or to the changes in technologies. Yet it is important to start, and to start quickly with what the Department knows today.

IV. EXPLICITLY INCORPORATE RELEVANT "BACKGROUND" INFORMATION INTO THE REGULATIONS

1. We compliment the Department for providing an extensive background statement accompanying the actual regulations. In that background statement, the Department has provided useful information on the legislative history of the SAFETY Act, the Department's interpretation of the Act and its regulatory philosophy for implementing the Act. The background section explains the inter-relationship between key provisions of the Act, and between this Act and other related provisions of law. Finally, the background section highlights areas where the Department is seeking additional public comments.

2. This extensive background section was extremely valuable. It provided the public with a clear indication of the Department's approach and areas of uncertainty. It requested public comments on areas where the Department thought additional commentary would aid in the development of final regulations and help guide the Department in the implementation of the Act. We encourage

---

[2] 68 F.R. 41420 (July 11, 2003)

the Department to keep the lines of communication with the public open and to accept additional comments on any provision of the emerging regulations.

3. In addition, we strongly recommend that, in any interim or final rule, the Department create a new subpart of 6 C.F.R. Part 25, possibly Part 25.0, entitled "Introduction", wherein the Department includes within the text of the regulations its key regulatory philosophy (such as the intent that the definition of anti-terrorism technology be viewed broadly, or that the Department "eschews a one-size-fits-all" approach. These are important regulatory statements that are important to all who will use the regulations today and into the future, to implement and use the SAFETY Act and its regulations.

4. This placement is more than an issue of administrative law and interpretation. Many will have ready access to the formal regulations but not all will have such ready access to the one-time Federal Register publication. By having the Department's philosophy and approach included in a single document, officials in every department and agency, interested Sellers, insurance organizations and the public will have the needed information in a single location with authoritative affect.

V. SPECIFIC COMMENTS ON THE PROPOSED REGULATIONS

A. SECTION 25.2 -- DELEGATION

1. We recommend vesting all regulatory decision-making for the SAFETY Act in the Secretary of Homeland Security. Under the proposed rules, certain final decision-making is vested exclusively in the Under Secretary. Throughout the regulations, we recommend that it is the Secretary that has the authority under the law and regulations. It was the Secretary, for example, that issued these proposed rules!

2. Section 862(a) of the Act vests responsibility for administration of the SAFETY Act in the Secretary of Homeland Security; other provisions of the Act require the Secretary to take certain actions.[3] Section 25.2 of the proposed rules provide that all functions of the Secretary under the Act may be delegated to the Under Secretary for Science and Technology or the Under Secretary's designees.[4]

3. Unless Congress has constrained the authority of the Secretary of Homeland Security to delegate functions assigned to him by law, the Homeland Security Act of 2002 allows the Secretary of Homeland Security to delegate any function to other officials within the Department.[5] We do not object to the Secretary's delegation of functions to implement the SAFETY Act to the Under Secretary or even delegating certain functions to the Assistant Secretary. While we appreciate the explicit information about who is responsible for implementing portions of the SAFETY Act, we are concerned that final authority for certain

---

[3] For example, Section 862(c) provides authority for the Secretary to issue regulations; section 863(d) grants the Secretary exclusive authority to review and approve technologies for the government contractor defense and to issue a certificate of conformance and place a technology on the "Approved Product List for Homeland Security"; section 864(a)(1) requires the Secretary to set the type and amount of liability insurance for Sellers; and section 865(2)(A) provides that the Secretary determines what constitutes "an act of terrorism."

[4] 68 F.R. 41428 (July 11, 2003)

[5] See, generally, Homeland Security Act of 2002, P.L. 107-296

critical determinations under the regulations improperly stops at a level below the Secretary.[6] Other concerns arise when no one is serving in the assigned position, such as with the position of the Assistant Secretary for Plans, Programs and Budget.[7]

4. We therefore recommend that any interim or final regulations state that the authority vests in the Secretary; to the extent that delegations are made (pursuant to Section 25.2 of these regulations or other authority provided to the Secretary), those delegations can be made administratively, with the public informed through separate administrative notices, the Department's website, the application process or otherwise about who in the Department has the authority to act on behalf of the Secretary in implementing this act.

B. SECTION 25.3 DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES ("QATT")

1. Scope of the definition

a. Section 862(b) of the Act authorizes the Secretary of Homeland Security to designate anti-terrorism technologies that qualify in accordance with the criteria in the Act and implementing regulations for protection under the risk management procedures of the statute.[8] The Act specifically defines the term "qualified anti-terrorism technology" as:

> "any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts may otherwise cause, that is designated as such by the Secretary."[9]

b. PSC worked directly with the Congress to ensure that a wide range of services, including support services and information technology, were included in the definition of "qualified anti-terrorism technology" ("QATT"). In our view, the types of services that may qualify as a QATT include, but are not limited to, training, maintenance, systems integration, testing, installation, repair, safety services, modeling, simulation, systems engineering, clean-up and remediation services, protective services, research and development, vulnerability studies, emergency preparedness planning and risk assessments. Information technology is also typically considered a service, although the Act separately identifies information technology as a "technology" under the Act.

c. We were pleased to see the Department's acknowledgment of this broad scope of coverage. Paragraph 1 of the "Specific Issues" discussion in the Background Section of the proposed rule properly notes that the "Department recognizes that the universe of technologies that can be

---

[6] Even Section 25.9 of the proposed regulations, entitled "Definitions" provides that the Assistant Secretary may be meant to apply to another other official of the Directorate of Science and Technology that the Under Secretary may designate. 68 F.R. 41432 (July 11, 2003)

[7] We note that the President nominated Dr. Albright for this position and on July 30, 2003 the Senate confirmed his nomination.

[8] Section 862(a) of P.L. 107-296 (Nov. 25, 2002)

[9] Section 865(1) of P.L 107-296 (Nov. 25, 2002)

deployed against terrorism includes far more than physical products."[10] We strongly recommend that the Department reiterate this expansive view in any interim and final regulations.

d. The Analysis portion of the Background section of the proposed rule also provides an important discussion of the Department's interpretation of the Act and the scope of the Secretary's authority. For example, the Background section notes:

> "the SAFETY Act applies to a very broad range of technologies...as long as the Secretary, as an exercise of discretion and judgment, determines that a technology merits Designation under the statutory criteria...Thus, consistent with Section 865 of the Act, Section 25.3(a) of the proposed rule defines qualified anti-terrorism technologies very broadly..."[11]

e. Section 25.3(a) of the proposed regulations provides that the Under Secretary may designate a qualified anti-terrorism technology for purposes of the protections under the Act, repeating the statutory definition.[12] We strongly recommend that the Department use its broad regulatory authority to also provide coverage for technologies that are "used, acquired or employed" as an anti-terrorism technology to better encompass the full range of services to be covered by regulations implementing the Act.

f. In addition, recognizing that providing "services" differs in some respects from providing "goods," we further recommend that a Seller may seek qualification eligibility based on coverage for a business area (such as for "hazardous material remediation services", not merely for anthrax remediation). We also recommend that the regulations provide for a "solicitation" qualification under which an offeror for a specific agency procurement may seek Designation for the specific use of a technology.

