HELPING BUSINESS PROTECT THE HOMELAND: IS THE DEPARTMENT OF HOMELAND SECURITY EFFECTIVELY IMPLEMENTING THE SAFETY ACT?

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

JOINT WITH THE

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 13, 2006

Serial No. 109–100

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

35–622 PDF WASHINGTON : 2007

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTE ON EMERGENCY PREPAREDNESS, SCIENCE, AND TECHNOLOGY

DAVE G. REICHERT, Washington, *Chairman*

LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, New York *(Ex Officio)*
BILL PASCRELL, JR., New Jersey
LORETTA SANCHEZ, California
NORMAN D. DICKS, Washington
JANE HARMAN, California
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

MIKE ROGERS, Alabama, *Chairman*

JOHN LINDER, Georgia
TOM DAVIS, Virginia
KATHERINE HARRIS, Florida
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*
KENDRICK B. MEEK, Florida
EDWARD J. MARKEY, Massachusetts
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

The Honorable Dave Reichert, a Representative in Congress From the State of Washington, and Chairman, Subcommittee on Emergency Preparedness, Science, and Technology:
Oral Statement 25
Prepared Statement 26
The Honorable Bill Pascrell, Jr., a Representative in Congress From the State of New Jersey, and Ranking Member, Subcommittee on Emergency Preparedness, Science, and Technology 4
The Honorable Mike Rogers, a Representative in Congress From the State of Alabama, and Chairman, Subcommittee on Management, Integration, and Oversight:
Oral Statement 1
Prepared Statement 2
The Honorable Kendrick Meek, a Representative in Congress From the State of Florida, and Ranking Member, Subcommittee on Management, Integration, and Oversight 2
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Oral Statement 21
Prepared Statement 22
The Honorable Donna M. Christensen, a Delegate in Congress From the U.S. Virgin Islands 33
The Honorable Charlie Dent, a Representative in Congress From the State of Pennsylvania 20
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washington 28
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas 29

WITNESSES

PANEL I

The Honorable Jay Cohen, Undersecretary for Science and Technology, U.S. Department of Homeland Security:
Oral Statement 6
Prepared Statement 9
Accompanied by:
Ms. Linda Vasta, Acting Director, Office of SAFETY ACT Implementation .. 29
Ms. Elaine C. Duke, Chief Procurement Officer, U.S. Department of Homeland Security:
Oral Statement 12
Prepared Statement 14

PANEL II

David Z. Bodenheimer, Esq., Crowell & Moring LLP:
Oral Statement 59
Prepared Statement 60

Page

Mr Brian E. Finch, Esq., Dickstein Shapiro LLP:
Oral Statement 52
Prepared Statement 54
Mr. Andrew Howell, Vice President, Homeland Security Policy Division, U.S. Chamber of Commerce:
Oral Statement 34
Prepared Statement 35
Mr. Michael M. Meldon, Executive Director, Homeland Security and Defense Business Council:
Oral Statement 39
Prepared Statement 42
Mr. Stan Z. Soloway, President, Professional Services Council:
Oral Statement 45
Prepared Statement 48

APPENDIX

QUESTIONS AND RESPONSES

Ms. Elaine Duke Responses 75

HELPING BUSINESS PROTECT THE HOMELAND: IS THE DEPARTMENT OF HOMELAND SECURITY EFFECTIVELY IMPLEMENTING THE SAFETY ACT?

Wednesday, September 13, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON MANAGEMENT,
INTEGRATION AND OVERSIGHT,
JOINT WITH THE
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittees met, pursuant to call, at 10:10 a.m., in Room 2175, Rayburn House Office Building, Hon. Mike Rogers [chairman of the Subcommittee on Management, Integration and Oversight] presiding.

Present: Representatives Rogers, Reichert, Linder, Dent, Thompson, Pascrell, Meek, Dicks, Jackson-Lee, and Christensen.

Mr. ROGERS. [Presiding.] This joint hearing of the Homeland Security Subcommittee on Management, Integration and Oversight and the Subcommittee on Energy Preparedness, Science and Technology will come to order.

I am pleased to join our colleagues on the other subcommittee in this joint subcommittee hearing on the implementation of the SAFETY Act.

Let me first begin by welcoming our panelists of distinguished witnesses and thank them for taking time out of their busy schedules to be with us today.

The SAFETY Act was enacted in November 2002 as a part of the Homeland Security Act. At that time, it was the intent of Congress to spur the development and deployment of innovative antiterrorism technologies.

The bill does this in part by limiting the liability exposure of the companies that provide these technologies in the event of a terrorist attack. Since the law was enacted, however, the number of applications to DHS for SAFETY Act protection has fallen well below expectations.

Critics have charged that this disappointing performance is due to a number of factors, including the department's slow evaluation and approval process, understaffing in key offices, and lingering questions about the act's ability to shield technology providers from liability.

This summer DHS issued a final rule to implement the SAFETY Act as well as a revised application kit with a goal of addressing many of these private-sector concerns.

The feedback we have received from industry about the revised process has been mostly positive. I look forward to hearing from our witnesses more about these recent changes and whether they address the key questions.

First, is the application and review process swift, efficient and effective? Second, how can DHS more closely integrate the application and review process with the department's procurement of antiterrorism technologies and services? And third, is there sufficient awareness of and confidence in the protection provided by the SAFETY Act in the public and private sectors?

I want to again thank the witnesses for joining us today, and I look forward to their testimony on this important subject.

PREPARED OPENING STATEMENT OF THE HONORABLE MIKE ROGERS

I am pleased to join Chairman Reichert in holding this joint subcommittee hearing on the implementation of the SAFETY Act.

Let me first begin by welcoming our two panels of distinguished witnesses, and thank them for taking time out of their busy schedules to be with us today.

The SAFETY Act was enacted in November 2002 as part of the Homeland Security Act.

At that time, it was the intent of Congress to spur the development and deployment of innovative anti-terrorism technologies.

The bill does this, in part, by limiting the liability exposure of companies that provide those technologies in the event of a terrorist attack.

Since the law was enacted, however, the number of applications to D–H–S for SAFETY Act protections has fallen well below expectations.

Critics have charged that this disappointing performance is due a number of factors, including:

- the Department's slow evaluation and approval process;
- under-staffing in key offices;
- and lingering questions about the Act's ability to shield technology providers from liability.

This summer, D–H–S issued its final rule to implement the SAFETY Act, as well as a revised Application Kit, with the goal of addressing many of the private sector's concerns.

The feedback we've received from industry about the revised process has been mostly positive.

I look forward to hearing from our witnesses more about these recent changes, and whether they address three key questions.

First, is the application and review process swift, efficient, and effective?

Second, how can D–H–S more closely integrate the application and review process with the Department's procurement of anti-terrorism technologies and services?

And, third, is there sufficient awareness of—and confidence in—the protections provided by the SAFETY Act in the public and private sectors?

I want to again thank the witnesses for joining us today, and look forward to their testimony on this important subject.

I now yield to the Ranking Member, Mr. Meek, for any statement he may have.

I now yield to the ranking member, Mr. Meek, for any statement that he may have.

Mr. MEEK. Thank you, Mr. Chairman.

I would like to welcome Secretary Cohen and also Chief Procurement Officer Duke back to the committee, along with the representative from the SAFETY Act office.

And also, to the second panel, we want to also welcome you to the committee and look forward to your testimony.

The idea behind the SAFETY Act was to encourage development and the deployment of cutting-edge homeland security technologies

that would not otherwise have been procured. For the past 3 years, Homeland Security has not really had a system in place to administer the program.

It has been frustrating to watch the lack of activity in the SAFETY Act office. That is why I was pleased to hear that the department has issued a new rule and application kit.

Initial feedback on the new kit seems to be positive. I am told that the application kit looks easier to fill out, and the overall process appears to be less burdensome.

At the same time, we don't want to come to the podium and go too far away from the original intent of the SAFETY Act. And I think that the application—the application states for the technology that has been inquired or utilized in the past on ongoing procurement would be significantly expended.

I think also it is important that the testimony that we have here today would hopefully push us in the direction that we want the SAFETY Act to move in.

Also, Mr. Cohen, I am looking forward to your testimony as it relates to the future of the SAFETY Act and the integrity of the SAFETY Act and making sure that it sets out to move in the direction that we need to move in of how the original act called for to be moved in.

I want to say, because we have these committees, and sometimes it is very frustrating to come and spend time in these subcommittees, and we don't hear exactly what you need for us to know.

I know that we have public-and private-sector members on the second panel. I would ask that panel to share with us what we need to know, not what you may think we want to hear, but what we need to know.

Both of these subcommittees have been pulled together today to be able to make sure that the process move forward. As you know, Ranking Member Thompson and a number of other members of the subcommittee and the overall committee asked for some forward progress as it relates to the SAFETY Act implementation.

So you can see the chart that is behind you that we really didn't have any action until this year, and many members of the private sector who want to assist us in our technology field also wanted to be covered by what the SAFETY Act provides, the blanket of not—of the whole liability issue.

They had some level of frustration, but from what I am hearing now they feel that it is a new day. We want to make sure that the sun continues to shine.

So, Mr. Chairman, I look forward to the testimony. And I know the chairman and I have two committees going on at the same time—two of us have a committee going at the same time, Armed Services, where they are going to be having some votes a little later on, and so we will be going in and out as those votes are called.

But our staff will be here to be able to hear the kind of input that we need to hear to be able to allow us to continue to assist not only the department but the private sector in the technology field to help us protect Americans.

Mr. Chairman, with that I yield back.

Mr. ROGERS. I thank the gentleman.

The chair now recognizes the ranking member of the Subcommittee on Emergency Preparedness, Mr. Pascrell, for any statement he may have.

Mr. PASCRELL. Thank you, Mr. Chairman.

I want to thank Mr. Reichert—he will be here with us shortly—as well as yourself and Ranking Member Meek for helping to convene this meeting.

I want to welcome our witnesses. We have met several times, talked about things that are at hand. I believe that all of you appearing before us today are exemplary public officials. And I really appreciate the fact that you have been pretty straightforward. Please don't change.

I think that this hearing is pretty critical. The Support for Antiterrorism by Fostering Effective Technologies Act of 2002 provides critical incentives for the development and deployment of antiterrorism technologies for homeland security.

The success of this act, the SAFETY Act, is a vital component to our nation's homeland security efforts. The SAFETY Act limits the liability of providers of qualified antiterrorism technologies for claims arising out of, relating to or resulting from an act of terrorism.

It was Congress's intent that the SAFETY Act would address businesses' liability concerns and pave the way for innovative development. We want to encourage that and foster it so that we could develop key antiterrorism technologies.

Industry remains skeptical about the burdens imposed by this act—I can understand that—and the durability of the legal protection that the act provides. We have to be, I think, very definitive about this.

Today's hearing will give us a good perspective as to what has been done and what further needs to be accomplished in order to make this act as effective as possible. To be sure, some recent success has indeed been instituted.

I want to join many of us here by commending the department and the general counsel's office for putting out the final rule—it has only been 4 years—and the new application kit for the SAFETY Act certification.

My understanding—correct me if I am wrong—is that the initial reaction from applicants is that this is a much-improved kit, it will be easier to fill out, to apply, to do what we want to do, to have innovation, to think, to use our imaginations, easier to understand—I mean, the last was a disaster—and require fewer burdens than the previous kit that we saw.

The final rule also does a very good job of clarifying an array of key problems that arose from the earlier rules. However, as is often the case, there is still unfinished business. The SAFETY Act is intended to influence the production of technologies that otherwise would not have been produced.

But the department states in the application kit that, "It may be very important and could significantly expedite your application if your technology has been acquired or utilized or is subject to an ongoing procurement."

This brings forward the concern of many of us here today, that the department may view the act as a blanket liability waiver for every technology.

Additionally, the language as it is written makes me worry that the department wishes to encourage companies to invest their research dollars in antiterrorism technology ready to be fielded now rather than in breakthrough technologies that may offer a needed transformation in the way we combat the war against terror.

Industry still seems to harbor some serious reservations and doubts about the ability of the department to keep and safeguard sensitive business concerns and confidentiality. I am puzzled about that area of confidentiality, to be very truthful with you.

Many have expressed deep dissatisfaction with the department's stated policy with regard to safeguarding proprietary information submitted as part of the SAFETY Act application. And I want to hear, hopefully, how the department intends to assure applicants that their proprietary information will be, in fact, kept confidential.

We have also heard that while there are dozens of contractors from the general counsel's office helping to move the SAFETY Act forward, there is only one full-time employee actually working at the SAFETY Act office. Am I correct in stating that?

If true, that is unacceptable, as we intended the legislation. Either the Congress or the department needs to address the problem immediately.

Lastly, it does appear that the link between the SAFETY Act office and the procurement office in DHS must be improved. If a product meets a test for procurement officials, there is no reason why the SAFETY Act office should have to run through an entirely new and an entirely superfluous process to test the effectiveness of the product. If I am wrong, teach me. I am educable, believe it or not.

In the fight against terror, we must be quick and nimble. We can never forget that. If we can get the SAFETY Act to an optimal operating level, our nation will be well served. It is the austere responsibility of this committee and the witnesses before us to ensure that this happens.

I want to thank the chairman. In this critical oversight hearing I look forward to a robust discussion.

Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentlemen.

The other members are reminded that opening statements may be submitted for the record.

We are pleased to have with us two distinguished panels. And let me remind the panelists, all panelists, that your full opening statement will be submitted for the record, so if you would like to abbreviate it in your opening oral remarks, that would allow more time for questioning.

Also, I would like to, before we empanel the first panel, ask for unanimous consent that the acting director of the Office of SAFETY Act Implementation, Ms. Linda Vasta, be empaneled along with Mr. Cohen to assist in answering questions.

Without objection, welcome, Ms. Vasta.

The chair now calls the first panel and recognizes the Honorable Jay Cohen, undersecretary for science and technology for the U.S. Department of Homeland Security.

Welcome, Mr. Cohen. We look forward to your statement.

STATEMENT OF HON. JAY COHEN, UNDERSECRETARY FOR SCIENCE AND TECHNOLOGY, DEPARTMENT OF HOMELAND SECURITY

Mr. COHEN. Well, good morning, Chairman Rogers, Chairman Reichert, Congressman Meek and Congressman Pascrell and the other distinguished members of the subcommittees.

It is a distinct pleasure for me to be here today to discuss the Department of Homeland Security Science and Technology Directorate and, in particular, our implementation of the SAFETY Act.

Mr. Chairman, you have already indicated very kindly that my written testimony will be mad a part of the record. And thank you so much for accommodating having Ms. Linda Vasta at the table with me. As you know, I have been in the saddle now for about 1 month. I am not lawyer, and I am not an expert.

And as Congressman Pascrell has already indicated, I try and use straight talk, and I am learning very quickly about the SAFETY Act, but I have much more to learn.

And so with that, I will abbreviate my comments so that we provide more time for your very important questions in the time that is allotted.

I always like to start off by reminding the people who are listening, because I know the members are very well aware of this, of why we are here, who we enable, what we are all about. And we just recognized—I don't want to say celebrated—the fifth anniversary of the tragic events of that terrible day, the 11th of September, 2001.

We would not have the Department of Homeland Security if it were not for that event. As I testified previously, I thank the Congress and the administration so much for establishing that department. And now we need to make it more effective as each day goes on.

I have already talked about Linda Vasta. I am also pleased to have sitting to my left Ms. Elaine Duke. She is our chief procurement officer at the Department of Homeland Security. We work very closely together. I must tell you, I feel a little bit like a thorn amongst the roses here. But I am honored to be sitting at the same table as them.

I am pleased to discuss the progress that we have made on the implementation of the SAFETY Act. Congressman Meek has already addressed the histogram that I have to my right.

Because I am the new kid on the block, I will not take credit for that, but I will give credit to Secretary Chertoff and Deputy Secretary Michael Jackson who have given this the attention that it has required and deserves.

And sitting behind me is Mark Rosen, who is my general counsel, who likewise has been fully engaged in this. I will tell you, ladies and gentlemen, that barely a day goes by at the end of the day that Mark Rosen doesn't come in with a new SAFETY Act for my review and approval, and that is how we get this kind of progress.

It was interesting and it was serendipitous that on the 11th of September, on Monday, we approved the 100th SAFETY Act technology since initiation of the SAFETY office. There are currently 40 cases undergoing technical review.