2. Approval criteria

Furthermore, Section 862(b) of the Act lists seven non-exclusive criteria that the Secretary shall consider when determining whether to make such Designation.[13] Section 25.3(b) of the proposed regulations repeats these seven criteria, and adds an eighth: "Any other factor that the Under Secretary may consider to be relevant to the determination or to the homeland security of the United States."[14] Consistent with the broad coverage of the Act and the recognition of the changing nature of the technologies that exist or that may emerge in the future to respond to threats to the homeland, we support the inclusion of this additional eighth evaluation standard.

3. Use of standards

a. Section 25.3(c) of the proposed rules provides that the Under Secretary may develop, issue, revise and adopt safety and effectiveness standards for various categories of anti-terrorism technologies, and may consider compliance with such standards that are applicable to a particular

---

[10] 68 F.R. 41423 (July 11, 2003)
[11] 68 F.R. 41421 (July 11, 2003)
[12] 68 F.R. 41428 (July 11, 2003)
[13] Section 862(b) of P.L. 107-296 (Nov. 25, 2002)
[14] 68 F.R. 41428 (July 11, 2003)

anti-terrorism technology before any Designation will be granted.[15] We support the Department's acknowledgment that externally established standards might be useful in determining whether to adopt and use standards in the Designation of a QATT. By the same token, as the Analysis portion of the Background section of the notice states:

> "These criteria are not exclusive—the Secretary may consider other factors that he deems appropriate... The Secretary may, in his discretion, determine that failure to meet a particular criterion justifies denial of an application... However, the Secretary is not required to reject an application that fails to meet one or more of the criteria."[16]

b. Thus, while the use and reliance on standards may be appropriate in certain circumstances and for certain types of technologies, we believe the Act and the regulations also permit the Secretary flexibility to not apply external standards to certain technologies – such as services. We encourage the Secretary to provide notice to the public, hopefully with an opportunity to comment, before instituting such standards against a specific type of technology. It is also important that this portion of the regulations refer to the ability of a technology to qualify for Designation by meeting the substantial equivalence standard included in proposed Section 25.3(d).

c. Paragraph 7 of the Specific Issues section of the Background section requests comment on how the Department can best develop standards and implement the SAFETY Act provisions to provide market and industry incentives for the development and deployment of anti-terrorism technologies.[17] From our perspective, we view the use of standards as an important, but evolving practice. Applicants are encouraged to identify external studies and analyses that may exist or that could be reasonably available to demonstrate that a technology meets performance requirements. However, as noted above, external standards are not appropriate for all technologies and the Department should not try to force the application of standards to all technologies, including services. We encourage the Department to use its rulemaking authority under the SAFETY Act specifically, and other statutes, to seek additional public input on any specific standards that may be considered for adoption and application to these technologies. In addition, we believe the pre-Designation consultation process can be an effective way for the Department to identify relevant standards.

4. Substantial Equivalence

a. Section 25.3(d) provides that a technology may satisfy the criteria under paragraph (b) and be designated as a QATT, and comply with the standards in paragraph (c), by taking into consideration evidence that the technology is "substantially equivalent" to other, similar technologies ("predicate technologies") that have been previously designated as a QATT under the Act.[18] The proposed rule provides only two tests for determining whether a technology may be deemed to be "substantially equivalent to a predicate technology."[19]

---

[15] 68 F.R. 41428 (July 11, 2003)
[16] 68 F.R. 41421 (July 11, 2003)
[17] 68 F.R. 41425 (July 11, 2003)
[18] 68 F.R. 41428 (July 11, 2003)
[19] 68 F.R. 41428 (July 11, 2003)

b. We strongly support the recognition of the concept of substantial equivalence and of a Seller's ability to point to predicate technologies to qualify for Designation as QATT. Even in paragraph (e) – relating to the duration and depth of review – the proposed regulations note:

> "For technologies with which the Federal Government or other government entity already has substantial experience or data (through the procurement process or through prior use or review), the review may rely in part upon that prior experience and, thus, may be expedited."[20]

c. We strongly support an expedited review and the authority provided in the regulations to rely on prior experience and substantial equivalence in making that eligibility determination.

5. Pre-application consultations

a. Section 25.3(h) provides flexibility to the Under Secretary to consult with potential SAFETY Act applicants regarding the need for or advisability of particular types of anti-terrorism technologies, although no pre-approval of any particular technology may be given. We strongly support this pre-application consultation. The Department and potential Sellers, as well as prospective developers of potential anti-terrorism technologies, will benefit from such consultation.

b. However, while the proposed regulations are properly silent on the scope of any technology that can take advantage of this pre-application consultation process, the supplemental information states, in part, that the Department may "provide feedback to manufacturers" regarding whether proposed or developing anti-terrorism technologies might meet the qualification factors under the Act, such that such feedback "may provide manufacturers with added incentive to commence and/or complete production of ...technologies that may otherwise be produced or deployed..."[21] We encourage the Department to highlight in the text of Section 25.3(h) that the pre-application consultation process is technology-neutral and available to any and all potential applicants of anti-terrorism technologies, whether manufacturing or services.

c. The proposed regulations also state that this pre-consultation is discretionary by the Under Secretary, "although no pre-approval of any particular technology may be given."[22] Specific Issue #2 in the Supplemental information states: "To be sure, the Department cannot provide advance Designation, as some of the factors for the Secretary's consideration cannot be addressed in advance."[23] We acknowledge and agree that the pre-consultation process cannot be the source of a pre-Designation. However, we recommend that the regulations use the phrase from the supplemental information: "cannot provide advance Designation;" nothing in the regulations focuses on the "approval" of a technology – only whether the elements of the statute can be met so as to grant "Designation."

d. The proposed regulations also explicitly provide that the confidentiality provisions are applicable to such pre-application consultations.[24] We strongly support such statement and recommend that it be retained in any interim or final regulation.

---

[20] 68 F.R. 41428 (July 11, 2003)
[21] 68 F.R. 41423 (July 11, 2003); Specific Issues #2 – Development of New Technologies
[22] 68 F.R. 41429 (July 11, 2003); Proposed Section 25.3(h)
[23] 68 F.R. 41423 (July 11, 2003); Specific Issues #2 – Development of New Technologies
[24] 68 F.R. 41428 (July 11, 2003)

6. Term of Designation

a. Proposed Section 25.5(f) provides that a Designation made by the Under Secretary shall be valid and effective for a term of five to eight years (as determined by the Under Secretary based upon the technology) commencing on the date of issuance.[25] The regulation also provides that the protections conferred by Designation shall continue in full force and effect indefinitely.[26] The Department specifically requests comments on the validity period of the Designation.[27]

b. While this term of Designation is addressed under the heading of Procedures in Section 25.5(f) of the proposed rule, we address it here as directly relevant to the Designation of a QATT. There is no statutory provision or legislative history to indicate that Congress intended that the Designation would exist for a fixed period of time. Furthermore, since one of the purposes of the Act is to encourage interested Sellers and developers to commit resources towards the development of anti-terrorism technologies, fixed periods of limitations may have a chilling affect on those developers. In our view, absent a change in circumstances after the approval of the Designation, or fraud in the application process, there is no public policy reason to impose a fixed period of time on the Designation period of a QATT.

c. However, if the Department does determine to impose a fixed term limitation, we strongly recommend that it be a uniform, single fixed period of time, and for as long as possible. A ten-year term would not be inappropriate. Of course, an application for renewal, if approved, would extend this term for an additional period, as determined by the Secretary.

d. Elsewhere in the regulations, the Department has proposed that Designation may be withdrawn or cancelled under specific circumstances. We address those circumstances in our comments relating to Section 25.5(i).

C. SECTION 25.4 OBLIGATIONS OF SELLERS

1. The coverage for liability insurance and its relationship to the Designation of QATT, to the continuing obligations to maintain coverage and protections and to the impact on the insurance industry are among the most difficult issues in the Act and the most challenging for the regulatory coverage. The supplemental information accompanying the rule notes that the "Department eschews any 'one-size-fits-all' approach to the insurance coverage requirements."[28] We strongly support that philosophical approach to the regulations and urge that this statement be included in the introductory provisions of any interim or final rule.

2. Section 864(a)(1) of the Act requires any person or entity that sells or otherwise provides a QATT ("Seller") shall obtain liability insurance of such types and in such amounts as shall be required in accordance with the section and certified by the Secretary to satisfy otherwise compensable third-party claims when QATT has been deployed in defense against or response or recovery from a terrorism act.[29] Proposed Section 25.4(a) repeats the statutory requirement, and adds authority for the Under Secretary to request at any time that the Seller or other provider of

---

[25] 68 F.R. 41430 (July 11, 2003)
[26] Id.
[27] 68 F.R. 41422 (July 11, 2003)
[28] 68 F.R. 41424 (July 11, 2003); Specific Issue #6 – Amount of Insurance
[29] Section 864(a)(1) of P.L. 107-296; November 25, 2002

QATT submit information that would assist in determining the amount of liability insurance required, or show that the Seller or other provider has met all of the requirements of this section.[30]

3. We support the authority of the Under Secretary to request information that would assist in making the determination of the amount of liability requested. However, once the amount is set for a specific Designation based on a specific application submitted by a specific Seller, we do not believe the Department should subsequently and unilaterally vary the amount of insurance required for that Designated Seller to maintain its qualification, absent a request from the Seller for a reconsideration of the insurance certification due to changed circumstances or other reasons. This reconsideration approach is already addressed in proposed Section 25.4(h) – Under Secretary's certification – where the Seller may petition the Under Secretary for a revision or termination of the certification.[31]

4. The Act also provides for a maximum amount of required liability insurance and a necessary scope of coverage for such insurance.[32] Proposed Section 25.4(b) repeats the statutory requirement and adds the requirement for the Under Secretary to determine the amount of liability insurance required for each technology or family of technologies. The proposed regulations also permit the Under Secretary to consider nine non-exclusive factors in setting that amount.[33] Information derived from this list will assist the Department in setting the appropriate insurance amounts. We support the inclusion of the phrase "family of technologies" as supportive of the Department not looking at a case-by-case determination for each application or for each specific technology. Since the insurance may be looked at on a "family of technologies" basis, we find support for our earlier recommendation that an applicant may also apply for Designation for a "family of technologies."

5. The supplemental information accompanying the regulations, but not the regulations themselves, notes that the Department may consult with the Seller, the Seller's insurer and others.[34] While we support the Department's broad outreach to understand the appropriate insurance coverage that would be applicable to a technology, we urge the Department to use caution when discussing a Seller's insurance with an insurer without the Seller's knowledge and participation. Numerous business decisions are included in a Seller's decision to obtain coverage; the Department should have the benefit of the totality of the Seller's considerations, not simply the insurer's perspectives on the Seller's choices. Of course, we support the Department's continued outreach to the insurance community for assistance in assisting the Department in executing its responsibilities under the Act.

6. Section 864(a)(2) of the Act and Section 25.4(b) of the regulations address the maximum amount of insurance that a Seller is required to obtain. We encourage the Department to combine the regulatory coverage of this section with the provisions in Section 864(c) of the Act and to interpret the requirements of Section 864(c) of the Act (that establishes the maximum liability of all claims against the Seller at an amount required to be maintained by the Seller under Section 864 of the Act) as applying the maximum insurance amount as provided for in Section 864(a)(2) of the Act and Section 25.4(b) of the regulations.