So in the short time I have been on board with the pending case load—we have a responsibility, as you have indicated, to earn the trust of industry and the American people. We must ensure that the SAFETY Act is a credible program and that we are in this for the long haul.

The new rule and the new application kit have already been addressed. Although I am not from Oklahoma, I do believe in "show me," and so I went to Google, and I just typed in "SAFETY Act" to see what I would find. And lo and behold, number one on the list—and we don't pay Google; we are not one of the paid advertisers—is www.safetyact.gov.

And then I went to that Web site, which is the new, improved Web site that you have already talked about. In the Navy, we always talk about the Major Smith test. I am not trying to be derogatory to the Army or the Air Force, but the Major Smith test is when we think we have a good idea, we give it to an uninitiated person to see does it really pass the common sense check.

And that is what I was attempting to do. And so then I went to download the application. It is 93 pages on Adobe. I am not trying to give an ad here to them, but it came up very quickly, and I printed out the table of contents and then worked my way through as if I were an offerer. And I appreciate very much your comments.

I would also like to say good morning to Congressman Thompson, and I apologize. We have not had the chance to meet personally before this, but I look forward to that very much, sir.

So I have done the Major Smith test, and I am comfortable with the feedback that we have been receiving on that new application.

One of the major provisions of the final rule is moving the time line from 150 days to 120 days. I see that as an outer limit. I believe that we can do better.

And we will, I am sure, as part of answering questions, address the issue of staffing, manning, process and metrics. But all of the trends, all of the vectors, I believe, are in the right direction.

I had a chance to testify before Chairman Reichert and Congressman Pascrell's committee last week on the realignment of the S&T Directorate, which was approved last Wednesday, by Secretary Chertoff, and I briefed all of my people yesterday, all hands, on that. It is now in place.

We will be updating the Web site so people will know who to come to independent of the SAFETY Act with their technologies, et cetera. But as part of that brief, I indicated we would have six departments and three cross-cutting—three matrix directors, one for transition, one for innovation—that is HSARPA—and one for research. Those are the laboratories and the universities.

Because my director of transition in an integrated process team will sit as a team member first with the customer, whether that is TSA, Customs and Border Protection or the directorates in Homeland Security, and sit across the table from Ms. Duke's acquisition professionals, I believe that the best alignment for the SAFETY Act Implementation Office is under my director of transition.

That is a senior executive service person. He is very familiar not only with Homeland Security but also the entire output portfolio of my directorate. And so that is the direction in which I am proceeding.

There has been discussion here of being nimble. I prefer to use the word agile. Our enemy is agile. Our enemy is devious. They stop at nothing to achieve their goals. And I believe we have to be as motivated, and I hope to bring that intensity and enthusiasm to my directorate.

I will tell you that I am extremely honored to be here today representing those good men and women, government service, interagency personnel act, detailees from our laboratories, industry and our contract staff who make the S&T Directorate the organization it is today.

I will work to make it a world-class S&T management organization that is both effective and agile and meets and exceeds the desires of the Congress and the administration and the implementation of the law.

Having said that, as good as we think the final rule may be, and as good as we think the improvements in the new application kit are, we still have to listen, and we should listen, and I look forward to listening to our customer, and our customer, of course, are industry. They are the R&D and the S&T component of this incredible country.

And so I look forward to staying and listening to the comments and the recommendations of the second panel. One of the things that I think you will hear from that panel, and I will conclude my remarks, are on the 10th of August, the day that I was sworn in by Secretary Chertoff, the liquid explosives plot against airlines flying from England to the United States broke.

That sort of became the focus of my life around reorganizing, realigning the department and all the other things that we have accomplished in the last month.

But it was clear to me that when you looked at the threat, you looked at the inconvenience to the traveling public, the economic impact, that we had to address, as I call it, the wolf that is closest to the door.

Now, in the area of terrorism and technologies, there are many wolves on the porch. But our public expects us to respond, and so the very next day, on the 11th of August, I established the rapid response team for liquid explosives.

We assigned a program manager. We assigned a scientist who understood the chemistry, had worked with the Israelis, with the Brits, and with our laboratories. And also, we brought the Transportation Security Laboratory of Atlantic City to the table.

We had communications immediately with all of our Department of Energy laboratories, which you have so graciously given me access to, for their technology and their science and their innovation.

And we brought in some of the representatives who will be on this second panel today, but we invited industry representatives. And we went out with a request for information. We have over 40 responses today. It closed yesterday.

We are move forward very quickly, within 30 days, to test these technologies to detect the liquid explosives of concern.

But in a proactive way, for the first time—and this was leadership direction at Homeland Security; it was not my idea, but I am very pleased to have implemented it—we used the SAFETY Act in a proactive way where we informed all the applicants that they would get SAFETY Act protection for their technologies.

So with that, I will conclude my comments. Again, it is an honor to be here. I look forward to your questions. And I think that Ms. Duke may have a short statement also.

[The statement of Mr. Cohen follows:]

FOR THE RECORD

PREPARED STATEMENT OF THE HONORABLE JAY M. COHEN

SAFETY Act Testimony

Good Morning Chairman Rogers, Chairman Reichert, Ranking Members Meek and Pascrell, and distinguished Members of the Subcommittees, it is a pleasure to be with you today to discuss the Department of Homeland Security (DHS) Science and Technology Directorate (S&T Directorate) and in particular our implementation of the SAFETY Act program. I appreciate your invitation to discuss our programmatic accomplishments and my vision of how the Directorate can improve the use of the SAFETY Act to meet the mission needs of our customers—the DHS Components—and the technology providers that will make use of the SAFETY Act to enable them to field technologies that will make the Nation safer. I similarly appreciate the important role that the SAFETY will continue to make in eliminating barriers to full participation by the private sector in developing and fielding new types of anti-terrorism technologies.

I am honored to have this opportunity and privilege to serve with the dedicated men and women, scientists, engineers, and professionals who are working to secure our homeland and defend our freedoms. While the SAFETY Act program is still a work in progress, I am very proud of what has been accomplished in a relatively short time. I have with me today Linda Vasta who is the Acting Director of the Office of SAFETY Act Implementation. I will look to Linda to help respond to any questions of the Committee that call for specific facts and figures about how the program is performing.

The S&T Directorate has a significant role in bringing to bear solutions to the Department's homeland security challenges. During my tenure at the Office of Naval Research, especially after 9–11, I learned first hand the incredible value that a sustained, customer focused basic and applied research program adds to America's ability to bring advanced technology to our (and our allies) asymmetric advantage against the enemies of freedom. It can mean the difference between life and death, victory and defeat. DHS's enabling legislation, the Homeland Security Act of 2002, established a separate Science and Technology Directorate with a well-defined mission in recognition of the importance of robust science and technology programs in the War on Terrorism. I intend to move the S&T Directorate forward by instilling efficient processes, ensuring accountability and empowering people to conduct the important work of the Directorate. The SAFETY Act plays a key role in enabling the fullest possible participation of industry in this effort.

The SAFETY Act (Support Anti-terrorism by Fostering Effective Technologies Act) was enacted as part of the Homeland Security Act of 2002. The mission of the SAFETY Act is to facilitate the development and deployment of qualified anti-terrorism technologies by creating a system of risk and litigation management. These protections apply to a company when the worst happens—an act of terrorism. The SAFETY Act is intended to ensure that the threat of liability does not deter potential manufacturers or sellers of anti-terrorism technologies from creating or providing products and services that could save lives.

The last year has been a time of significant growth and improvement for the SAFETY Act program, building on the S&T Directorate's proactive efforts to develop the program since the Department was created in 2003. The increase in the number and types of technologies extended SAFETY Act protection has been impressive. Since September of 2005, DHS has issued 60 award decisions. As you can see from the chart, over last three years, the growth is strong and continues to climb. We currently have issued SAFETY Act Designations or Designation/Certifications to over 100 companies that are developing Qualified Anti-Terrorism Technologies. While I am encouraged with the trend indicated by these numbers, I believe we can

more fully utilize what is an important homeland security tool. However, I wish to report several developments that (i) reveal the Department's commitment to improving upon efforts to date, (ii) indicate that progress is being made, and (iii) should with time greatly increase the number of companies applying for and receiving SAFETY Act protection.

The first improvement is the promulgation and implementation of the SAFETY Act Final Rule, which became effective on July 10, 2006. The terms of the final rule reflect lessons learned and experience gained from our operational experience and provide for a more efficient and user-friendly application process. They also reflect the many comments and suggestions that were made by the private sector and industry experts while the program operated under the Interim Rule.

Perhaps the most dramatic change in the Final Rule is the reduction of the evaluation cycle from 150 days to a maximum of 120 days, while maintaining the same quality level of analysis. Expediting this process is vital for the companies who cannot wait months for decisions to be made when their capital and intellectual property is on the line. Our hope is that our elimination of 30 days from the review cycle sends an important signal to the private sector that we are committed to their success and improves their overall experience with the application process. Moreover, I expect that decisions on certain applications will be made in time frames far shorter than 120 days, and assure you that, in any event, the 120 day regulatory cycle will be strictly adhered to. Since coming on board, I have learned that the Department's track record in processing applications within the SAFETY Act's regulatory deadlines is troubling. I have learned that, through the practice of issuing numerous "requests for information," in some cases the Department might have caused unnecessary delay and imposed undue burdens on applicants. This is not consistent with my goals for a full service, efficient, and customer oriented organization. Going forward, the Department will strictly adhere to regulatory deadlines and will ensure that only information necessary to reach a decision on an application will be required. Time is of the essence. Furthermore, I will, while preserving the integrity of the technical review process, continue to look for ways to improve the program's level of efficiency and further reduce the SAFETY Act application evaluation cycle.

Already, the Office of Safety Act Implementation (OSAI) and the Office of the Chief Procurement Officer are working together to align the SAFETY Act application review process more closely and effectively with the procurement processes within DHS and throughout the Federal Government. We have briefed members of the DHS acquisition community to facilitate the integration of these two processes. We are also streamlining our review processes and are working to eliminate duplicative technical reviews of candidate technologies that are the subject of government procurements. We take very seriously our responsibility to ensure that technologies receiving SAFETY Act protections are effective in helping to protect America; however, if a thorough evaluation of a technology has already been conducted as part of the government's RDT&E or acquisition process and particular technologies found to be effective, we are comfortable eliminating duplicate technical reviews and "fast tracking" applications for SAFETY Act protections to coincide with government acquisition schedules. We are doing this now with our current initiative to seek technologies to detect liquid explosives. The Department did this effectively last November with regard to the procurement by the Domestic Nuclear Detection Office (DNDO) of Advanced Spectroscopic Portal technology. Other examples include coordinating with the Transportation and Security Administration (TSA) on private airport screening services. We recently worked with procurement and other officials to integrate SAFETY Act into planning and acquisition activities associated with the Secure Border Initiative, US-VISIT, and the Registered Traveler program.

The Final Rule also establishes that some of the protections of the SAFETY Act can be afforded to qualified anti-terrorism technologies that are undergoing developmental testing and evaluation. By creating "Developmental Testing and Evaluation Designations," the Final Rule encourages investment in promising technologies that could serve as an important homeland security resource.

Another major enhancement to the SAFETY Act program is the new Application Kit which was released on August 14, 2006. The SAFETY Act program is in its third year, and experience in administering the program has demonstrated that procedural processes built to administer the Act could be improved. The Department recognized that the initial SAFETY Act Application Kit was overly burdensome and the application process could be streamlined and made less bureaucratic. The Department has refined the SAFETY Act Application Kit and the application process more generally to reduce burdens and to focus more precisely on collecting the information necessary for the review of a particular anti-terrorism technology.

The Department recognizes that each SAFETY Act application is different. Our aim is to have an interactive and flexible application process and to focus the SAFE-

TY Act Application Kit on soliciting essential information that may be supplemented as necessary on a case by case basis. And as part of the new Application Kit, the Office of SAFETY Act Implementation will be proactively engaging applicants much earlier in the process. The new Application Kit is designed to be more "user-friendly," and the Department, through a Notice in the Federal Register dated August 17, 2006, is inviting comments and suggestions for how we may further refine the kit to make the SAFETY Act application process even more effective.

With the Final Rule and new Application Kit in place, the SAFETY Act Office will be redoubling their efforts to encourage an increasing number of SAFETY Act applications. To this end, continuing the proactive outreach that began with the S&T Directorate's first SAFETY Act presentations in five cities in the Fall of 2003, we are participating in or presenting at a number of homeland security-related conferences to spread the word to individual companies. We are also beginning a comprehensive system of outreach to high-tech trade associations, technology incubators, relevant members of the legal community, and leading business associations. Our outreach will involve one-on-one meetings, participation in industry events, articles in industry publications and greater information dissemination via the SAFETY Act website, *www.safetyact.gov*.

For example, there are dozens of high tech trade associations in the DC area representing thousands of technology companies. By working with them to spread the word about the SAFETY Act, we can dramatically increase our number of applicants and thereby find valuable anti-terrorism technologies for use by DHS. Personal briefings with members, newsletter articles and targeted events as well us field visits and "town hall" meetings allow us to inform more companies about the protections available to them as we continue to fight the war on terror. This opportunity also exists across the country with state, county and city technology associations. Building a relationship with them will help facilitate our grassroots outreach. Successful utilization of the SAFETY Act program truly depends on effective public-private partnerships and we will work to make the most of this opportunity.

I believe the best way to judge the progress we are making is by the statements of the companies that have received SAFETY Act awards. We have worked diligently to listen to the feedback from private industry and their comments speak volumes about the quality of the work we are doing. In the June 19th issue of *Government Security News* magazine, a number of companies issued statements about the benefits of the Act and how it has impacted their business.

- Wackenhut Chairman and CEO Gary Sanders stated, "By granting these much sought-after awards, the DHS has validated these important processes and declared that Wackenhut's services are designed to envision and defend against possible terrorist scenarios; deny terrorists access to secure facilities; and, to respond to terrorist related security breaches."
- Mitigation Technologies Managing Member Craig Schwartz stated, "Mitigation Technologies continues to develop and deploy innovative life-saving products while seeking added benefits like DHS' SAFETY Act coverage to provide safety, comfort and peace of mind for citizens worldwide."
- Smith Detection Americas President Cherif Rizkalla stated, "SAFETY Act certification provides our customers with real assurance the Hi-SCAN 7555i and the Sentinel II are effective, reliable and safe anti-terrorism technologies. . . We plan to obtain SAFETY Act approval for additional Smiths products in the near future."
- Boeing's Vice President of Advanced Homeland Security, John Stammreich stated "to us, the SAFETY Act is vital. . . .we're really encouraged how far the government has come in the last 18 months to two years. . . .Boeing is feeling very bullish about the SAFETY Act environment."

In conclusion, the SAFETY Act is a vital tool for our government to remove barriers to full industry participation in finding new and unique technologies to combat an evolving enemy. Technological and scientific innovation continues to be a major factor in our Nation's success, and the SAFETY Act is one means by which we can help leverage that strength in our War on Terrorism. The SAFETY Act can, when used to its full potential, create market incentives for industry to increasingly invest in measures to enhance our homeland security capacity. While more needs to be done, I am pleased to report there are over 100 SAFETY Act protected technologies that we have enabled to be deployed around the country, and over 40 additional technologies under review. The fact that we have a growing number of applications in the pipeline is testament to the fact that this program is becoming increasingly credible and important to the business and government acquisition community. This fiscal year alone OSAI has processed and issued twice as many Designations and Certifications for Qualified Anti-terrorism Technologies as in previous years. Moreover, DHS has set the stage for even greater progress and accomplishment for im-

plementation of the SAFETY Act. The SAFETY Act will continue to provide needed protection to the most dynamic creators of anti-terrorism technologies, while also safeguarding the American public. Thank you for your time and I look forward to your questions.

Mr. ROGERS. Thank you, Mr. Cohen.

And the chair now recognizes Ms. Elaine Duke, chief procurement officer for the Department of Homeland Security.

And we welcome you back and look forward to your statement.

STATEMENT OF ELAINE DUKE, CHIEF PROCUREMENT OFFICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. DUKE. Thank you. Good to be back. Good morning. Chairman Rogers, Chairman Reichert, Ranking Member Meek, Ranking Member Pascrell and members of the committees, I am Elaine Duke, and I am the chief procurement officer for the Department of Homeland Security.