---

[30] 68 F.R. 41429 (July 11, 2003); Proposed Section 25.4(a)
[31] 68 F.R. 41430 (July 11, 2003); Proposed Section 25.4(h)
[32] Section 864(a)(2) of P.L.107-296; November 25, 2002
[33] 68 F.R. 41429 (July 11, 2003); Proposed Section 25.4(b)
[34] 68 F.R. 41424 (July 11, 2003); Specific Issue #6 – Amount of Insurance

7. Section 864(a)(3) of the Act and Section 25.4(c) of the regulations address identically the scope of the liability insurance coverage. This broad scope of coverage is understandable under the regime set for in the Act. We encourage the Department to provide flexibility in the administration of this section such that the scope of the insurance coverage must be in place by the time the application for Designation or Certification is granted – not necessarily at the time the application is submitted. We encourage the Department to provide flexibility in the administration of this section such that the scope of the entities protected by the insurance coverage may vary over time and typically many of these entities will not be known at the time of the application submission or application approval. Thus, we recommend that the Department require only that the insurance coverage be in place only by the time the application for Designation or Certification is granted – not necessarily at the time the application is submitted and that the scope of protected entities be fixed at the time of application approval. Given the length of time the Department has to review and approve an application, requiring such coverage prematurely could have a significant financial impact on Sellers, particularly small businesses. Furthermore, the Department should specifically recognize that the extension of the insurance protection to designated entities will vary over time as a technology moves from concept to sale; the number of entities to be protected will also vary over time as new sales are made. Nevertheless, an applicant and the Department must have some certainty in the application process in addressing only known coverage and known designated entities at the time of the application. The Department should explicitly provide that the unintentional omission of a designated party does not nullify the application or, by itself, rise to the level of fraud in the application process. The regulations should address the procedures for modifying the insurance coverage and for adding additional designated entities unintentionally omitted during the application process or first identified after an application is approved, and for deleting entities no longer subject to the protections. We do not believe the Department needs to treat these evolving requirements as a new application requiring further advance Departmental approval. In our view, adding or deleting entities is not, by itself, the "change in the types or amounts of liability insurance coverage" that requires notification to the Under Secretary pursuant to Section 25.4(g).

8. Section 864(a)(4) of the Act and Section 25.4(d) of the regulations provide identical requirements for the scope of coverage for third party claims. We encourage the Department to provide flexibility in the administration of this section such that the scope of the insurance coverage for third party claims must be in place only by the time the application for Designation or Certification is granted – not necessarily at the time the application is submitted. Given the length of time the Department has to review and approve an application, requiring such coverage prematurely could have a significant financial impact on Sellers, particularly small businesses.

9. Section 864(b) of the Act and Section 25.4(e) of the regulations provide identical requirements for the Seller to obtain a reciprocal waiver of claims from any party involved in the production or use of the QATT. Like the requirements of Section 25.4(c) regarding scope of coverage, we encourage the Department to provide flexibility in the administration of this section such that the scope of the reciprocal waivers for known entities must be in place only at the time the application for Designation or Certification is granted – not necessarily at the time the application is submitted. We also encourage the Department to provide flexibility in the administration of this section such that the identification of those entities for which cross-waivers are required may vary over time; typically many of these entities will not be known at the time of the application submission or application approval. Nevertheless, an applicant and the Department must have some certainty in the application process in addressing only known

designated entities at the time of the application. The regulations should address the procedures for adding additional designated entities first identified after an application is approved. The Department should also explicitly provide that the unintentional omission of a designated entity or the inability to obtain a particular waiver does not nullify the application or, by itself, rise to the level of fraud in the application process. The regulations should address the procedures for adding additional designated entities previously identified or unintentionally omitted during the application process, or first identified after an application is approved, or where despite good faith efforts no cross-waiver can be obtained; this is likely, in fact, when the customer is the federal government (or any other unit of government) that will not be initially familiar with the requirements of the SAFETY Act and lack policy guidance on the scope of authority to enter into such cross-waivers. The regulations should also address the procedure for deleting designated entities. We do not believe the Department needs to treat these evolving requirements as a new application requiring further advance Departmental approval; in our view, adding or deleting entities is not, by itself, the "change in the types or amounts of liability insurance coverage" that requires notification to the Under Secretary pursuant to Section 25.4(g).

D. SECTION 25.5 PROCEDURES

1. Application procedures

a. Section 25.5(a) provides a statement on the application procedures. It requires any Seller seeking Designation to submit "all information" supporting such request to the Assistant Secretary.[35] However, the word "all" is not otherwise explained. We recommend deleting the word "all" to avoid any implication that the Seller is under an obligation to undertake a comprehensive search for any information that has a bearing on the application and Designation process. Such a requirement would be inconsistent with the goals of the statute and the related provisions of the regulations. If necessary, it would be appropriate to indicate in this Section that applicants must fully complete the items on the Department's application form, including submitting the information requested by the Department.

b. The proposed rule provides that the application request is submitted to the Assistant Secretary, or such other official as the Under Secretary may designate from time to time. The additional disjunctive phrase is unnecessary; the Delegation provisions in proposed Section 25.2, and the definition of the term "Assistant Secretary" in proposed Section 25.9 already provide such flexibility.

c. This proposed paragraph also provides that the Under Secretary will make the application form available through various means. We strongly encourage the Department to expeditiously create the initial application form and make it widely and promptly available to facilitate interested Sellers making application for Designation. Timeliness of the application form is particularly important to meet the Department's goals, and industry's desire, to begin implementation of the SAFETY Act immediately with regard to Federal acquisitions and for the Department to begin accepting other SAFETY Act applications by September 1, 2003.

2. Initial notification

---

[35] 68 F.R. 41430 (July 11, 2003)

Section 25.5(b) begins the 150-day Departmental review process for Designation (unless expedited). We encourage the Department to sufficiently staff the review process so that this initial notification process can move expeditiously. We encourage the Department to be as specific as possible with the applicant if the Department determines that its application is incomplete.

3. Review Process

Section 15.5(c) provides that the Assistant Secretary may, but is not required to, consult with others, in addition to the applicant. While we fully support the flexibility for the Department to consult with individuals or other entities to assist in the analysis of the information in the application, the regulations should explicitly provide that such consultation will be conducted to the maximum extent practicable without disclosing any of the applicant's proprietary information; if proprietary information must be disclosed, such consultation should be held only with those entities that agree in advance to protect the applicant's proprietary information.

4. Recommendations of the Assistant Secretary

Proposed Section 25.5(d) provides for the actions by the Assistant Secretary. The regulations provide authority for the Assistant Secretary to unilaterally extend the time period for more than ninety days upon notice to the Seller, but without the need to provide any reason or cause of such extension. While we can perceive of situations where information may be in the Department's possession that cannot for national or homeland security reasons be disclosed to the Seller, we encourage the regulations to provide that the Assistant Secretary will use this unilateral extension sparingly and will, to the maximum extent practicable, notify the Seller of both the amount of additional time the Assistant Secretary expects to take and any reason or cause for invoking the automatic extension.