Thank you for the opportunity to appear before you to discuss the Department of Homeland Security SAFETY Act implementation.

The SAFETY Act of 2002 serves as a critical tool in expanding the creation, proliferation and use of antiterrorism technologies.

While the Undersecretary for Science and Technology is responsible for executing the functions of the act, including the designation of technologies as qualified antiterrorism technologies, I am responsible for integrating the SAFETY Act into the DHS acquisition program.

Because the SAFETY Act will apply to all federal agencies procuring antiterrorism technologies, federal-wide policy and guidance is needed to ensure the SAFETY Act protections are appropriately considered during the procurement process.

Therefore, the SAFETY Act procurement regulations, like other federal-wide acquisition regulations, will be implemented through a change to the Federal Acquisition Regulation, or FAR.

Since the issuance of procurement regulations was contingent upon publication of the program final rule, DHS initiated this change to the FAR in June 2006, just after the SAFETY Act final rule was published.

In July, DHS Office of Chief Procurement Officer submitted a concept paper to the FAR law team case manager. And on August 16th, 2006, DHS presented a draft case to the FAR council, which is composed of representatives from the General Services Administration, NASA, Department of Defense and Office of Federal Procurement Policy.

Since proper acquisition planning is critical to the success of the SAFETY Act implementation within the federal procurement system, DHS's proposed FAR language emphasizes the need for federal agencies to initiate early planning and coordination with the DHS Office of SAFETY Act Implementation for acquisitions involving potential antiterrorism technologies.

The FAR council has accepted DHS's request to initiate the rulemaking case for the proposed rule to establish uniform federal procurement policy implementing the SAFETY Act.

We are pleased that this is occurring, since the SAFETY Act has broad application to acquisitions throughout the federal govern-

ment, and the FAR case is the bet method for increasing awareness of this important program.

While S&T is responsible for the SAFETY Act program, including the approval of SAFETY Act application, evaluation and determination, the Office of the Chief Procurement Officer is responsible for ensuring DHS solicitations and contracts appropriately convey requirements and address all aspects of the process, including those associated with the application of SAFETY Act protections.

DHS program officials and contracting officers will play a key role in facilitating the SAFETY Act process, and S&T will retain the responsibility for reviewing and approving the SAFETY Act applications.

Therefore, to effectively integrate SAFETY Act into the procurement process, we have partnered with the Office of SAFETY Act Implementation in Science and Technology to facilitate open communication and align processes.

Since release of the final rule, our office, in collaboration with Science and Technology, has issued a memorandum to the heads of all the DHS contracting activities, the component Office of General Counsel and the DHS Program Management Council discussing the implementation of SAFETY Act in DHS.

We have trained our chief acquisition officers of each component in DHS so that they can implement SAFETY Act provisions in their procurements. We have briefed the DHS Procurement Management Council and initiated dialogue with industry to discuss our path forward.

As the procurement rulemaking process continues to the FAR council, DHS remains dedicated to ensuring that consideration for SAFETY Act coverage is addressed in all applicable procurements.

For example, in the advanced spectroscopic portal program, or the ASP program, the Undersecretary for Science and Technology predetermined that the products and services being acquired from successful offerers under ASP would be designated as qualified antiterrorism technologies.

This effort allowed DHS to significantly fast-track the SAFETY Act process in the procurement of the ASP program last November.

For the SBInet secure border initiatives acquisition, in addition to incorporating SAFETY Act language into the solicitation, DHS, in response to industry inquiries, sent a letter to all offerers clarifying the application of SAFETY Act under this procurement and offering to meet with each offerer one-on-one to address any additional guidance concerns they may have.

Finally, recently in liquid explosives, as Undersecretary Cohen already discussed, we have addressed SAFETY Act in the requests for information. We continue to look for more opportunities to proactively use the SAFETY Act within the Department of Homeland Security.

In closing, successfully implementing the SAFETY Act requires collaboration and strong working relationships, and we have built those and will continue to build those. I am committed to fostering those relationships.

And I thank you for the opportunity for testifying before this committee about DHS contracting procedures, and I am glad to answer any questions that you may have.

[The statement of Ms. Duke follows:]

PREPARED STATEMENT OF ELAINE C. DUKE

Chairman Rogers, Chairman Reichert, Congressman Meek, Congressman Pascrell, and Members of the Committees, I am Elaine Duke and I am the Chief Procurement Officer for the Department of Homeland Security. I appreciate the opportunity to discuss the Department of Homeland Security's final rule on implementing the SAFETY Act. As the Chief Procurement Officer, my top four priorities are:

- First, to build the DHS acquisition workforce to enhance the Department's acquisition program.
- Second, to establish an acquisition system whereby each requirement has a well defined mission and a management team that includes professionals with the requisite skills to achieve mission results.
- Third, to ensure more effective buying across the eight contracting offices through the use of strategic sourcing and supplier management.
- Fourth, to strengthen contract administration to ensure that products and services purchased meet contract requirements and mission need.

Effective implementation of the Safety Act is critical to the fourth priority.

SAFETY Act Implementation

The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 (Subtitle G of Title Vlll of the Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135, 2238–2242 (6 U.S.C. §§ 441–444)) creates incentives for companies to bring new anti-terrorism technology to the market place by limiting the seller's and other parties' potential liability if the technology is deployed in defense against, response to, or recovery from an act of terrorism. The SAFETY Act serves as a critical tool in expanding the creation, proliferation and use of anti-terrorism technologies (or services). The provisions of the SAFETY Act provide explicitly that the SAFETY Act's liability limitations apply whether approved technologies are sold to the government or by and between private parties. The Under Secretary for Science and Technology (S&T) is responsible for executing the functions of the Act including the designation of technologies as "Qualified Anti Terrorism Technologies" ("QATTS"). I am responsible for integrating the SAFETY Act into the DHS acquisition program.

Federal Acquisition Regulation (FAR) Council Rulemaking

On June 8, 2006 the Department published the SAFETY Act Program final rule, which went into effect July 10, 2006. Because the SAFETY Act will apply to any federal agency procuring anti terrorism technologies, federal wide policy and guidance is needed to ensure SAFETY Act protections are appropriately considered during the procurement process. However, the initiation of procurement regulations was contingent upon the publication of the final Program rule. On August 16, 2006, DHS requested that the FAR Council, composed of representatives from the General Services Administration (GSA), National Aeronautics and Space Administration (NASA), Department of Defense (DOD) and the Office of Federal Procurement Policy (OFPP), initiate a proposed FAR case to establish uniform federal procurement policy implementing the SAFETY Act. The FAR Council has accepted the DHS request to initiate the rulemaking case for the proposed rule. We are pleased that this is occurring since the SAFETY Act has broad application to acquisitions throughout the federal government and the FAR case is the best method of increasing awareness of this important program.

Key to the success of SAFETY Act implementation within the federal procurement system is proper acquisition planning. Therefore, the proposed FAR language emphasizes the need for federal agencies to initiate early planning and coordination with the DHS Office of SAFETY Act Implementation (OSAI) for acquisitions involving anti terrorism technologies.

In a parallel action, my staff is preparing a revision to our own Homeland Security Acquisition Regulation/Manual (HSARIHSAM), to complement and supplement the FAR change. Similarly, other agencies including the Department of Defense will determine whether to publish FAR supplementing language in their respective supplements.

Implementing SAFETY Act Provisions in DHS Procurements

While S&T is responsible for the SAFETY Act program, including the approval of SAFETY Act application evaluations or determinations, the Office of the Chief Procurement Officer (OCPO) is responsible for ensuring DHS solicitations and contracts appropriately convey requirements and address all aspects of the process, including those associated with application of SAFETY Act protections. DHS program

officials and contracting officers will play a key role in facilitating the SAFETY Act process; however, S&T retains the responsibility for reviewing and approving SAFETY Act applications.

Therefore, to effectively integrate SAFETY Act considerations into the procurement process, the Office of the Chief Procurement Officer (OCPO) has partnered with the OSAl and S&T to facilitate open communication and align processes. Since the release of the final rule, OCPO, in collaboration with S&T, has:

- Issued a memorandum on August 7, 2006 to the heads of the DHS contracting activities (HCA), the component Offices of General Counsel (OGC), and the DHS Program Management Council (PMC) discussing the implementation of the SAFETY Act in acquisition planning.
- Briefed the Chief Acquisition Officers (CAOs) of each Component at the monthly CAO Council meeting so that the CAOs can disseminate information concerning the SAFETY Act and its procedures to the acquisition workforce personnel within the Department of Homeland Security.
- Briefed the DHS Program Management Council on the SAFETY Act and related processes and procedures. The Program Management Council is a component of the Program Management Center of Excellence, which works to develop the policies, procedures and other tool sets needed for DHS Program Managers to succeed.
- Initiated dialog with industry to discuss the path forward with SAFETY Act implementation for affected DHS procurements, and will continue to engage industry during the Procurement rule making process by soliciting input and feedback through a public meeting.

Although the Procurement rule making process continues, DHS remains dedicated to ensuring that consideration for SAFETY Act coverage is addressed in all appropriate procurements. For example, in the Advanced Spectroscopic Portal (ASP) program, the Under-Secretary for Science and Technology pre-determined that the products and services being acquired from successful offerors under ASP would be designated as QATT, as that term is defined by the SAFETY Act. This effort allowed DHS to significantly ″fast track the SAFETY Act review process in the procurement of the ASP Program last November. For the SBlnet acquisition, for example, in addition to incorporating SAFETY Act language into the solicitation, DHS, in response to industry concerns, sent a letter to offerors clarifying the application of the SAFETY Act to the acquisition and offering to meet with companies one on one to provide any additional guidance. Finally, in the recently issued Request for Information (RFI) concerning Liquid Based Explosive Detection Technologies we announced, in coordination with the S&T Directorate, that technologies which were effective in detecting liquid-based explosives and capable of deployment would receive SAFETY Act protections.

We will continue to look for more opportunities to proactively use the SAFETY Act to facilitate the widest possible industry participation in our procurements. The fact that the SAFETY Act limits the downstream liability of suppliers and subcontractors of the technology is an especially powerful tool in streamlining procurements in the public and private sector. To that end, OCPO will develop SAFETY Act training for contracting professionals so that application of the Act within DHS procurements will be effectively facilitated and coordinated from the procurement perspective. Furthermore, OCPO is currently working to modify the Department's current acquisition planning guide, which is contained in the Homeland Security Acquisition Manual (HSAM), and describes DHS internal policies and procedures.

Conclusion

In closing, successfully implementing the SAFETY Act requires collaboration and strong working relationships with all DHS stakeholders, to include private industry, other federal agencies, and members of Congress, to ensure DHS meets its mission as effectively as possible. I am committed to continuing with fostering those relationships. Thank you for the opportunity to testify before the Committees about DHS contracting procedures and I am glad to answer any questions you or the Members of the Committee may have.

Mr. ROGERS. I thank you.

And I would like to start off with a couple of questions for Ms. Duke specifically.

You heard Secretary Cohen make reference to how optimistic he was that you all had turned the corner in this application process, and it is going to be a much more rapid and simplified process. Do you share that perspective?

Ms. DUKE. I do. I think that from both the process and how it is integrating into procurement and the application itself—the biggest step we have taken forward is that we have a prequalification designation, so early in the planning process of major acquisitions, we can go to science and technology from the acquisition world and ask them to predesignate the technology that would be proposed under this procurement. So that really gives us a parallel process.

The second thing that the department has done is simplified the actual application process and shortened the review time. So in both aspects I do agree with that.

Mr. ROGERS. Was the 93-page form the simplified form?

Ms. DUKE. It is the simplified form, but there are many different types of applications. It is not 93 pages for one form.

Mr. ROGERS. Because 93 pages doesn't sound real simple to me. But a second question: As I understand it, the SBI procurement specifically states that proposals in which pricing or any other term or condition is contingent upon SAFETY Act protections of the proposed product or service—or it will not be considered for award.

And how or when are you going to police this? Could you describe that?

Ms. DUKE. If an offer was contingent on SAFETY Act coverage, an offerer would have to have completed and have his designation and certification be for award.

The way we are policing it is when we first got the offers we reviewed each offer to ensure that that contingency was not in the proposal.

The reason we stated that affirmatively up front is we felt that it was important for industry to know that we would not accept offers that said they were contingent so that the offerers could appropriately price and submit their proposals.

The other reason for doing that is because offerers do not have to wait until they are selected for a contract to apply for SAFETY Act coverage.

And so that was an indicator to industry that because we are not going to accept contingent offers, they are not going to be able to say we won't accept a contract unless we have coverage, it allows them to—it indicates to them that if they want to apply for SAFETY Act coverage they should do that before waiting to be notified that they are a potential awardee.

Mr. ROGERS. Secretary, I wanted to ask you—I understand from your comments and Ms. Duke's comments that you all have established a good working relationship and have much better communication.

Do you have similar channels of communication and relationships established with your customers, those folks in the private sector that you are going to be interacting with? If so, what are they, and how long have they been in place, and what do you see their prospects for enhancing the speed of this process, this application process?

Mr. COHEN. Well, the short answer, Mr. Chairman, is that that is a work in progress. As I indicated on the 11th of August, not knowing what those processes were, thanks to some of the gentlemen sitting behind me, the Chamber of Commerce and other representatives, we do have a business office.

There is an outreach at the department level as well as my directorate level. We went ahead and engaged directly with them. But we are in the process—and some of this has already occurred, but having—my words now—a road show, an outreach where we not only go to various conventions, various symposia, but just like I have done previously in Navy with the SBIR, the small business innovative research, where we go out to districts, to small groups of businesses.

It is easier to touch, of course, the big businesses?

Mr. ROGERS. Right.

Mr. COHEN. —than it is the small because they are so diverse. But we live in a Web-enabled world, and it is hearings like this that get covered in the press, that get out to the public to let them know that we have this program.

But the short answer is this is a work in progress to ensure that we cover both geographically and economically large and small and technological risk from low to high how we do that.

But that is more my responsibility than the SAFETY office's responsibility, because I see our outreach hand in glove with looking for the cutting-edge technologies that we need, and the SAFETY office merely provides the protections that the Congress intended.

Mr. ROGERS. Great. Thank you very much. That is all the questions I have.

The chair now recognizes the ranking member, Mr. Meek.

Mr. MEEK. Thank you, Mr. Chairman.

Secretary Cohen, I want to ask you—you said in your testimony that there is not a day that goes by that you don't get an application. Is there a waiting list or a logjam as it relates to the processing of the applications?

And since you have one person on the SAFETY Act office—I know that it is supported by the legal office. Can you just enlighten us a little bit about the process? Are there any areas where we need improvement?

Mr. COHEN. Well, the short answer is there have been logjams, and there continue to be smaller logjams. Right now I have a handful of applications. These are fairly detailed and difficult issues that have exceeded the 120-day window that I feel is very important for us to meet.

And as I have indicated in my verbal comments earlier, while I may not want to change the rule, I do want to get the performance down, and we do that by metrics and feedback and resourcing. I have a total of about 16 people in the office.

Ms. Vasta, of course, is the government service. This is inherently government service. This is not something that I want to contract out. But I have a very lean organization. And the Congress and the administration intentionally made the Department of Homeland Security lean.

Mr. MEEK. Mr. Secretary, if I can?

Mr. COHEN. Yes, sir.

Mr. MEEK. —when you say a handful of applications, what are you talking about? When you say a handful, is that 16, 20?

Mr. COHEN. Six or less.

Mr. MEEK. Six or less.

Mr. COHEN. Six or less.

Mr. MEEK. Okay.

Mr. COHEN. And I will take that for the record, so that I get you the exact number.

Mr. MEEK. Okay. I am going to tell you what my concern is, and I told you this subcommittee meeting was very frustrating for me because I was here when we had the select committee, and we had all of these technology companies come and sit at the table where you are sitting and saying, oh, we have technologies, we would like to share them, we would like to be a part of protecting America, but we are not going to stick our necks out there, only to find out, you know, 6 months ago that we are, you know, with under 30 applications approved, and we have technology companies and other companies that are saying we want to be a part of the solution?

Mr. COHEN. Yes, sir.

Mr. MEEK. —but the department won't allow us to be a part of the solution.

So that means those of us that are sitting up here and individuals over at the Department of Homeland Security, that now we are standing in the schoolhouse door not allowing safety and protection of Americans to happen.

So if I sounded a little frustrated in my opening comments, I was. But I just want to say that I am glad that we are moving down the line, and I don't want us to go and start, you know, saying okay, let's start an assembly line here and let's start approving everything, because when you look at the SAFETY Act, it is written in a vague way to allow not only technology but support services.

Well, support service, what is that? You know, is that a security guard at the door of the Department of Homeland Security? You know, so we have to really look at these things. We are not asking for an assembly line effect.

We are asking for a process that would be user-friendly for those companies that are willing and support services that are willing to come forth to help protect Americans.

But we do not want to hear—we just passed 9/11—oh, all of this is in place, here is a company that had the technology, they wanted to come, and their application has been stuck over at Department of Homeland Security because someone said we want to be lean and mean.

I am going to tell you right now, when it comes down to protecting Americans, when we have technology that is out there, I don't want us to be the problem. That is what I am saying.

So that is the reason why I am saying in a very blunt way, in very plain English, if there is something that we need to know, something that you need, then somebody needs to say it. If not this panel, the next panel. If not the next panel, somebody needs to send an e-mail, drop a letter off without a name on it, or whatever the case may be, and say this is where the logjam is taking place.

We don't want folks to get frustrated. I don't want to pick up U.S. News & World Report and hear about how some other country is beating the United States, or some U.S. company has gone over there because they give them the coverage that they need under a similar act, you know, as the SAFETY Act.

So I will leave it at that, Mr. Chairman. I just hope that this will bubble up through the process before we leave this room today. If not, the members and staff will be able to get that information.

Ms. Duke, do you have anything that you want to add?

Ms. DUKE. No. I agree with you totally. This is important for businesses to be able to work effectively, both large and small, and we are jointly committed to continuing to improve that.

Mr. MEEK. Okay. Thank you.

Mr. COHEN. Mr. Meek, I know you have other commitments, but I want to make sure that I clarify what I said. First of all, you are right to be frustrated. The department, as you can see, long before I got here has taken that aboard, has taken action, but that is not a production line.

This is a due diligence process with all the reviews that—again, I am not a lawyer—that I believe the Congress intended us to do. But you are also right to remain skeptical. And what is the right balance?

While I believe in a lean organization, I also understand my statutory responsibility, and it is my signature that goes on each of those certificates and each of those approvals. And my father, may he rest in peace, said son, the only thing you have in this life is your good name, don't give it away.

And so I believe you and I are very much aligned on this and that Congress has never denied me, in the years that I have dealt with them, those tools that I have needed to do the right thing. And I thank you so much.

Mr. MEEK. Well, Mr. Cohen—Mr. Chairman, if I can—you know, it wasn't meant as an individual holding the horse or holding the cart, you know, up from making it to the market. I just want to make sure that, like you are saying, you are clear. I want to make sure that you know that we are clear.

Mr. COHEN. Yes, sir.

Mr. MEEK. The frustrating part on the oversight, again, especially for the subcommittee that I am the ranking member of, is the Monday morning quarterback theory. The game is on Sunday. We want to play it on Sunday. We want to win it on Sunday.

We don't want to on Monday talk about well, you know, when we came before you last time, we really needed this but, you know, it didn't quite come out in that meeting, because at the Department of Homeland Security—revolving door of undersecretaries and executive directors. And so you really are dealing with a new person every time you sit down. Hopefully that will stop. I want you to stay in the position that you are in.

But I just want to make sure that if we have companies that are out there—and I heard from some of them that are saying we have this technology, but we can't participate in the SAFETY Act program.

So when people come to me and say that, what am I supposed to do?

Article I, section 1 of the U.S. Constitution, as a member of Congress and a representative of the people of the United States of America, is to make sure the department, A, has what it needs to carry out the mission; B, make sure that they have the will and the desire even if they don't want to carry it out.

So I am Mr. Johnson and Ms. Johnson who went to vote one day at 7 a.m. in the morning for representation. I am the body and the flesh of those individuals. So I just want to make sure that neither you nor the department takes my comments out of context to say that maybe I just didn't have my coffee yet. That is not the case.

I just want to make sure that we break it down to the point that everyone understands what we need and how we need it and when we need it. And if you need it, you need to say it.

Thank you, Mr. Chairman.

Mr. REICHERT. [Presiding.] Thank you, Mr. Meek.

The chair recognizes Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman.

Good morning. My question is this—I have a few questions, but we will start with this one. Why did the RFP for the SBI, the secure border initiative, specifically exempt contractors from the SAFETY Act liability protections? Either one of you.

Ms. DUKE. It actually told offerers that we would be providing SAFETY Act protection. It did have a statement that we would not accept offers that were contingent on SAFETY Act protection prior to award.

And the reason for not accepting contingent offers is that the way that the SBInet procurement is worded, each offer is going to come in with a unique technology. We cannot accept—I am sorry.

It was to put offerers on notice that they would have to seek SAFETY Act protection before award, which they always can do and should do, or they would have to accept the contract and continue to go through SAFETY Act coverage.

So it is not really excluding them, but it is to put them on notice that if they say we will not accept a contract without SAFETY Act protection, and they don't get that SAFETY Act protection, that we would not award.

Mr. COHEN. If I may follow up, I have received a full brief on the SBInet program, although I specifically asked not to know who the bidders or offerers were, and I am very comfortable in telling you that whoever the winning offerer may be that they will receive SAFETY Act protection. I think they understand that as the process has gone along.

And that protection will be for the activities that they would perform under that contract. And I am very comfortable in doing that. We are spring-loaded to go forward on this. This is so important.

But I am comfortable in having my office, to the maximum extent possible, endorse the work of Ms. Duke's source selection panel and their detailed technical review of those proposals so that we don't have to unnecessarily revisit that.

And again, I think this is all part of the process improvement. But, Congressman, this is a big one, and we want to get this right.

Mr. DENT. Thank you.

And also, I just wanted to publicly thank Ms. Duke for your participation in the homeland security procurement center that we held up in my district at Lehigh University. It was well received, and I want to thank you for that publicly.

Ms. DUKE. Thank you.

Mr. DENT. Your staff did a wonderful job.

My next question deals with this: What specific steps can DHS undertake to reach out to small businesses which might have products of interest to the DHS and which might not know about the liability protections that you just went over that were offered by the SAFETY Act?

Ms. DUKE. Well, one of the best programs for small business is the small business innovative research program, and we do have many initial evolving technologies awarded under that program. In fact, we used it recently on liquid explosives through TSA.

Another way is we are, as a standard, including SAFETY Act in our small business briefings. We do many events like the one held in your district, and we have gotten many inquiries, so that is now a standard part of our presentation.

The other thing we are doing in the procurements coming forward, once the Federal Acquisition Regulation, FAR, case is done, we will be having standardized language, and we will clearly tell the businesses if they would have a predesignation notice or not.

So we are going to continue the training. We are going to continue the outreach. And that is the biggest way that we can reach out to the small businesses.

Mr. DENT. And finally, if you could do anything in DHS to streamline the application process in order to make the whole process more user-friendly, particularly for those smaller companies, that would be greatly appreciated, because, as you know, a lot of them don't have the manpower or the capacity to deal with all the bureaucratic issues that are required.

Ms. DUKE. S&T does offer a preapplication meeting, and I would encourage all small and large businesses to have those to help them before they actually get started in the application process.

Mr. DENT. Thank you. I have no further questions.

Mr. REICHERT. Thank you, Mr. Dent.

Mr. Thompson is recognized for 5 minutes.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I have testimony I would like to submit for the record that I was not here earlier to give personally.

Welcome, Mr. Secretary. I am happy to get a chance to see you, although we will have our meeting in the future.

Ms. Duke, always good to see you.

And I guess I have a question I would like to give both of you. It speaks in reference to the application for services process for the SAFETY Act as proposed. I am sure you are familiar with the Wackenhut situation and the notion that they were one of the first contract service providers for security.

And we know what happened at the situation at headquarters. But they also had received designation, basically, that we would defend them against terrorist scenarios, deny terrorists access to secured facilities and to respond to terrorist-related security breaches.

And I guess I have two questions as it relates to that. When we give these kind of waivers to people, what happens when they provide less-than-adequate service in this procurement?

I know sometimes you go out and rebid the contract, but what happens when they haven't trained the people for the service that

they said they would? Do we then take that shield away, or just what?

[Information follows:]

FOR THE RECORD

BGT Talking Points

SAFETY Act Hearing

September 13, 2006

- Congratulations to the Department and the General Counsel's office for putting out the final rule and the application kit.
- Though I am happy to see Under Secretary Cohen here, I would have liked to see a representative from the General Counsel's office who could testify to some of the changes to the rule and the application kit.
- I'm going to be meeting with Phil Perry, the General Counsel, in the upcoming days—I'd like him to explain why the Department did not want him—as its top lawyer—to be testifying here today.
- In the meantime, that means Mr.Cohen you are going to be on the hot seat today as we have a lot of questions about the Department's performance and decisions to date.
- As background, I first requested a hearing on this issue back in April.
- Since then, my staff and I have received a significant number of comments from applicants and other folks in the private sector who have had experience with the SAFETY Act.
- Not all of the comments were negative, but a significant number of people expressed some dismay in the Department's efforts in dealing with the SAFETY Act.
- One group told me that the SAFETY Act office was acting like a "Mini-FDA" in granting certifications and designations. I can assure you that this was not the intent of Congress.
- But after the Department issued its final rule, and after the Department issued its final kit, those complaints have become less frequent.
- And that's why I cautiously congratulate the Department's efforts here—it's not a perfect product, but you listened to folks here on the Hill and the applicants in the private sector and you put a better product forward.
- But not everything is perfect.
- Shortly, we'll be getting into some of unfinished business, particularly:
  - The administration issues within the SAFETY Act Office;
  - The confidentiality of the information that the Department retains;
  - The certification of "services";
  - The burden of the application kit;
  - The duration of a SAFETY Act designation;
  - The possibility of creating an appeals process; and
  - The necessary linking of the procurement office with the SAFETY Act Office, and the efforts of the Department to promote the application of the SAFETY Act across different levels of government, particularly in the state and local procurement process.
- I look forward to working with the Under Secretary and the Department in resolving some of these issues.
  - Above all, we have to remember what the SAFETY Act is supposed to be doing: putting technologies out in the field that otherwise may not have been developed. Clearly, this Act was not intended to be a blanket liability waiver for every anti-terrorism technology out there.
  - But it is clear that the way the Department had been implementing the Act in the past has left something to be desired. I am confident that with the new kit, the new rule, and continued feedback from folks here and in the private sector, we can all work together to achieve the optimal result.

Ms. DUKE. Well, I can address the contract performance. A contractor getting SAFETY Act coverage does not relieve them of the responsibility for performing satisfactorily and performing well.

So the SAFETY Act coverage looks at it in the plan. Is it antiterrorist technology? Does it show that they are going to perform as intended by that technology or that services?

Once the contract is awarded, then we get into the performance issue. And in the case of Wackenhut, as you know, they are no longer performing services.

So I would address that by taking contract action and either not renewing or terminating the contract as appropriate for not performing the service, whether or not they had SAFETY Act coverage.

And I think that in the case of—so as planned, they might have met the requirements of the SAFETY Act to get coverage, but the execution has to be there, and that is a contracting issue.

Mr. THOMPSON. So if the execution is not there, do they continue SAFETY Act coverage?

Ms. DUKE. That is probably a question better for you to answer.

Mr. COHEN. Well, Congressman, I am not a lawyer, and I don't presume to be. We are very appreciative of the SAFETY Act and the intent to get technologies to protect the homeland. But this is an area of new law.

And at some point, there will be a lawsuit or there will be an event—the very kinds of questions you are talking about in this case, performance. I have been a senior acquisition official in my time in naval research in the Navy, and I think the overriding fact here is the one of performance.

And so if a provider or performer is not meeting the performance criteria to satisfy the contract, then as Ms. Duke indicated we have a variety of remedies from warnings, to termination, et cetera, all of which have been used in other instances.

And I think this is an area that you have identified where Ms. Duke and I need to sit down along with the general counsel and in consultation with the Congress to find out at what level of action by the contract office do we say your performance is no longer adequate to meet the protection of the SAFETY Act certification that has been granted.

Mr. THOMPSON. Well, before my time runs out, Mr. Chairman, I would like to get some explanation from the department to the committees here as to why the general counsel is not present for this hearing.

This is clearly something in his bailiwick that he should have been here to respond to. It is a legal question, and he is the department's lawyer. And I think we would be better served if Mr. Perry was here to interpret that piece of legislation.

Mr. REICHERT. And we will certainly get the answer to that question. Thank you, Mr. Thompson.

I think I will go to Mr. Pascrell.

Mr. PASCRELL. Mr. Chairman.

I want to ask my first question to Ms. Duke. And in linking procurement with the SAFETY Act, the link between the act office and the procurement office, you know and I know, must be improved, and I think you are working toward that end, and both of you are.

In preparing for this hearing, some in the private sector have characterized the SAFETY Act approval process as a mini–FDA, and we know that is not a very complimentary thing that we are saying there.

The purpose of the SAFETY Act, as I understand it, is to get this country producing antiterrorism technologies, not to create an enormous bureaucratic regime.

If a product meets a test for procurement officials, there is no reason why the SAFETY Act office should have to run through a new process to test the effectiveness of the product. How will the SAFETY Act office work with the office of procurement to achieve these results? And do you agree with my conclusion?

Ms. DUKE. This is something we have talked about very recently, and we are looking at ways where we can have the SAFETY Act office be in the proposal evaluation process so that we can run a parallel process.

Whether they would need additional work would depend on the actual procurement on a case-by-case basis. But we do think that that is an area where we can reduce duplication by having the SAFETY Act application process integrated more completely with the proposal review process, yes.

Mr. PASCRELL. Would you add anything to that, Secretary Cohen?

Mr. COHEN. I think as an example, you will see when SBInet, you know, goes to contract that we are taking the lead on this so that as part of the acquisition process, the due diligence and the complete review that has been done there, if that is adequate and satisfactory, then very quickly—very quickly; days, if not weeks—the SAFETY Act certification will follow.

Mr. PASCRELL. And that leads me to my second question to you, Mr. Secretary. You know, I don't want to get into the minutiae here. You folks know your jobs, and I think you are doing them very well.

But you know, George Kennan a great architect of international affairs, said that democracy is like a huge dinosaur, and it needs its tail whacked many times. I don't, up until very recently—maybe I changed my mind a little bit. I have never sensed a sense of urgency in the Department of Homeland Security.

And we are talking about American lives here. I think there is a lack of urgency. And you look at your chart to prove it in one way, and that is only just one slice since September 11th.

And we talk a lot about this. We talk how important it is to protect America, and we are going to do this, and we are going to do that. But in the very nature, the very center, the very essence of attempting to do that, and something very specific of developing the science and then the technology to protect Americans, we have done a lousy job.

I mean, you are going to have your hands full. You know it. We talk academically here, but you take the issue that you brought up here, the issue of liquid explosives. I mean, we talked about that right after 9/11. And here we are looking like we are reinventing the wheel 5 years later.

And, you know, we are causing all kinds of havoc about what, for instance, women can carry on an airplane 5 years after 9/11. Now, we can have camaraderie here and congeniality, and we should, and be civic and civil to each other.

But that is unacceptable. So when people say, you know, the question, is America safer now than it was 5 years ago, you know,

I don't really have an answer for that. Maybe you do. And we can make it up politically. If you are a Democrat, you will say one thing. You are Republican, you say another thing.

I can't answer that question, but I could tell you one thing. It is 5 years later and we do not have the technology to deal with liquid explosives. That is unacceptable. And I know it is unacceptable to you. So now what are you going to do about it?

Let me ask you this question. On information sharing, the final regulations information state that DHS may use information that has been submitted to the department under the SAFETY Act.

Who is the department planning on sharing this information with? What regulations have been established to guard this confidential information? Okay? I mean, we know that patents in certain industries are protected. This is more important, now. We are talking about life and death.

And what efforts are under way to safeguard the interest of the applicants? Would you please address those three questions, sir?

Mr. COHEN. I would like to take that for the record so I can give you a thorough answer, if I may.

Mr. PASCRELL. Yes.

Mr. COHEN. Thank you.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. REICHERT. Thank you, Mr. Pascrell.

The chair will take a moment to ask a few questions.

Good to see you again, Mr. Cohen.

Mr. COHEN. Mr. Chairman.