5. Actions by the Under Secretary

Proposed Section 25.5(e) provides for the actions by the Under Secretary. The regulations provide authority for the Under Secretary to unilaterally extend the time period for more than thirty days upon notice to the Seller, but without the need to provide any reason or cause of such extension. While we can perceive of situations where information may be in the Department's possession that cannot for national or homeland security be disclosed to the Seller, we encourage the regulations to provide that the Assistant Secretary will use this unilateral extension sparingly and will, to the maximum extent practicable, notify the Seller of both the amount of additional time the Assistant Secretary expects to take and any reason or cause for invoking the automatic extension.

6. Term of Designation; renewal

Proposed Section 25.5(f) provides for the term of the Designation, proposing a term of five to eight years, as determined by the Under Secretary.[36] One element of this section is the imposition of a five to eight year term on the length of time for a Designation. As noted earlier in our comments, in our view, absent a change in circumstances after the approval of the Designation, there is no public policy reason to impose a fixed period of time on the Designation period of a

[36] 68 F.R. 41430 (July 11, 2003)

QATT. However, if the Department does impose a fixed term limitation, we strongly recommend that it be a uniform, single, fixed period of time, and for as long as possible; under such circumstances, a fixed ten-year term (with authority to extend based on reapplication) would not be inappropriate.

7. Termination of Designation resulting from substantial modification

Proposed Section 25.5(i) provides that a Designation shall terminate automatically, and have no further force or effect, if the QATT is significantly changed or modified. The proposal defined the term "significant change" as one that "could significantly affect the safety or effectiveness of the device," including a significant change or modification. We strongly oppose the automatic termination of the QATT Designation based on significant changes or modifications.

8. Termination of Designation resulting from substantial modification

a. Proposed Section 25.5(i) provides for the automatic termination of a Designation if the QATT is significantly changed or modified. We oppose the automatic termination provision provided for in the proposed rule; nothing in the statute or legislative history requires such automatic termination. Furthermore, by imposing such an automatic termination requirement, none of the entities that are covered by the protections of the Act and regulations will be able to rely on the Designation. Yet, we recognize that the Department's grant of approval is based on information submitted in good faith by an application and reviewed and approved by the Department. On balance, we believe Sellers should be informed that the application could be null and void if there is a significant change or modification and Sellers are encouraged to apply for the Modification of the Designation using the procedures of the Act. However, since the grant of Designation is solely within the jurisdiction of the Department, so to a Designation should be terminated only by the Department based on a finding of significant change, such as if challenged during litigation or at any time if any entity is aware of a circumstance that may indicate a significant change.

b. We also encourage the Department to adopt a shorter, even expedited, review process for an application for modification or a determination of significant change.

9. General

Any interim or final regulation should clearly state that any application process – whether the initial application, an application for modification, or an application for renewal -- will be covered by the provisions of Section 25.8 relating to the confidentiality and protection of information, and recommend that the regulations explicitly state such coverage. We comment below on our suggestions for the treatment of proposed Section 25.8.

E. GOVERNMENT CONTRACTOR DEFENSE

1. Section 863(d) of the Act and proposed Section 25.6 of the regulations address the provisions for Certification of a QATT as issuing a Certificate of Conformance and place the technology on the "Approved Product List for Homeland Security" for purposes of eligibility for the government contractor defense. This is one of the central provisions of the Act that deserves careful attention and clear regulatory guidance.

2. As an initial matter, we assume that the title "approved product list" in the Act and the regulations is not intended by Congress or the Department to exclude services. In our view, since the Act and the regulations intentionally use the term "anti-terrorism technology" as that term is defined in the Act and regulations – that this term specifically includes services.

3. The proposed regulations include a requirement that the Seller provide safety and hazard analyses and other relevant data and information regarding such technology. This is a good example of how the regulations recognize the need to address differently the information that may be available and applicable to products that may not be available or applicable to services. We urge the Department to interpret this statutory provision so that the Seller is only obligated to submit this information if it is relevant and applicable to the technology; such information may not exist for services and should not be a threshold qualification standard for Certification. However, the Department should not share any company-designated proprietary information outside the Department without a specific non-disclosure agreement.

4. Section 25.7 of the proposed regulations addresses the procedures for requesting and granting Certification as an "Approved Product for Homeland Security." The application procedures in the proposed rule for Certification are similar to the application procedures for Designation under Section 25.5 of the proposed rules, and in our view, the processes should be substantially similar. By the same token, PSC's comments relating to the application for Designation in Part E above are also applicable here; we have not repeated them.

5. Section 25.7(a) further provides that an application for Certification may not be filed unless the Seller has also filed an application for Designation for the same technology.[37] The Department permits both an application for Designation and an application for Certification to be filed simultaneously.[38] Section 25.7(f) further requires the Secretary's Designation of a technology under Section 25.3 as a pre-condition for Certification under this Section. We acknowledge the distinction between the two Secretarial approvals.[39] Thus, it is extremely important that the Department specify the Certification application form and the information submission requirements required to accompany a request for Certification, to the maximum extent practicable consistent with the flexibility required to account for the variations in technologies. In the interest of conserving time and maximizing the use of scarce government and Seller resources, we will also encourage Sellers who have an interest in obtaining both Designation and Certification to submit both applications together and urge the Department to review both simultaneously.

6. Finally, any interim or final regulation should clearly state that any consultation that the Under Secretary may consult with as part of the Certification process will be covered by the provisions of Section 25.8 relating to the confidentiality and protection of information, and recommend that the regulations explicitly state such coverage. We comment below on our suggestions for the treatment of proposed Section 25.8.

---

[37] 68 F.R. 41431 (July 11, 2003)

[38] Id.

[39] 68 F.R. 41422 (July 11, 2003) stating "The distinction between the Secretary's two actions is important, however, because the approval process for the government contractor defense includes a level of review that is not required by the Designation of a qualified anti-terrorism technology."

F. SECTION 25.8 CONFIDENTIALITY AND PROTECTION OF INTELLECTUAL PROPERTY

1. We compliment the Department for recognizing the importance of protecting the confidentiality of an applicant's intellectual property, trade secrets and other confidential information.[40] Proposed Section 25.8 provides that the Secretary, in consultation with the Office of Management and Budget, shall establish confidentiality protocols for maintenance and use of information submitted to the Department under the SAFETY Act and this Part. Such protocols shall, among other things, ensure that the Department will utilize all appropriate exemptions from the Freedom of Information Act. [41]

2. We recommend that the heading be revised to read "Confidentiality and protection of information" since the scope of coverage is much broader than just "intellectual property." Furthermore, any interim or final rule should explicitly provide procedures that applicants should follow. For example, we strongly recommend that the Department develop a proprietary data marking or other application notice by which applicants highlight or disclose those portions of its application it considers to be proprietary. The Department would be well advised to adopt the various markings for proposal submissions and/or rights in technical data, already provided for in the Federal Acquisition Regulation and well understood by most contractors and government officials engaged in the federal procurement process.