Mr. REICHERT. We just held a hearing not too long ago, a couple of weeks ago, where you are the star witness at that hearing also.

Welcome, Ms. Duke. Thank you for being here.

I would like to ask unanimous consent to my opening statement also be entered into the record.

I have just been listening to some of the comments and I want to cover some statements made by some of the other members of the committee and just have a brief question or two.

Sometimes we look at the things that we haven't done. We have done a lot, I think. And I think most people in the country would agree that one of those indicators is that this country has not been attacked in the last 5 years, and that is a great accomplishment, I think, by the American people and its government and those who work hard to protect our country.

One of the things that we often forget is that we are in a different world. We have to think about things like every container crossing the ocean headed for this country, every container on every ship, every day, and how we secure this nation and protect this country.

We have to think about every airport, every airplane that lands at every airport coming from any part of this country or any part of this world. Railroads, light rail, bridges, critical infrastructure, viaducts, ferry systems, all of those things, now border patrol, and UAVs, and surveillance cameras and all of those things now.

As I said in our last hearing, Mr. Cohen, you are on the hot seat and have been there for 1 month on the hot seat and understand fully what your job is. You laid out a well-thought-out organized

plan to address the issues of science and technology and where we might be headed as a nation.

But we can talk about method and level of communications and procurement officials and the office of SAFETY, the communication, whether it takes place or doesn't, is it formal, is it informal, is there a prequalification, is it simplified, expedited, and all those things.

The bottom line is what Mr. Meek had to say. Where is the logjam? And specifically, if we can just take a look at it, if you could just go through one piece of this. We talked about interoperability, emergency communications in our last hearing. But the whole question of liquid-based explosive detection technology.

Can you explain the process of that one piece of technology and where it is, and what has taken place, and kind of what the logjam has been, if there has been a logjam there?

PREPARED OPENING STATEMENT OF THE HONORABLE DAVE REICHERT

I would like to thank our witnesses for joining us this morning. We greatly appreciate your appearance before us today for this joint hearing. Mr. Under Secretary—welcome—it is a pleasure to see you again. I know my staff will agree with me when I say we are grateful for all your time, outreach and diligence in only a month on the job. Although there's no doubt that you have your work cut out for you, I honestly think that the Science and Technology Directorate is in good hands moving forward.

Looking back five years and two days to September 11, 2001, the world as we knew it changed forever that day. We began to realize then what we know to be true today, that victory over such single-minded killers requires every ounce of American might, commitment and know-how. As citizens and businesses alike come forward to help protect their neighbors, their children, and their grandchildren, nothing should stand in their way.

In the years since 9/11, Congress has worked to remove barriers and give first responders the tools they need to be better prepared. For example, in the year following those tragic events, Congress passed the Homeland Security Act and the Maritime Transportation Security Act. During the last Congress, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, which implemented many of the 9/11 Commission's recommendations. I am proud this Subcommittee continued this work by recently passing the 21st Century Emergency Communication Act of 2006, which will help our first responders have the communications equipment they need to effectively respond to a future terrorist attack.

When it comes to emergency response, effective partnerships are of paramount importance. The federal government needs the private sector to serve as our partner in developing new technologies so that American citizens may benefit from them in the event of a disaster. Under Secretary Cohen, just last week you testified before my Subcommittee that government is not the innovator, but that you work with the private sector to ensure they are developing the next generation technologies that we need.

This hearing focuses on keeping legal liability reasonably in check when a business sells a product to the government to protect our homeland—the Supporting Antiterrorism by Fostering Effective Technologies Act of 2002 or, "the SAFETY Act."

Congress enacted the SAFETY Act in 2002 as part of the Homeland Security Act for good reason—it is a necessary dimension of the homeland security mission. The SAFETY Act paves the way for businesses to quickly develop and deploy anti-terrorism technologies for homeland security. It accomplishes this by keeping a business' liability "on a leash" when it sells critical anti-terrorism technologies to the Federal government.

To me it is common sense: when people or businesses want to help defend America, they should not have to worry about frivolous lawsuits. Almost four years after the Homeland Security Act of 2002, industry remains skeptical about the burdens imposed by the SAFETY Act application process and the durability of the legal protection the Act provides.

Just last month, Prepared Response Incorporated, a company near my district in Seattle, Washington, earned SAFETY Act certification for its "Rapid Responder" crisis management system. The Rapid Responder system gives first responders a

bird's-eye view of critical infrastructure with an on-the-ground accounting of key features and assets. This "Rapid Responder" system gives first responders instant access to a digital map and inventory of critical infrastructure including: tactical response plans, evacuation routes, satellite and geospatial imagery, exterior and interior photos, floor plans, and hazardous chemical inventories. I'm proud to say that the Rapid Responder system developed by Prepared Response now protects more than 1,500 sites nationwide, including 7,000 individual facilities. This company is proof positive that companies stand side by side with our first responders in defending our homeland.

We are here today almost four years after it was enacted into law to ensure that Congress' vision for the SAFETY Act is being realized. We are here to ensure that companies like Prepared Response in Seattle can help protect their neighbors and their fellow Americans across the country, without fear of unrestricted lawsuits. I look forward to hearing from our witnesses about what we are doing to make certain that nothing keeps us from doing our utmost, day in and day out, to keep our families and our Nation, safe and secure.

Mr. COHEN. Well, first of all, you know, after our last hearing I asked my people, I said, what do you think the headline will be, and they said, you are on the hot seat. So I want to assure you that I am not putting any of our resources into asbestos underwear research, sir.

But on liquid explosives, there have been technologies in use for some period of time. Some of them are nascent. Some of them are mature. And some of them are direct and some of them are a spin-off of the other screening devices that we have.

But the enemy is agile. The enemy is devious. The enemy is nefarious. And technology doesn't stand still just for us. It moves forward for those that would attack us. And whereas we may use technology for the good, there are people and groups that would use it for bad.

And this will always be a measure, countermeasure, counter-countermeasure. That is how life goes. And so your question was where are we on the liquid explosives. Over a year ago, the Transportation Security Lab took onboard 10 COTS, commercial off-the-shelf, detectors.

These are the kinds of things you see on headline news, where good people come forward and show on the T.V. what these devices can do. But we know that those don't always work as advertised, or may need product improvement, et cetera. And so those were undergoing evaluation over the last year at the Transportation Security Lab.

Additionally, last April, an additional three under the SBIR program were brought on board for further evaluation. As it turns out, almost all of those were scheduled for testing at Socorro, New Mexico in August, September of this year.

But then we had the events of 10 August, and I was not satisfied with the extent of the net that we had put out to find solutions for TSA, Kip Hawley, the throughput issues, the validity of the testing issues.

Were there improvements we could make to screening devices by new algorithms, so that the existing sensors might have higher fidelity to see the liquids of interest without having to hold them up to handheld detectors and the time that takes?

And so that is why I went forward with the request for information. I went forward immediately at the same time with the SAFETY Act proposal. And that RFI closed yesterday. We now have over

40 proposals. I am not going to tell the offerers what looks good, what looks bad.

But there are a lot of very intriguing technology proposals and solutions that we are going to take within 30 days of receipt to Socorro or Tyndall Air Force Base, two different setups, and test them against full-scale, meaning 500 milliliter Gatorade-sized bottles, of the actual liquid explosives that we know are being used or proposed by the terrorists. And we will see which works.

And that work we will put on a fast track into an acquisition program to enhance our screeners and our security in TSA. But as I said at my hearing previously, Mr. Chairman, I like the BSAF analogy. I don't make the device, S&T makes the device better.

And so I am fast-tracking to make those devices better, to raise the level of confidence, to reduce the lines and improve the security. And I would tell you there are a lot of wolves on the porch, but this is the wolf closest to my door.

Mr. REICHERT. Well, just another quick follow up. Since you are on the hot seat and you are now on the fast track of this issue, in your short tenure did you identify and have you identified any logjam that may have existed prior to your taking the office in this specific area of detection technology?

Mr. COHEN. I will tell you that in the dual-use world, it is the unintended use or the unintended consequences of technology that tends to give us the breakthrough. So there are many examples in drugs, and I won't, you know, detail those.

But what we are finding is our DOE labs, industry and small laboratories who are working on technologies for other purposes, and when we went out and identified the need for liquid explosive detection, they had the eureka effect. They said wow, I didn't think about this, but this might be used for this purpose.

And that is what we are seeing right now with these respondents. And I am excited about several of them. I think I would like to leave it at that.

Mr. REICHERT. Thank you.

The chair recognizes Mr. Dicks.

Mr. DICKS. Thank you, Mr. Chairman. And I want to thank Secretary Cohen for his great service at the Office of Navy Research over many years, and I enjoyed working with him. And I told him this morning, Mr. Chairman, that I thought it was great to have somebody at S&T who would be a leader.

I mean, I think that is what the Congress basically is saying, is help us figure out a way to implement the SAFETY Act and do it expeditiously. Ninety-three pages, by the way, sounds a little bit long to me.

You know, and I just have a couple questions I want to ask you. One is, some of the statements mentioned concerns about situations where we are going to use a technology, and it is going to be used overseas. I think of the container security initiative, for example.

And how do you work out the liability issues there when, you know, the company that has the technology might be sued in a foreign court? What do we do about that problem? That is one that was mentioned in the panel, two people. What ideas do you have on that?

Mr. COHEN. Congressman, you know it is not my style, but I will have to take that one for the record, because—

Mr. DICKS. Right. That is okay. I think we need an answer to that, though.

Mr. COHEN. Yes, sir.

Mr. DICKS. And we need to work with the industry on how we are going to deal with that situation.

The other thing is I understand that this isn't just for federal procurements, SAFETY Act, that it is also for a situation where a company wants to, you know, protect itself and limit liability on something that he might be selling to the state and local governments or to the private sector for safety purposes. Is that correct?

Mr. COHEN. That is absolutely correct, and—

Mr. DICKS. But I understand that we haven't had one single application approved for that purpose. Is there some reason that people aren't applying for that protection?

Mr. COHEN. Linda?

Mr. DICKS. What I am told by our learned staff back here is that all the applications so far have been for people who were trying to compete for federal procurements, that nobody has come in to try to get liability protection under the SAFETY Act for selling something either to the private sector or state and local governments.

And I was just curious as to why that is. I mean, has there been adequate outreach to these companies? Why haven't they applied?

Ms. VASTA. Sir, I will have to take that one for the record, but I will indicate that in the 7.5 months that I have been the acting director, I don't believe I have seen any applications that have come in under that.

I can assure you that we have an aggressive outreach program planned for the SAFETY Act program which not?

Mr. DICKS. Well, why don't you tell us about that?

Ms. VASTA. Well, to further what Ms. Duke indicated, the outreach program will certainly reach out to the entire procurement community to educate more.

We want to look at obviously not only the larger companies but also the smaller companies and those which not just the companies themselves serve but also to the government, state and local governments, and educate them on the protections that are afforded under the SAFETY Act.

Mr. REICHERT. Could I interrupt just for a second and ask you to state your name and title, please, for the record?

Ms. VASTA. Pardon me, sir. My name is Linda Vasta. I am the acting director of the Office of SAFETY Act Implementation. I have been the acting director since mid February of this year.

Mr. REICHERT. Thank you.

Mr. DICKS. Thank you, Mr. Chairman. I have no further questions.

Mr. REICHERT. Ms. Jackson-Lee?

Ms. JACKSON-LEE. Thank you very much to the chairman and the ranking member and ranking member of the full committee.

And thank you to Mr. Cohen and to Ms. Duke and to the other presenter.

I guess I want to start out with my frustration as well in terms of this whole process that has taken place and, as well, the lack

of fulfillment of a commitment to you now leading the department in terms of being fully staffed.

So I just want to go through a line of questioning to know whether we are real, whether the doors are open and lights are on, because it is interesting that as we approach the election, which those of you who serve us try to stay as far away as possible, I would assume, but it is, of course, in the backdrop of 9/11, a rising highlight.

What are we doing about homeland security? And the SAFETY Act's good intentions were we are at the cutting edge of technology. That was in 2002. And we are now facing a situation where, one, the pipeline has been slow, and the staffing that would help streamline the pipeline along with the new changes is slow as well.

So take me through your department right now. Tell me what kind of team do you have in existence and do you intend to put together to make this work.

The other concern that I have is to the private sector. And there are no entities more creative than those who already have money. And that, of course, is the business sector who successfully are on the cutting edge and hopefully have a big sign and therefore they are being rewarded in the capitalistic system.

My thought of this legislation was to ensure that we are seeking the cutting edge small guys and gals in the hinterlands, don't have access, but really have brainpower and have something that is really going to turn the corner of homeland security technology.

So I want to know what you are doing to ensure that the large giants—and I have no angst with them—already getting ready to put Product A on the market 2 weeks from now, and they have got an application at your door, versus the Colorado mountain person who is in the mountains with their single lab, or the university labs, and they are on the verge of discovery and yet may not even be aware of the SAFETY Act, and certainly don't have the wherewithal in the midst of their research to get your attention. What kind of outreach will you have on that?

And then I would be interested, as well, in—and I have looked through the bill, and I thought, well, this must be what I missed, but I am going to read it again in the minority and small business outreach.

I know there is a general procurement element here, but I think, Secretary Cohen, we want to know what your mission and message is with respect to minority-serving institutions who have been the second-class citizens as relates to research and anyone knocking on their door to find out—either to encourage them to engage in this or to find out what they are doing, and specifically, of course, Hispanic-serving institutions and historically black colleges.

With that, I will yield to you for a moment and hope maybe I will have a moment more to ask a question.

Secretary Cohen, thank you for your service.

Mr. COHEN. Thank you very much, Congresswoman Jackson-Lee. And, you know, this weekend I was down in Galveston, Texas, for the first time.

Ms. JACKSON-LEE. Excellent. You are in the right place, then.

Mr. COHEN. And went down with my wife on my own nickel. We went down for the commissioning of the USS Texas—

Ms. JACKSON-LEE. Yes.

Mr. COHEN. —and it was a wonderful event. About 7,000 people showed up, and it didn't rain until 15 minutes after—

Ms. JACKSON-LEE. It was outstanding.

Mr. COHEN. —the event. And, you know, when people heard I was in Homeland Security, first they thanked me for my service, and then they came up to me with ideas. And this is what I find all around the country.

And serendipitously, I sat next to the port director, and we have an experiment going on right now, one of three ports in Galveston, on container security, safety, et cetera, and we had a wonderful interchange. And I look forward to re-engaging with him.

But your questions are right on the mark, and so let me take them one at a time. I think if we can go ahead and put up the existing organization, I think this goes to meet Mr. Meek's comments, because I think he and I are actually in violent agreement.

It is not about process. It is about product. It is about the end result. It is about the security. It is about bringing, as Congressman Pascrell said, the cutting-edge technologies to the fight. And we have a long history in this country of doing that. It is not a pretty process. Science and technology, discovery, invention are not a pretty process.

But where we are going, and we are going there very quickly, and it is part of my confirmation process. And also at Chairman Reichert's hearing last week I was asked about the morale of my directorate. I was asked about the turnover. I was asked about the understaffing, et cetera.

And in the end, I believe in success-oriented organizations. I only served with volunteers. I expect them to work hard, to be rewarded and to achieve success, and that is mission success.

And I had an all-hands yesterday with over 500 of my people, laid out the new organization, which Secretary Chertoff kindly approved last Wednesday, which was briefed to the Hill and all the staffers.

I am so pleased with the bipartisan, non-partisan reception that I have received by the staff and the members. It is what I am used to from defense. And I think that is totally appropriate and heartwarming in the area of homeland security, as you have indicated.

Ms. JACKSON-LEE. So how many do you have on staff now?

Mr. COHEN. Right now, we have 16. I have one government service employee. She has three assistants. And then we are using IDA, the Institute for Defense Analysis, on a contract basis to do the technical evaluation.

Of course, those individuals must recuse themselves. They must not have holdings, all of the appropriate safeguards relative to the technologies and the companies that they are evaluating.

Ms. JACKSON-LEE. And how many more do you need?

Mr. COHEN. We do need more, absolutely, we do need more.

Ms. JACKSON-LEE. How many?

Mr. COHEN. This is the organization. I would like Ms. Vasta just to quickly walk through that, so that you see the rational approach that we are trying to take. I know time is short. She will make it very quick.

Ms. VASTA. As the undersecretary alluded to, we currently have one federal employee. That, of course, is me. I have been acting in that position since mid-November of this year.