3. In addition, during the consultation period with potential applicants and until an application is approved, we recommend that the Department treat even the submission of the application as confidential. Once an application is approved, the Department must still recognize the importance of protecting company proprietary information included in the application; in fact, from a homeland security perspective, the Department may even want to protect details about the technology and its potential uses. However, we recognize that the public has an interest in knowing who has received Designation and Certification from the Department and the Department should develop a mechanism of publicly disclosing such information. Here, too, the Department could benefit from adopting procedures used by federal agencies when announcing contract awards of unclassified contracts over a given threshold. These techniques are well understood by agencies contracting, public affairs and FOIA offices.

4. Regardless of the status of an application, the Department should not share any company-designated proprietary information outside the Department without a specific non-disclosure agreement.

G. RELATIONSHIP OF SAFETY ACT TO P.L. 85-804

Section 865(6) defines the term "non-Federal Government customers" to mean any customer of a Seller that is not a federal agency with P.L. 85-804 authority. The Specific Issues discussion highlights the relationship of the SAFETY Act to the indemnification provisions of P.L. 85-804.[42] We compliment the Department for acknowledging both the Congressional and Departmental coverage of the relationship between these two important government contracting

---

[40] 68 F.R. 41423 (July 11, 2003); Specific Issue #3, Protection of Intellectual Property

[41] 68 F.R. 41432 (July 11, 2003)

[42] 68 F.R. 41425 (July 11, 2003); Specific Issue #8, Relationship of the SAFETY Act to Indemnification under P.L. 85-804.

statutes; clearly there are circumstances under which these two acts can, and should, co-exist. However, there is no coverage in the proposed regulations even on procedures that a Seller, a potential Seller, or a federal government customer should follow to more fully understand the relationship between these two acts, the consultation procedures required by Executive Order 13286 (February 28, 2003) and the means for the Secretary to advise whether SAFETY Act coverage would be appropriate. Minimal procedures, such as a new Part 25.10, entitled "Relationship between SAFETY Act and P.L. 85-804," addressing an application form, points of contact within the Department of Homeland Security, and factors that the Department (and possibly OMB) would consider in making the determination would be extremely valuable.

VI. CONCLUSION

1. PSC fully supports the SAFETY Act, and encourages the Department to move expeditiously with interim regulations on key initial sections of the regulations. We strongly support the Department's stated goal of applying the SAFETY Act to any relevant pending federal procurement, and to begin applying the Act to other provisions effective September 1, 2003; thus we urge the Department to not wait for the next phase of rulemaking but to promptly publish the application forms for both Designation and Certification so that prospective applicants may begin their preparations.

2. The Act is clear and unmistakable about its applicability to services. Congress intended that services be treated the same as any other anti-terrorism technology in terms of procedures to be followed and benefits to be conferred. PSC was instrumental in achieving that legislative construct. We appreciate that the Department has followed through on the legislative design by including services in this proposed rule. We recognize and support the fact that the uniform application process for Designation and for Certification may require additional information to be submitted by firms offering services technologies. We also believe, as noted earlier, that additional rulemaking and public discourse is essential if the rule is to meet its full objectives.

3. We urge the Department to move expeditiously on interim regulations focusing on the necessary application procedures and Designation and Certification procedures. In addition, while we compliment the Department's recognition that any information submitted by private sector firms may be proprietary and thus subject to protection, the proposed regulations are silent on the coverage; we strongly urge the Department to "fill in the gaps" by explicitly addressing this critical area through expanded regulatory coverage in addition to the statement of regulatory philosophy. For example, the Department could draw easily from the marking and identification process used in the federal procurement system.

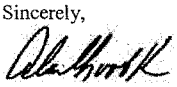
4. While all aspects of the SAFETY Act require full and prompt regulatory coverage, we believe some aspects of the regulatory coverage of the SAFETY Act can be deferred for a few weeks while more critical, short-term aspects, are addressed.

5. We encourage the Department to consider a public meeting to provide a dialogue between the Department and the affected industry communities to further explore key elements of the regulatory implementation.

6. Finally, PSC would welcome any opportunity to work cooperatively with the Department on the further development of the regulations and in monitoring the implementation of the Act and regulations.

We appreciate the opportunity to comment on these proposed regulations. In the interim, if PSC can provide you with any additional information, please do not hesitate to let us know.
I can be reached at (703) 875-8059 or at Chvotkin@pscouncil.org.

Sincerely,



Alan Chvotkin
Senior Vice President and Counsel

AdvaMed Statement to Committee on Government Reform Hearing on Implementing the SAFETY Act September 25, 2003

The Advanced Medical Technology Association is pleased to submit this statement to the Committee on Government Reform regarding the implementation of the SAFETY Act.

AdvaMed, the Advanced Medical Technology Association, represents more than 1,100 innovators and manufacturers of medical devices, diagnostic products and medical information systems. Our members produce nearly 90 percent of the $71 billion health care technology products consumed annually in the United States, and nearly 50 percent of $169 billion purchased annually around the world. Many of these technologies – such as rapid tests to diagnose diseases that may be caused by bioterrorism, gels and foams that can rapidly close wounds, bioengineered skin products for burn victims, and information systems to communicate critical public health information – form an important part of a timely, effective response to terrorist attacks.

Our statement includes background information as well as general and specific comments on the Department of Homeland Security's proposed regulation implementing the SAFETY Act.

Information About AdvaMed's Role in Preparedness

AdvaMed's Technology Preparedness Council

In response to the events of September 11, 2001, AdvaMed established the Medical Technology Preparedness Council to assist federal agencies in ensuring that the health care delivery system is fully prepared. Recently, AdvaMed's Board of Directors approved AdvaMed's participation during times of national emergency in the Department of Health and Human Service's Command Center.

AdvaMed strongly supports the principle of a public-private partnership in the area of preparedness. AdvaMed sponsored a sold-out conference on February 6, entitled "Innovation for Preparedness: the Public-Private Partnership," to strengthen the partnership between the government and the private sector on preparedness and to connect medical technology innovators with appropriate federal preparedness entities. Representatives from key preparedness entities within the federal government, including the Office of Emergency Preparedness (OEP), the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA), the Department of Defense, the National Institute of Allergy and Infectious Diseases (NIAID), the U.S.