The proposal is that we have a director for the office, which would be a federal employee; a deputy director, a program manager, and I am pleased to report that that acquisition is in process.

Of course, that individual would be continuing to be supported by the contract support staff. In addition to the other federal employees that are proposed, we are looking at an economic director, as well as a technical director, as well as an outreach coordinator. These are all full-time federal employee positions.

And at some point, we hope to seek funding for an on-site attorney in that office.

Ms. JACKSON-LEE. Right now those are all vacant? What you just listed are vacant?

Mr. COHEN. I would like to say, again, this is the organization that I am going to—in 3 weeks, since coming on board the 10th of August, the secretary has approved a total reorganization which is now in place.

This is a subset of that. I am used to, being a submariner, having very small groups of officers and crews, and we dual-hat. We have collateral duties.

So as we put this new organization in effect over the next several weeks, and that is the time frame for this organization. I will not hesitate to reach down into the talent that I enjoy—my scientists, engineers and program managers—and dual-hat them as necessary to ensure that we get this off to the right start, because you saw from the chart, the histogram, SAFETY Act is a growth industry, which is what we wanted all along.

Ms. JACKSON-LEE. Mr. Chairman, I ask unanimous consent for an additional 1 minute, because he did not finish the last two answers.

And if you could quickly do that on the choice between big companies and small. I would only just answer my own question. I hear you, but right now these are vacant positions. And I will just—

Mr. COHEN. Yes, ma'am.

Ms. JACKSON-LEE. All right. But can you just answer the last two—

Mr. REICHERT. The gentlelady's time has expired.

Mr. Cohen, please answer the question that the chair—

Ms. JACKSON-LEE. Thank you. An additional 1 minute—

Mr. REICHERT. —because the chair has a reputation for being generous with his time, but we have a second panel with five witnesses, so if you could—

Ms. JACKSON-LEE. Thank you. If you could quickly answer, I would appreciate it. Thank you.

Mr. COHEN. My record at Naval Research is strong in outreach and with historically black and minority institutions. To me, the outreach should be an integrated outreach, as Ms. Duke has indicated.

Everywhere we go, we need to talk about the SAFETY Act. We need to talk about the authorities that you have given me of the transaction, et cetera. That will kick-start people coming in.

I am not going to share with you my own prejudices of big companies versus small companies of cutting-edge technology, but I think you had it exactly right.

And Thomas Friedman, in "The Earth is Flat"—and we addressed this last week—he had to revise his book because he was giving credit to Bangalore and China, and he was badmouthing American innovation, and he had it wrong.

And he has admitted that now publicly, because it is about the innovation that we enjoy and the system of government that we have that allows protection of intellectual property and allows people to be the best that they can be.

And we have not yet begun to tap all of those sources, and I commit to you the things that I did in Navy I will do in Homeland Security. That is what I have been asked to do. And we will have a very wide blanket.

Ms. JACKSON-LEE. Thank you.

Mr. REICHERT. The chair recognizes Ms. Christensen.

Ms. JACKSON-LEE. Thank you very much.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

I am going to just ask one question in the interest of time about the appeals process for the SAFETY Act application, because the rules do not allow any opportunity for an administrative or any kind of appeal.

And I guess it is you that has the final word, and no question. No question can be asked. So that seems to send the wrong message, and I know that it comes up in at least one of the next panelists' testimony, and I wonder if you would respond to that.

Why is it that there is no appeals process?

Mr. COHEN. Well, Ms. Christensen, I am not omniscient. I have been known to make mistakes. people who work for me may make mistakes.

And to the extent that we can do process improvement, I look forward to the thoughts of the next panel and working with industry, working with our customers, because you are right, I don't want to send any message that in any way limits participation.

We live in a democracy, and I believe that should pervade all of our processes.

Mr. REICHERT. Thank you. I would like to thank the witnesses for your valuable testimony. This panel is excused.

And I would ask that the second panel take their seats, please.

Welcome. Thank you for being here today. We appreciate your taking time to be with us.

We all have very busy schedules. And if I could just remind the witnesses to abbreviate your testimony and allow us time to ask questions. I know some of the other members have to move on to other appointments.

First, I would like to recognize Mr. Howell, the vice president of the homeland security policy division for the U.S. Chamber of Commerce to testify.

Mr. Howell?

STATEMENT OF ANDREW HOWELL, VICE PRESIDENT, HOMELAND SECURITY POLICY DIVISION, U.S. CHAMBER OF COMMERCE

Mr. HOWELL. Thank you. I would like to thank Chairman Rogers, Chairman Reichert, Representative Meek and Representative Pascrell and all members of the two subcommittees for the opportunity to testify here today.

My name is Andrew Howell, and I am vice president of homeland security policy at the U.S. Chamber of Commerce.

The chamber represents more than 3 million businesses through our federation, which includes direct corporate members of all types and sizes, trade and professional associations, state and local chambers of commerce and 104 American chambers of commerce around the world.

I would like to express our appreciation to the subcommittees for holding this hearing on the SAFETY Act. The program is one of the few incentives to spur the development and deployment of cutting-edge technologies, services and systems to protect our homeland.

Ensuring the security of our citizens should be America's top priority. The SAFETY Act is an important tool to realize that objective.

The chamber applauds the Department of Homeland Security's efforts to ensure that the SAFETY Act provides the protections intended by Congress.

The final regulations issued in June provide needed certainty in several areas: The definition of an act of terrorism, coordination of the timing of SAFETY Act awards with antiterrorism procurements, explanation of the relationship between the SAFETY Act and indemnification, and a process for SAFETY Act protections en masse through block designations and block certifications.

Additionally, we were pleased to see a process for SAFETY Act awards when products are in the developmental test and evaluation phase. Let me now expand on each of these areas.

Terrorism is a global issue that demands a global policy response. However, U.S. regulation does not easily reach foreign shores. Given this reality, how can we protect firms providing antiterrorism technologies abroad?

In the final SAFETY Act regulation, DHS notes, "The department does not interpret the language of the SAFETY Act to impose a geographical restriction for purposes of determining whether an act may be deemed an act of terrorism."

Additionally, the regulation says that an act on foreign soil may indeed be deemed an act of terrorism for purposes of the SAFETY Act, provided that it causes harm in the United States. The department interprets harm in this context to include harm to financial interests.

We agree with this approach, which protects vendors advancing U.S. homeland security policy interests by deploying technology abroad. At the same time, there may be areas where this definition is not sufficient. Therefore, in some cases, it will be necessary to combine SAFETY Act protections with indemnification offered by Public Law 85–804.

We are pleased that DHS in the final regulation acknowledges this approach "might appropriately be made available." We look forward to further guidance in this area.

Regardless, however, of the location of antiterrorism technology deployments, DHS has struggled to coordinate acquisition and procurement with the SAFETY Act award determinations. We have heard a little bit about that.

Recent DHS practice as well as the text of this final SAFETY Act rule demonstrate its progress. The advanced spectroscopic portal monitor and SBInet procurements which were mentioned earlier are steps in the right direction.

However, consideration of SAFETY Act has consistently been left until after the release of DHS procurements. Acquisition professionals, in our view, should systematically consider the SAFETY Act early in the acquisition process, not at the end.

Another area where DHS has made progress is in the block designations and block certifications, which would award SAFETY Act to vendors whose solutions or products meet a predetermined specification. We would like to see details on how this good idea will work.

At the same time, the block designation section of the new SAFETY Act application is the only reference to a streamlined process, which is essential. We are eager to see specifics in this area.

One more area I would like to cover is developmental test and evaluation designations. By providing coverage in this area, the new regulation embraces the spirit of the SAFETY Act, which was to spur the development of new technologies.

We are keen to see how this process will function and will work with DHS to ensure that it works smoothly and effectively.

Clearly, in our view, DHS has made great strides in this new regulation and new application kit. At the same time, DHS must implement several new and updated business processes for the SAFETY Act to reach its potential.

The first is the new application kit now open for comment. This kit asks applicants for the information that DHS is actually now using to make decisions. Of course, there is still room for refinement. We also hope that DHS will soon publish a streamlined SAFETY Act kit.

Last year, the chamber joined with the Professional Services Council and others to provide recommendations in this area. We are eager to see how DHS utilizes our suggestions.

In conclusion, we congratulate DHS for all the work done to implement the SAFETY Act more effectively and efficiently. At the same time, government and industry must continue working in partnership for this program to realize its potential to protect the American public.

Thank you for this opportunity to testify today, and I look forward to any questions or comments you might have.

[The statement of Mr. Howell follows:]

PREPARED STATEMENT OF ANDREW HOWELL

Introduction

I would like to thank Chairman Rogers, Chairman Reichert, Representative Meek and Representative Pascrell, and all Members of the Subcommittee on Management,

Integration and Oversight, as well as the Subcommittee on Emergency Preparedness, Science and Technology, for giving me the opportunity to testify before you today.

My name is Andrew Howell, and I am the Vice President for Homeland Security Policy at the U.S. Chamber of Commerce. The U.S. Chamber of Commerce ("the Chamber") is the world's largest business federation, representing more than 3 million businesses through our federation, which includes direct corporate members of all types and sizes; trade and professional associations; state and local chambers through the United States; and 104 American Chambers of Commerce abroad (AmChams) in 91 countries.

On behalf of the Chamber, I would like to express our appreciation to the two subcommittees for providing this opportunity to comment on the implementation of the "Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act)". We applaud your efforts to bring attention to this important program, which is one of the few incentives offered to spur the development and deployment of cutting-edge technologies, services and systems to protect our homeland. The Chamber believes that ensuring the security of our citizens should be America's top priority. The SAFETY Act is an important tool necessary to realize that objective, and one that helps to harness the creativity and innovation of the private sector. We look forward to working with members of this committee, and the appropriate subcommittees, as you conduct important oversight of this key DHS program.

The Final SAFETY Act Implementing Regulation

The Chamber applauds the Department of Homeland Security in its efforts to ensure that the SAFETY Act provides the full protections intended by Congress. The final regulations issued on June 8, 2006 provide much-needed certainty on this critical program in several key areas:

- The definition of an act of terrorism;
- Coordination of the timing of SAFETY Act awards with important federal anti-terrorism procurements;
- Explanation of the relationship between the SAFETY Act and indemnification under Public Law 85-804; and
- A concrete process for the use of SAFETY Act protections en masse through "block designations and "block certifications."

Additionally, we were pleased to see an explicit process for SAFETY Act awards when products are in the developmental test and evaluation phase, which can either test a promising anti-terrorism technology or identify something that may form the basis for future anti-terrorism technologies.

Let me now expand on each of these areas, which we consider to be among the most important parts of the new regulation.

Definition of an act of terrorism

As you know, terrorism is a global issue that demands a global policy response. For example, Homeland Security Presidential Decision Directive 13 notes that:

> *The security of the Maritime Domain is a global issue. The United States, in cooperation with our allies and friends around the world and our state, local and private sector partners, will work to ensure that lawful private and public activities in the Maritime Domain are protected against attack and criminal and otherwise unlawful or hostile exploitation.*

Additionally, the Container Security Initiative, announced several years ago by former Customs and Border Protection Commissioner Robert Bonner, is based on the principal of "pushing our border out" by stationing U.S. Customs and Border Protection officers at foreign ports shipping goods to the United States.

However, as we all know, U.S. regulation does not easily reach foreign shores. Given this reality, in the context of the SAFETY Act and the global nature of our homeland security policy, how can the government effectively protect firms providing anti-terrorism technologies abroad, where U.S. regulations have limited impact?

Recognizing the need to think differently on the liability threat facing firms selling anti-terrorism technologies that would carry out U.S. policy objectives, our comments in August of 2003 on the proposed SAFETY Act regulation, pointed out the need to clarify the definition of an "Act of Terrorism" to provide clarity for vendors selling anti-terrorism technologies for deployment abroad.

In the final SAFETY Act implementing regulation, DHS offers thoughtful language in this regard, noting that "The Department does not interpret the language of the [SAFETY] Act to impose a geographical restriction for purposes of determining whether an act may be deemed an 'Act of Terrorism'". Additionally, the regulation notes that "an act on foreign soil may indeed be deemed an 'Act of Terrorism' for purposes of the SAFETY Act provided that it causes harm in the United

States. The Department interprets 'harm' in this context to include harm to financial interests."

In our view, this appropriately protects vendors with financial interests—including equity stakes, shareholders, plants, assets and the like—from an Act of Terrorism abroad if it affects the value of those financial interests in the United States.

Relationship between the SAFETY Act and indemnification under Public Law 85–804

At the same time, there may be areas where this definition does not sufficiently protect a firm with an overseas deployment of technology—particularly if a product liability lawsuit is brought in a court outside of the United States.

Therefore, we believe it is necessary, in some cases, to combine SAFETY Act protections with the benefits of Public Law 85–804, which allows the Government to indemnify private parties acting on the Government's behalf. In our view, those deploying anti-terrorism technology abroad in support of U.S policy to push our borders out, are, in effect, acting on the government's behalf. Therefore, these technologies would be obvious candidates for a dual track SAFETY Act/P.L. 85–804 approach.

This is something we have been calling for since our comments of August 2003 on the Proposed Implementing Regulations for the SAFETY Act. We are pleased that the department, in this final regulation, acknowledges that a combined SAFETY Act/P.L. 85–804 approach "might appropriately be made available." At the same time, we look forward to seeing further guidance from DHS in this area so that important programs with both domestic and international deployments—like perhaps SBINet—can benefit from a strong pool of bidders, undeterred by potential liability concerns.

Coordination with anti-terrorism procurements

Regardless of the location of the anti-terrorism technology deployment, however, one very basic element of a comprehensive SAFETY Act program implementation has been lacking—coordination between acquisition and procurement and SAFETY Act determinations.

The Chamber, in collaboration with our members and several other trade associations, has been working hard with procurement officials and DHS leadership to build SAFETY Act provisions into important procurements. However, this approach has been haphazard and has too often been in reaction to a procurement that has already been issued.

Recently, as well as in this final SAFETY Act rule, DHS has appropriately recognized the need to coordinate SAFETY Act benefit determinations with acquisition and procurement operating procedures. The establishment of a "Pre-Qualification Designation Notice," is a good tool for federal buyers to use during the early stages of acquisition and would be accompanied by an "expedited review of a streamlined application for SAFETY Act coverage. . .and, in most instances, establish the presumption that the technology under consideration constitutes a QATT" (i.e. qualified anti-terrorism technology), according to the new regulation.

We are also pleased to see this rule states that the Office of SAFETY Act Implementation (OSAI) may also expedite applications for vendors responding to an ongoing solicitation and that the Department may unilaterally decide that a procurement is eligible under the SAFETY Act. While there are still details to be worked out—for example, the timeline for an application being expedited—these are all steps in the right direction.

However, all the process improvements in the world will not help unless DHS simultaneously strengthens its procurement and acquisition corps. We need to find a way to help DHS procurement officials better research markets; plan their procurements; develop meaningful performance metrics; and buy goods and services cost effectively. Incorporating the SAFETY Act into the process of planning an acquisition is essential, and because it is a new program, training will be absolutely essential. By taking the time to carefully consider performance metrics, liability concerns and the role of the SAFETY Act prior to developing and issuing a request for proposals (RFP), our government, our citizenry and the anti-terrorism technology vendor community can do a better job managing risk and protecting our homeland.

Block designations and block certifications

Another area where DHS has made significant progress in this final regulation is the strong statement made for block designations and block certifications. The department decides that all solutions or products that meet a certain specification can be deemed to have streamlined SAFETY Act reviews.

From our perspective, there are several programs where this mechanism should be used in the near term. One that comes to mind is the Registered Traveler (RT)

program. Vendors of RT solutions, as you may know, will all have to meet a certain specification set by the Transportation Security Administration. Therefore, it would make sense to designate or certify this group of services, which will be more widely deployed later this year.

At the same time, it is worth noting that the block designations section of the new SAFETY Act kit is the only place in the entire document that makes mention of a "streamlined" process. We believe that there are many areas where DHS can and should streamline the technology evaluation process, and we are eager to understand how the Department intends to carry this out.

Developmental test and evaluation efforts

One final area in the final regulation that merits attention is the section on developmental testing and evaluation designations. The SAFETY Act is designed to spur the development of new technologies; this specific category of SAFETY Act application provides further details on exactly how DHS plans to work with industry partners to protect them from liability in the risky, early stages of a program. We all know that liability can, indeed, extend all the way back to the development phases of a technology. Therefore, awarding SAFETY Act benefits is entirely appropriate.