Army Medical Research Institute of Infectious Disease (USAMRIID) and the Environmental Protection Agency (EPA) all participated in the conference.

Medical Technology: the Key to a Rapid and Effective Response

Many of the technologies our companies manufacture or are developing are integral to a rapid and effective response to any potential terrorist attack. These include among others:

- **Diagnostic Tests**
- **Vaccine and Drug Delivery Devices**
- **Biochemical Decontamination Technologies**
- **Blood Safety Technologies**
- **Advanced Burn and Wound Care Technologies**
- **Health Information Systems**
- **Basic Medical Technologies**

AdvaMed also supports the Project BioShield initiative and we are pleased that the House and Senate legislation adopted our recommendation to make medical technologies eligible for *all* aspects of Project BioShield, including as qualified countermeasures (i.e., eligible for procurement as part of the national stockpile) and for use in a national public health or military emergency.

General Comments

AdvaMed's membership is committed to helping meet the nation's preparedness needs in the health care arena. Our manufacturers routinely overcome significant biomedical challenges in order to detect diseases earlier and to offer new, more effective treatment options for patients. However, we agree with the Department's conclusion that "the current development of anti-terrorism technologies has been slowed due to the potential liability risks associated with their development and eventual deployment."

There are numerous challenges *and* additional liability risks in the area of bioterrorism preparedness including:

- Pathogens that have been deliberately engineered to cause harm and that may progress unpredictably.
- An inability to obtain needed human clinical data prior to a bioterrorist attack for some medical devices.
- Developing tests to detect and technologies to treat dangerous pathogens will require significant investments in biocontainment equipment and processes.
- Because of the potential chaotic nature of a bioterrorist attack, the normal mechanisms for communicating intended use, contra-indications, etc. to those who will be using or administering the technologies will be much more difficult and challenging.

All of these challenges could potentially translate into additional and substantial liability risks for medical technology manufacturers.

We would also note that the intent of Congress in enacting the statute was to extend the protections of the SAFETY Act to products that can be used to prevent or respond to a terrorist attack, even if these same products can be used in other circumstances. Such protection may be necessary to encourage companies to deploy basic medical technology and to plan for its use in the event of attack. Consequently, the final rule should make clear that basic medical technology is eligible for the protections of the Act even though it can be used to treat illness and injury in many situations in addition to terrorist incidents.

Specific Comments

Preamble

 # 8 Relationship of the SAFETY Act to Indemnification under Public Law 85-804

Because of the potential for substantial liability risk associated with the development and deployment of medical technologies used both in advance of and during a potential terrorist attack, AdvaMed is very concerned about limitations in liability protection caused both by the Department's proposed interpretation of the SAFETY Act and by apparent limitations in the SAFETY Act itself.

We believe that there is support for an interpretation of the SAFETY Act that allows manufacturers of qualified anti-terrorism technologies to have access to both the liability protections of the SAFETY Act and to the indemnification protections of P.L. 85-804 which allows the Government to indemnify private parties acting on the Government's behalf. A broader, rather than narrower interpretation of the relationship of the SAFETY Act to P.L. 85-804 is especially critical given that it appears that the liability protections of the SAFETY Act only apply to actions taken in response to "an act of terrorism," not those that are taken preemptively or preventatively, such as in a vaccination program.

Specifically, former Representative Richard K. Armey, who chaired the House Special Committee on Homeland Security and was a key figure in drafting and shepherding the Homeland Security Act through Congress, spoke to the Congressional intent behind the SAFETY Act in comments made on the record. As noted in the preamble, Rep. Armey stated that "all of the liability reforms and litigation measures of the SAFETY Act are intended to complement other government risk-sharing measures that some contractors can use such as Public Law 85-804. Thus, in those situations both types of measures could apply." Importantly, Rep. Armey did not delineate any restrictions on the use of P.L. 85-

804 when manufacturers availed themselves of the protections of the SAFETY Act.

While provisions may be in place to provide liability protections to certain vaccine manufacturers, there are a number of other technologies that might be used preemptively or preventatively to protect citizens in advance of an act of terrorism. These products would be covered by the Act in the event of a terrorist attack and resulting liability claims. However, they would not be covered by the SAFETY Act in the event that liability claims were brought in other circumstances. Yet, because they "could" qualify under the SAFETY Act, the proposed rule suggests that they would ordinarily not be eligible for the indemnification provisions of P.L. 85-840 under any circumstances. At the very least, there should be a presumption that these products would be eligible for the protections of P.L. 85-804 for liabilities resulting from non-terrorist incidents.

AdvaMed's concern is that enactment of the proposed regulations might heighten, rather than relieve, the potential liability of sellers by making it harder to avail themselves of the protections of P.L. 85-804 to which they might otherwise be entitled.

For these reasons, we urge the Department to employ a broader rather than narrower interpretation of the relationship between the SAFETY Act and P.L. 85-804, and make it clear that P.L. 85-804 can continue to be used, particularly for those technologies that will be used preemptively or preventatively.

Text of the Proposed Rule

§ 25.3(a)(1), § 25.3(c) § 25.3(e), § 25.6 – Determinations of Safety and Effectiveness

The proposed rule contains several sections dealing with the determination of safety and effectiveness of products before they can qualify for the protections of the Act, including the government contractor defense. Section 25.3(a)(1) provides that one criterion for qualification is prior Government use or "demonstrated substantial utility and effectiveness." Section 25.3(c) provides that DHS may develop safety and effectiveness standards for products. Section 25.3(e) provides that the Under Secretary of DHS may consider any "scientific studies, testing, field studies, or other experience with the technology that he deems appropriate and that are available or can be feasibly conducted…." Section 25.6 provides that, in determining whether to designate a product as eligible for protections of the government contractor defense, DHS will "conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended."

In applying all these provisions, we urge DHS to consider the role of the FDA in regulating medical devices. All medical devices require FDA premarket approval or premarket notification prior to marketing.

The complex marketing approval process for medical devices, codified in the Medical Device Amendments of 1976, was enacted by Congress in 1976 after extensive debate and careful review (see, e.g., H.R. Rep. No. 853, 94th Cong., 2d Sess. (1976)). Congress identified different categories of devices based on the level of risk that they presented and the appropriate level of control for each category. This regulatory scheme takes into account the benefits to the public from regulatory controls as well as the costs of regulation for both manufacturers and the government. The goal of this regulatory process is to ensure that all medical devices are safe and effective. In addition, Project BioShield clearly contemplates FDA approval or review for medical technologies developed under that program.

Although the proposed rule appears to contemplate that DHS will consider the conclusions of a federal regulatory agency, the proposed rule does not expressly state that DHS will accept the conclusions of the FDA or any other federal agencies regarding the safety and effectiveness of particular products. We urge DHS to state expressly several policies, which we believe are consistent with Congress's intent in enacting the SAFETY Act as well as the interests of the public in being able to take advantage of products that can reduce the harm of terrorist attacks. First, the rule should make clear that the extensive and comprehensive review and approval process of FDA will satisfy any requirement that a product is effective for purposes of the basic determination in section 25.3(b). Second, DHS should not develop safety and effectiveness criteria under section 25.3(c) in addition to or as a substitute for such standards. Review and approval of medical technologies according to a different set of safety and effectiveness standards will unnecessarily delay access to needed medical technologies for preparedness purposes, and create confusion regarding appropriate standards.

Third, for purposes of section 25.3(c), DHS should not determine that additional testing is required once FDA approval has been made even if additional tests are theoretically "feasible." Finally, FDA approval should satisfy the requirement in section 25.6 that products must be safe and effective in order to receive the benefits of the government contractor defense.

§ 25.3(d) – Consideration of substantial equivalence

Similar considerations apply in the application of § 25.3(d) regarding substantial equivalence. The notion of substantial equivalence is well-established and well defined in the medical device authorities in the Federal Food, Drug and Cosmetic Act. Substantial equivalence has been utilized since medical devices began to be regulated in 1976 and has helped to expedite through the regulatory process,

review and approval of incremental improvements in medical devices. Again, we believe and recommend that the extensive and comprehensive FDA review process should satisfy and substitute for any substantial equivalence process established by DHS. Review and approval of medical technologies according to a different set of review criteria will only delay access to needed medical technologies for preparedness purposes[1].

§ 25.3(b)(3) – Criteria to be considered

This section discusses "extraordinarily large" or "extraordinarily unquantifiable" potential third party liability risk but does not provide any guidance about how such a standard would be measured or defined. We would urge greater definition of these terms and would further recommend that where the manufacturer is the only party in the chain of product use that is not covered by some form of immunity or other liability limitation, that this fact be construed as a form of extraordinary risk.

§ 25.4 (a) - (b) – Provisions on liability insurance

By requiring "any person or entity that sells or otherwise provides a qualified antiterrorism technology to Federal and non-Federal government customers" to "obtain liability insurance of such types and in such amounts" "to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed . . .," the proposed regulation appears to assume that manufacturers insure their products on a product-by-product basis. However, medical device manufacturers typically self-insure or purchase insurance that covers the manufacturer's operations. Given the tremendous potential liabilities associated with medical technologies used in a bioterrorist attack, there is no assurance product-specific insurance will be available.

Given the possibility that a manufacturer may not be able to obtain any liability insurance at all for a particular technology or product, this section should include an indication of how much self-insurance may or may not be required in such an instance, and a statement of what measures a manufacturer would have to provide in order to demonstrate that it had made a good faith attempt to obtain liability insurance.

Alternatively, the regulations could provide for allowing an appropriate portion of a manufacturer's company-wide insurance policy to be designated for the qualified anti-terrorism technology.

[1] See Statement Regarding the Demonstrations of Effectiveness of Human Drug Products and Devices, 60 Fed. Reg. 39,180 (1995).

§ 25.4 (c) Liability of Sellers

The Preamble in Paragraph 5 states that "only one Federal cause of action exists for loss of property, personal injury, or death when a claim relates to performance or non-performance" and "such cause of action may be brought only against the Seller." We agree with this interpretation of the Act. It appears clear that Congress intended to limit product liability litigation in the event of a terrorist attack by ensuring that liability insurance is available to compensate victims and to limit the exposure of a single entity – the Seller – to the limits of its liability insurance. This conclusion is extremely important because it creates an incentive for qualified Sellers as well as others in the manufacturing and distribution chain of a Seller to provide products or components. By limiting the cause of action to Sellers, other parties can determine whether they need liability insurance and how they should take into account possible liabilities in making basic business decisions.

Unfortunately, because of ambiguity in the legislation, the proposed rule is internally inconsistent by providing in §25.4(c) that Sellers must obtain liability insurance to protect, "to the extent of their liability," contractors, subcontractors, suppliers, vendors and customers of the Seller and of the customer. This language undercuts the clarity of the statement in the rule that only Sellers can be liable for suits stemming from terrorist incidents. As a result, the proposed rule does not provide a clear regulatory interpretation, which can guide courts in their interpretation of the statute. The benefits of a clear rule limiting liability to a single entity are, if not lost altogether, at least undercut.

We recognize that the inconsistency in the rule stems from the ambiguity of the statutory language and that DHS cannot simply ignore the text of the statute. However, we believe Congress's intent was simply to guard against any possibility that another entity would be held liable, notwithstanding the intent of Congress to limit liability to the Seller. Thus, we urge the Department to state expressly that the provision requiring coverage of other parties is only intended to protect against a misapplication or misinterpretation of the principle of seller-only liability and, thus, the potential liability of another party should be rare.

§ 25.4(d) – Third party claims

This section has the effect of limiting the liability protections in the SAFETY Act to only those situations "arising out of, relating to, or resulting from an act of terrorism when the applicable qualified anti-terrorism technologies have been deployed in defense against, response to, or recovery from such act." As we noted above, this will substantially and unrealistically limit liability coverage to only those situations where a qualified technology is directly deployed in a terrorist attack and it will prevent needed liability coverage for technologies used preemptively or preventatively to help protect against such terrorist attacks.

§ 25.6 – Government Contractor Defense

As we noted above, FDA's extensive and comprehensive review and approval process should be sufficient to certify the manufacturer as a "government contractor" eligible for the rebuttable presumption. Further, in the event a seller applies for the rebuttable presumption, we recommend that the Department establish an expedited review process under which prior designation as a qualified anti-terror technology and FDA approval or clearance would create a rebuttable presumption that the seller should be certified as a "government contractor" for purposes of this section.

In closing, we look forward to working closely with the Committee and the Department to ensure that we make significant progress in enhancing our nation's ability to prevent, detect, and treat threats to public health and safety from terrorism.