Of course, once the benefits of the developmental test and evaluation segment of a SAFETY Act certification's benefits have expired—presumed to be 36 months in the regulation and kit—some applicants will, we hope, want to extend their coverage. How DHS handles the continuation of benefits—whether a firm has to fill out an entirely new kit, simply file a modification application, or exercise some other alternative—will need to be worked out. We are eager to see exactly how that process will work, and we will work with DHS to ensure that it functions smoothly and effectively for both the government and the applicant.

Beyond the Implementing Regulations—Making the SAFETY Act Reach its Potential as an Anti-Terrorism Tool

In order to make the SAFETY Act reach its true potential, DHS must implement several new and updated business processes.

The first such process is a new application kit. Now open for public comment, we believe this new kit effectively asks applicants for the information the Department is now actually using to make evaluation decisions. At the same time, while the questions asked are more precise and better guide applicants to provide the right data, we believe the overall burden on the applicants does not, at this point, seem to be reduced.

Therefore, we hope that DHS will continue to work with us and others to limit the amount of information that application evaluators seek, while also making the SAFETY Act process as effective as possible.

We also hope that DHS will soon develop and publish a streamlined SAFETY Act kit. In September, the Chamber joined with a host of other organizations—including the Professional Services Council, the National Defense Industrial Association; the Information Technology Association of America and the Aerospace Industries Association—to develop our version of an effective, streamlined kit for use in specific circumstances. Attached for the record is a letter transmitting our vision of an effective streamlined kit, complete with instructions for DHS.

In this document, we focused on gaining efficiencies and reducing redundancies across the Department. In our view, there is significant overlap between the SAFETY Act office's evaluation process and the review a procurement officer leads when assessing the efficacy of a product, service or integrated solution. As a result, we believe that for purposes of the SAFETY Act, deference can and should be given to the procurement evaluation—whether for an ongoing solicitation or for a prior procurement.

Of course, with regard to procurement, we must congratulate DHS officials for the many strides they have made to more effectively link SAFETY Act determinations and procurement awards. DHS thoughtfully issued a revised Request for Proposal (RFP) for its Advanced Spectroscopic Portal monitor procurement that included SAFETY Act protection for the winning bidder after realizing the liability challenges vendors would face from deploying this bleeding-edge technology. On its SBINet procurement, DHS included language in the original document, and then supplemented it with subsequent modifications.

However, in both of these cases, the SAFETY Act was omitted in the initial procurement process, leaving thoughtful DHS officials to address the liability issue once bidders began asking how their liability concerns would be addressed. As we all know, issuing a procurement is the end of a process which begins with market research and continues through the establishment of program requirements and metrics. To date, federal government acquisition professionals have not systematically included consideration of liability issues—and utilization of the SAFETY Act

to mitigate those issues—early in the overall acquisition process. As a result, those of us working on this program from the outside are left at the very last moment—preparation of a request for proposals—to try and have the SAFETY Act integrated into the procurement.

In order to achieve this, changes must be made to both the Department's acquisition regulations as well as the Federal Acquisition Regulation (FAR). We understand both are underway, and that is to be applauded. As soon as the Department and the FAR Council (which recommends changes to the federal purchasing rules) finish their work, the SAFETY Act can systematically be integrated into anti-terrorism procurements across the government

Once these steps have been taken, of course we anticipate there would be aggressive training of acquisition and procurement staff across the government. DHS and other federal acquisition and procurement officials need to better understand the SAFETY Act and appreciate how it provides benefits to buyers and vendors.

At the same time, guidance for state and local buyers—especially those receiving federal money to buy anti-terrorism equipment, services, technology and the like—is essential. Because federal tax dollars are being spent to secure our homeland at the local level, and because the SAFETY Act is not just for federal anti-terrorism procurements, DHS officials should find ways to educate the state and local homeland security community. By taking this step, state and local officials could either incorporate the Act into their acquisition process or buy technology that has already been certified or designated as a qualified anti-terrorism technology by DHS.

Of course, since 85% of our critical infrastructure is in private sector hands, this is also an important community that needs to appreciate the SAFTEY Act's benefit. Important steps have been taken in this regard, most recently through the release of the National Infrastructure Protection Plan, which includes a section on the SAFETY Act and outlines its benefits for critical infrastructure owners and operators.

Conclusion

In conclusion, we congratulate DHS for drafting and issuing a final rule that sets the appropriate legal framework for the deployment of anti-terrorism technologies, services and systems by federal, state, local and commercial buyers. This regulation will help make us safer by providing needed protection for vendors and buyers.

We also would note the excellent work that has been done drafting a new application kit that effectively implements this regulation.

At the same time, more needs to be done to have this program realize its true potential. As I have just outlined, issuing a new application kit with streamlined review processes; building the SAFETY Act into the acquisition process early on; training procurement and acquisition officials at all levels of federal, state and local government; modifying internal DHS acquisition rules; and concluding the FAR Council's work to provide needed guidance for federal government buyers are all essential steps.

Collectively, these steps will create a more robust homeland security environment where sellers of anti-terrorism technology innovate and deploy tools that most effectively protect the American public.

We thank you for this opportunity to testify today, and hope that this Committee will continue to exercise appropriate oversight to ensure that this program works to enhance the security of our homeland. We stand ready to assist you as you move forward in this effort.

Mr. REICHERT. Thank you, Mr. Howell.

The chair now recognizes Mr. Meldon.

STATEMENT OF MICHAEL MELDON, EXECUTIVE DIRECTOR, HOMELAND SECURITY AND DEFENSE BUSINESS COUNCIL

Mr. MELDON. Thank you, Mr. Chairman. Just before I start my remarks, may I say that I was one of the people that participated in the call that Undersecretary Cohen had with industry about liquid explosive detection.

There was a sense of urgency in that call. He took action. When the call to action went out, industry responded, and that is evinced by the actions and the responses that he go back. So we applaud that action, and we want to commend him for that.

Good afternoon, Chairman Rogers, and Chairman Reichert and distinguished members of the subcommittee. My name is Michael Meldon, and I am the executive director of the Homeland Security and Defense Business Council.

I am testifying on behalf of our member companies. The Homeland Security and Defense Business Council is a non-profit, nonpartisan organization that represents good governance and successful program outcomes.

The council offers straight talk and honest assessments of programs, technology and processes that are integral to the mission of the Department of Homeland Security.

The council's goal is to be a world-class private-sector component and partner to the public sector in all significant areas of homeland security, to include risk mitigation, mission effectiveness and management efficiency.

The council appreciates the opportunity to present our industry perspective on the SAFETY Act final rule recently released by the department.

There are a number of very positive changes that have occurred in the business processes and guidelines surrounding the SAFETY Act. To highlight some of these, the final rule makes these changes to the SAFETY Act.

A, it provides that technology includes services as well as equipment and software.

B, it removes the need for antiterrorism technology sellers to offer insurance coverage to third persons for acts of suppliers, vendors and subcontractors used to supply that technology.

C, lets a seller of qualified antiterrorism technology make changes to the product that modify its capabilities without approval by or even notice to DHS, and without the loss of the liability protections provided by the SAFETY Act.

D,, grants DHS the right to create so-called block designations and certifications for certain categories of antiterrorism technology.

And finally, addresses DHS's policy on safeguarding proprietary information regarding applications for antiterrorism designation and certification.

The new rule also addresses the application evaluation timeliness issues. We have seen from an industry perspective the information provided in the department's announcement of the final rule states that in the first 16 months following the passage of the SAFETY Act, six QATs, qualified antiterrorism technologies, were approved, and an additional 68 technologies were approved by March of 2005.

What this does not address is the number of applications that have been received by the department for which no action has been taken, and we are hopeful that as a result of the changes these applications will be expeditiously adjudicated.

Several issues remain in the SAFETY Act and its intended implementation, and I will focus the remainder of my time on those issues.

Number one, anticipated changes in the insurance industry. Insurance companies and the federal government paid more than 90 percent of the $38.1 billion awarded to victims of the 9/11 terrorist attacks, according to a 2004 study by the RAND Corporation.

Secondly, because of concerns about an avalanche of claims, Congress capped liability for airlines, airports, ports and cities and established the 9/11 Victim Compensation Fund of 2001.

To use it, recipients had to waive the right to sue. Still, about 70 families eventually filed wrongful death suits against the airlines.

Third, the potential liability exposure continues to be closely examined by the insurance industry as well as others, and the business considerations that resulted from that review are being implemented through new policy terms and conditions.

And finally, thankfully the United States has not suffered a terrorist attack or resulting lawsuit since the fall of 2001, so the protections of the SAFETY Act haven't come into play. But industry's concern about liability is no less real.

The government contractor defense. One, implementation and guidance regarding the government contractor defense is noted in the final rule as an area where DHS still owes industry specific direction and policies and procedures.

Two, the presumption of the government contractor defense applies to all approved qualified antiterrorism technologies for all claims brought in any kind of lawsuit arising out of, relating to, resulting from an act of terrorism when qualified antiterrorism technologies have been deployed in defense against or response or recovery from such act, and such claims may result or may result in loss to the seller.

While the government contractor defense is a judicially created doctrine requiring the contractor provider to provide essential elements in order to qualify for the defense, the SAFETY Act supplants the case law so that once the secretary approves the application for this additional protection, the government contractor defense applies.

Three, the statutory government contractor defense available under the SAFETY Act provides immunity not only against all claims that might be brought by third parties relating to sales to the government, it also applies to purely private transactions.

Fourth, under existing case law the government contractor defense is available only if the contractor manufactured the product in question in accordance with reasonably precise federal government specifications. And this is important.

Under the SAFETY Act, this is not the case. In reviewing an application, the secretary will perform a comprehensive review of the designation 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 act also provides that the seller will conduct safety and hazard analysis and supply such information to the secretary.

Next, this suggests that unlike the existing judicially crated government—

Mr. REICHERT. Mr. Meldon, excuse me. Could I ask you shorten and be brief in your closing comments? I am going to lose two members here in the next few minutes, and we want to give them some time to ask a question or two.

Mr. MELDON. Absolutely.

Mr. REICHERT. Sorry.

Mr. MELDON. Not at all. Let me summarize, then.

The proposed rule clearly adopts broad protections provided by the case law to the SAFETY Act version of the government contractor defense.

Next is the secretary may designate a technology as qualified antiterrorism technology, and he must examine the amount of liability insurance that the seller intends to maintain for coverage of the technology and certify that that level is appropriate, so that the secretary predetermines the amount of secondary coverage that industry needs for qualified antiterrorism technology.

Under accuracy and completeness, we note that that is also determined by the secretary in his review and is not against any particular federal standard that we are aware of at this time.

Modifications to qualified antiterrorism technology may occur on an ongoing basis. This raises the issue, however, that deals with QAT that has undergone in-place upgrades and enhancements without specific DHS review.

And finally, we want to reiterate the council's view that a number of very positive changes have occurred in the business processes and guidelines surrounding the SAFETY Act and that, in general, we are pleased with the modifications.

And we want to congratulate and commend the secretary of the Department of Homeland Security for his personal involvement in the final rule and the new regulations. Thank you very much.

[The statement of Mr. Meldon follows:]

PREPARED STATEMENT OF MICHAEL M. MELDON

Good afternoon, Chairman Rogers, Chairman Reichert, and distinguished members of the subcommittee. My name is Michael Meldon and I am the Executive Director of the Homeland Security and Business Council. I am testifying on behalf of our member companies. The Homeland Security & Defense Business Council is a non-profit, non-partisan organization that represents good governance and successful program outcomes. The Council offers "straight talk" and honest assessments of programs, technology, and processes that are integral to the mission of the Department of Homeland Security. The Council's goal is to be a world class private sector component and partner to the public sector in all significant areas of homeland security to include risk mitigation, mission effectiveness, and management efficiency.

The Council appreciates the opportunity to present our industry perspective on the SAFETY Act Final Rule recently released by the Department of Homeland Security.

There are a number of very positive changes that have occurred in the business processes and guidelines surrounding the SAFETY Act. To highlight some of these, the final rule makes these changes to the Safety Act:

- ***Provides that a technology includes services as well as equipment and software.*** This means maintenance contractors may be entitled to liability protection if they service equipment used for anti-terrorism purposes, or if they provide design, consulting, analysis or other professional services.
- ***Removes the need for anti-terrorism technology sellers to offer insurance coverage to third persons for acts of suppliers, vendors and subcontractors used to supply the technology.*** This expands the bargain struck in the Safety Act, which exchanged limitations on the seller's legal liability to the public for a requirement that the seller get liability insurance coverage.
- ***Lets a seller of a qualified anti-terrorism technology make changes to the product that modify its capabilities without approval by, or even notice to, DHS, and without loss of the liability projections provided by the Safety Act.*** Under the interim rule, a seller that made significant modifications to the technology that reduced its capabilities could lose its liability protection as of the time the change was made. Under the final rule, however, if the product modification is so significant that the product would no longer qualify for liability protection, and then the seller is required to give notice to DHS. The product retains the liability protections until DHS takes affirmative steps to terminate its qualification.

• ***Grants DHS the right to create so-called block designations and certifications for certain categories of anti-terrorism technologies.*** Sellers whose technologies fall within these will not have to demonstrate their technology's technical merits. They will be entitled to receive the liability protections simply by submitting an abbreviated application showing that the technology is covered by the pre-approved block determination.

• ***Addresses DHS' policy on safeguarding proprietary information regarding applications for anti-terrorism designation and certification.***

The new rule also addresses the application evaluation timeliness issues we have seen from an industry perspective. The information provided in the Department's announcement of the Final Rule (6 CFR Part 25, [USCG–2003–15425]/RIN 1601–AA15) states that in the first 16 months following the passage of the SAFETY Act, 6 QATT's were approved and an additional 68 technologies were approved by March 2005. What this does not address is the number of applications (thought to be in the hundreds) that have been received by the Department for which no action has been taken.

Several issues remain in the SAFETY Act and its intended implementation and I will focus the remainder of my time on these issues.

Anticipated changes in the insurance industry

The SAFETY Act was designed to encourage firms to bring homeland security products to market by eliminating the "bet-your-company" risk that might turn some of them away. Insurance companies and the federal government paid more than 90 percent of the $38.1 billion awarded to victims of the Sept. 11 terrorist attacks, according to a 2004 study by the nonprofit RAND Corp. Because of concerns about an avalanche of claims, Congress capped liability for airlines, airports, ports and cities and established the Sept. 11 Victim Compensation Fund of 2001. To use it, recipients had to waive their right to sue. Still, about 70 families eventually filed wrongful death suits against airlines. Plaintiffs also sued the former Riggs Bank—alleging that lax oversight facilitated the financing of two hijackers—and 12 families of firefighters sued Motorola Inc. and New York City over faulty hand-held radios. That suit later was thrown out of court. The nature of these suits and the potential liability exposure was closely examined by the insurance industry as well as others and the business considerations that resulted from their review are being implemented through new policy terms and conditions.

Thankfully, the United States has not suffered a terrorist attack, or resulting lawsuits, since the fall of 2001, so the protections of the SAFETY Act haven't come into play. But industry's concern about liability is no less real. Large contractors bolstering the blast-resistance of bridges, ports and other hard targets; system integrators designing buildings and technological systems; manufacturers of infrared cameras and motion detectors on the border; and biotech firms supplying vaccines all could face lawsuits after a terrorist attack.

Government Contractor Defense

Implementation and guidance regarding the Government Contractor Defense is noted in the Final Rule as an area that DHS still owes industry specific direction and policies/procedures.

The presumption of the government contractor defense applies to all "approved" qualified anti-terrorism technologies for all claims brought in any kind of lawsuit "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." While the government contractor defense is a judicially created doctrine requiring the Contractor/Provider to prove essential elements in order to qualify for the defense, the SAFETY Act supplants the case law so that once the Secretary "approves" the application for this additional protection, the government contractor defense applies.

Significantly, the statutory government contractor defense available under the SAFETY Act provides immunity not only against all claims that might be brought by third parties relating to sales to the government, it also applies to purely private transactions. Thus, once the Secretary "approves" a qualified anti-terrorism technology for this additional protection, the Contractor/Provider is immune from liability relating to sales of that technology in the commercial sector.

Moreover, under the case law, the government contractor defense is available only if the contractor manufactured the product in question in accordance with reasonably precise federal government specifications. Under the SAFETY Act, that is not the case. In reviewing an application, the Secretary will perform 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 Act also provides that the Seller will "conduct safety and hazard analyses" and supply such information to the Secretary.

Thus, unlike the existing judicially created government contractor defense, the DHS statutory government contractor defense will protect Contractor/Providers of technology in the commercial marketplace and will allow qualified anti-terrorism technologies to be approved for such treatment even if a federal specification is not involved.

The proposed rule clearly adopts the broad protections provided by the case law to the SAFETY Act's version of the government contractor defense. The proposed rule recognizes that the scope of the defense is very broad, and expressly states that Sellers of "approved" qualified anti-terrorism technologies cannot be held liable under the SAFETY Act for design defects or failure to warn claims (unless the presumption is established through evidence that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary in connection with its application). As noted above, applications to gain this protection may be submitted simultaneously with the application for "designation" as a qualified anti-terrorism technology. The immunity provided by the statutory government contractor defense is a remarkable protection afforded to sellers of anti-terrorism technologies, and we expect most sellers of such technologies to submit applications.

The court and case law test of DHS' interpretation will unfortunately be played out against another tragedy (hopefully averted) and the use of the DHS statutory rule which may come under pressure since it departs from the current PL 85–804.

Exclusive Federal Jurisdiction and Scope of Insurance Coverage

The Final Rule establishes that before the Secretary may designate a technology as a qualified anti-terrorism technology, he must examine the amount of liability insurance the Seller intends to maintain for coverage of the technology and certify that the coverage level is appropriate to satisfy otherwise compensable third-party claims that may be caused by an act of terrorism when qualified anti-terrorism technologies have been implemented. The SAFETY Act also provides that Contractor/Providers are not required to obtain insurance in excess of the maximum amount reasonably available that would not unreasonably distort the sales price of the anti-terrorism technology.

The rule states that the Secretary does not intend to set a numerical "one-size-fits-all" level of insurance requirement for all technologies. Instead, the required level of insurance will be determined on an application-by-application basis and will be based upon the examination of several factors, including: "the amount of insurance the Contractor/Provider has previously maintained; the amount of insurance maintained for other technologies or for the business as a whole; the amount of insurance typically maintained by sellers of comparable technologies; data and history regarding mass casualty losses; and the particular technology at issue." The rule also suggests that the Secretary might confer with the Contractor/Providers, and insurance carriers, to determine the appropriate level of insurance to require for a particular application. The proposed rule recognizes that over time the appropriate level of insurance may change based on the market for insurance, the predominance of a particular threat, and other factors. Accordingly, the Contractor/Provider is allowed to seek reconsideration of the insurance required.

The impact for not maintaining the required level of insurance are also addressed in the rule. If a Contractor/Provider allows its insurance to fall below the required level of insurance, the protections of the SAFETY Act will still apply. However, the maximum liability of the Contractor/Provider remains at the required level of insurance so they may be subjecting itself to an uninsured liability. In addition, allowing the insurance to fall below the required level will be regarded as a negative factor by the Secretary for any future application for renewal of the SAFETY Act protections and might be considered as a negative factor for any other SAFETY Act applications submitted by the same Contractor/Provider.

Confidentiality of Information

Under the Freedom of Information Act, Trade Secrets Act and other federal statutes, trade secrets and other proprietary information submitted to DHS by an applicant remain confidential. In the final rule, however, DHS has taken the position that all information submitted by an applicant, whether or not proprietary or a trade secret and including the applicant's identity, will be withheld from disclosure.

The breadth of the information that DHS may withhold is subject to debate, and DHS has staked out an aggressive position. Parties submitting applications for anti-terrorism technology designation or certification still should be careful because courts frequently have taken a more nuanced view of the proper balance between protecting commercially valuable information and the public's right to examine the decisions of its government agencies.

Certifying "accuracy and completeness"

The standard for performance of this final rule clause is almost impossible to determine—yet the industry case will rest heavily on the process that led them to seek the QATT in the first place. The parameters used for "accuracy and completeness" are also likely to be used in determining negligence or fraud. Since DHS is not dealing with a detailed federal government specification for defined products, services and support the method for certifying "accuracy and completeness" remains subjective.

Significant Modification to a Qualified Anti-Terrorism Technology

The final rule discusses the provisions of ongoing modification to QATT in service. The issue that this raises, however, deals with QATT that has undergone in place upgrades and enhancements without specific DHS review. The worst case scenario suggests that DHS could develop a finding that determines that a product thought to be on the QATT and covered with appropriate liability insurance, is not and a fraud has occurred. Third parties in this scenario then have additional options to recover from claims. However horrific it seems, the potential test of this rule could be in the aftermath of a significant terrorist attack on the US and the availability of 'clear and convincing evidence' to support claims against a Seller may not be possible.

Scope of Insurance Coverage

The final rule creates a single cause of action with exclusive jurisdiction in a federal district court. As a result, we might expect to see plaintiffs suing in foreign countries whenever possible to avoid the liability limitations of the Act. Industry will be carefully considering appropriate corporate structures necessary to ameliorate this possibility and to keep federal causes of action in the United States.

Reconsideration of Designations

The final rule also suggests that a designation as a qualified anti-terrorism technology will last for five to eight years and may be renewed, but seeks comment on this proposed duration. The SAFETY Act does not contain any time limit on the length of the "designation." There appears to be no logical reason why there should be any time-based limitation on the designation as a QATT—a technology that meets the criteria today and is afforded the protections of the statute, should be eligible for the same protection so long as the technology is available and in service.

Mr. REICHERT. Thank you, Mr. Meldon.

The chair recognizes Mr. Soloway, president of the Professional Services Council.

STATEMENT OF STAN SOLOWAY, PRESIDENT, PROFESSIONAL SERVICES COUNCIL

Mr. SOLOWAY. Thank you, Chairman Reichert, distinguished members of the subcommittee. I appreciate the invitation to testify this morning.

My name is Stan Soloway. I am president of the Professional Services Council, which is the leading national trade association of the government professional and technical services industry.

Many of our member companies are currently actively supporting DHS's critical mission. Many have applied for coverage under the act or are planning to do so. Despite a slow start, significant progress on implementation of the SAFETY Act has been made in the last few months.

And we certainly compliment and join the chorus of compliments to the Department of Homeland Security staff and particularly the leadership from the Office of the Chief Procurement Officer and the general counsel's office, Admiral Cohen and others for bringing us to this point.

More work does remain to be done, however. And in the interest of time and not to be redundant with my colleagues, let me just focus on a few key issues.

The department has been consistently clear and reasserted in this final rule that services are fully eligible for SAFETY Act coverage. The department in the final rule has restated its intent to assert appropriate exemptions to protect proprietary information submitted by companies during the application process.

They have clarified the scope of SAFETY Act coverage by allowing for block designations and block certifications for groups of technologies and, as Mr. Howell and others have mentioned, creating a new category of coverage, developmental test and evaluation.

All of these are excellent signs of progress, and we are fully supportive of this approach. But as the program continues to be a work in progress, so, too, are these final regulations.

There are additional steps the department should take, such as issuing a streamlined application kit so that companies can take full advantage of the new flexibilities, provide more clarity in addressing the relationship to federal and other procurement opportunities, and more clarity as well to address the relationship between the SAFETY Act and the extraordinary contractual relief available for federal procurement opportunities under Public Law 85–804.

Following the release of the final rule, the department issued in August an updated application kit, and by and large we are supportive of the new kit. It is consistent with the final rule and does include relevant application forms for the new block designation, block certification and DT&E designation.

The kit addresses the concerns PSC and others raised at the department and the Office of Management and Budget's Office of Information and Regulatory Affairs in February of 2005, particularly with respect to the quantity of highly proprietary financial information required of applicants.

Yet here, too, there are still some lingering concerns. The forms are indeed clearer and more logically arranged, and the amount of financial information that is required appears to be minimized.

However, we do not believe that the total amount of information requested will be significantly less than previously required.

In fact, new to this version of the application for designation is an instruction with regard to certain applications that instructs an applicant to, quote, attach a copy of any request for proposal or broad agency announcement that led to the award and a copy of your final proposal and statement of work.

The workload to meet this requirement, even though it only applies in certain circumstances, could be extraordinary. In addition, while more information is given on how to properly and fully complete the application forms, the new kit actually establishes some tougher standards for the department to find an applicant complete.

Furthermore, despite a reference to it in the rule, the streamlined application process does not yet exist. PSC and our partners such as the Chamber of Commerce and the SAFETY Act Coalition have provided DHS with a recommended streamlined application kit, and we are hopeful the department will move quickly to fill this significant gap.

As Ms. Duke and others have also made clear, the final rule clearly recognizes the importance of aligning the SAFETY Act proc-

ess with planned and ongoing federal procurement and the procurement processes of others.

For example, the final rules establish a flexible approach for coordinating consideration of a SAFETY Act application with the procurement process by allowing a government agency to seek a preliminary prequalification designation notice with respect to a technology to be procured.

That notice would state that the technology to be procured either affirmatively or presumptively satisfies the technical criteria necessary to qualify under the act.

The regulations provide that vendors chosen to provide the technology will receive expedited review of their application for designation, be deemed to have satisfied the technical criteria for SAFETY Act designation with respect to that technology, and be authorized to submit a streamlined application as set forth in the prequalification designation notice.

We strongly support this approach, but we must also recognize the great challenges inherent in the cross-agency and cross-governmental coordination needed to make this process work as intended. And we urge DHS to move quickly to clarify that vital element of the process.

We have also long asserted that companion regulatory coverage must be included in the Federal Acquisition Regulation and, if necessary, the department's own regulations. To its credit, and as Ms. Duke mentioned, the Office of Procurement has initiated this rulemaking with the FAR council and developed an initial outline for the rule.

With the final SAFETY Act rule now in place, it is essential that the acquisition rulemaking process move very quickly.

Once the final acquisition regulations are in place, the next critical step is to provide the necessary training to the federal acquisition workforce and others involved in the process. The DHS staff recognizes the importance of such training and has indicated a commitment to initiate that training at the earliest opportunity.

PSC and my colleagues at other associations would be more than happy to offer our assistance wherever appropriate.

Mr. Chairman, it has been almost 4 years since Congress took the significant step to enact the SAFETY Act. The law is intended to be a gas pedal to accelerate the deployment of antiterrorism technologies. The procedural issues relating to the act should not be a break on the applicants.

DHS has significantly moved the process forward and, to the department's credit, it has not waited for the final rule or for the acquisition regulations to apply the SAFETY Act protections to its own significant procurements.

As Mr. Howell mentioned, the advanced spectroscopic program award the department made earlier this year includes SAFETY Act coverage. The SBInet procurement now under review by the department includes specific provisions to address the act.

And finally, to address the emerging challenges of liquid-based explosives, the department issued an RFI for recommended technology approaches with SAFETY Act coverage addressed as part of that RFI.

We expect the next few months will yield even more progress on the acquisition regulations, process clarity, aligning the SAFETY Act needs with other agency procurements, training, and this important streamlined application kit.

We look forward to continuing to work with the DHS and the Congress in achieving these important objectives. Thank you for your time and attention today. And of course, I would be happy to answer any question you might have.

[The statement of Mr. Soloway follows:]

PREPARED STATEMENT OF STAN SOLOWAY

Chairman Rogers and Chairman Reichert, members of the Subcommittees, thank you for the invitation to testify on the implementation of the "Support Antiterrorism by Fostering Effective Technologies (SAFETY) Act, part of Title VIII of the Homeland Security Act of 2002 (P.L. 107–296). My name is Stan Soloway, president of the Professional Services Council (PSC). PSC is the leading national trade association of the government professional and technical services industry. PSC's more than 200 member companies represent small, medium, and large businesses that provide the full range of services to all federal agencies, including information technology, engineering, logistics, operations and maintenance, consulting, international development, scientific, environmental services, and more. Many of our member companies have applied for coverage under the Act or are planning to do so.

As you know, the SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of risk management and litigation management. PSC and our member companies were involved in the congressional action leading to the enactment of the SAFETY Act and we have been actively working on the implementation since then. Significant progress has been made in the last few months to bring the SAFETY Act forward and we compliment the Department of Homeland Security staff, in particular the leadership from the General Counsels' Office and the Office of the Chief Procurement Officer, particularly for bringing us to this point. More work remains to be done, however, and PSC plans to offer our expertise and support to build on the progress that has been made.

I have divided my testimony into four parts: the regulatory foundation, the application kit, DHS staff support for the SAFETY Act, and addressing the procurement process.

The Regulatory Foundation

On June 8, 2006, the Department published the final rule implementing the Act,[1] replacing an interim rule issued in October 2003.[2] While PSC recognized the challenges facing the new Department in implementing the SAFETY Act, we were critical of many elements of the interim regulations. We commented extensively on those interim regulations,[3] and urged the Department to address numerous issues as it developed their final regulations. We are very pleased that, in the final regulations, the Department addressed most of the concerns we raised. As the background statement accompanying the final regulation noted:

> The SAFETY Act program is now in its third year, and the Department has a substantial record of program performance to evaluate. While the Department concludes that the Department's core legal interpretation of the Act's provisions are fundamentally sound, experience in administering the program has demonstrated that certain of the procedural processes built to administer the Act can be improved.[4]

When the final regulations were issued, we said then and reiterate today that they were a critical step forward and give clear guidance to Department of Homeland Security officials, other government agencies and the companies that are encouraged to promote the development and deployment of anti-terrorism technologies.

There are several provisions of the final rule that bear mention and we particularly support. The Department has been consistently clear, and reasserted in this final rule, that services are fully covered by the Act and are eligible for SAFETY

---

[1] 71 F.R. 33147, et seq. (June 8, 2006).
[2] 68 F.R. 59684, et. seq. (October 16, 2003).
[3] See PSC comments on the interim rule, available at: *http://www.pscouncil.org/pdfs/ITAA-PSC%20IFR%20Comments.pdf* .
[4] 71 F.R. 33148 (June 8, 2006), column 1.

Act coverage."[5] The Department has restated its intent to assert "appropriate exemptions" to protect proprietary information submitted by companies during the application process,[6] although we hope that the Department would be forthcoming with broad statistical information about the program, such as how many applications have been received and how many rejected, without disclosing applicant names or even technologies being addressed. The Department has clarified the scope of its SAFETY Act coverage by allowing for "Block Designations" and "Block Certifications" for groups of technologies,[7] and creating a new category of coverage—Developmental Testing and Evaluation (DT&E)—with limited SAFETY Act coverage, that should facilitate the deployment of promising anti-terrorism technologies in the field either for test and evaluation purposes or in response to exigent circumstances.[8]

But as the program continues to be a work in progress, so too are these final regulations. In fact, as part of this final rule, the Department has specifically asked for comments on how the Department can and should address changes in insurance availability[9] and on the operation of the new DT&E designations.[10] PSC is developing comments on these two elements of the final regulations and anticipates submitting them to the Department in the near future.

At the same time, there are additional steps for the Department to take, such as issuing the streamlined application kit, so that companies can take full advantage of the new flexibilities and address the relationship to federal and other procurement opportunities. Another issue that needs further discussion about implementation, but probably not more SAFETY Act regulations, is the relationship between the SAFETY Act and the extraordinary contractual relief available for federal procurement opportunities under P.L. 85–804.[11]

The Application Kit

On August 16, 2006, the Department issued the revised application kit to implement the final rule.[12] Even though the Department has not yet received the necessary information collection approval from OMB for the new kit, the Department is directing new applicants to exclusively use the new application kit; applicants who registered with the Department prior to August 16 may continue to use the earlier version of the application kit.

We have reviewed this new application kit and intend to submit comments to both the Office of Management and Budget and the Department on the updated application kit by the October 16 deadline for the submission of comments. By and large, we support the new kit. In our view, it is consistent with the June 2006 final rule and includes relevant application forms for the new Block Designation, Block Certification, and DT&E designation. This kit is more user-friendly than the December 2004 version;[13] it addresses further the concerns PSC raised to the Department and OMB's Office of Information and Regulatory Affairs on February 10, 2005 about that earlier version of the kit, particularly with respect to the quantity of highly proprietary financial information required of applicants.[14]

Yet there are still some lingering concerns even with this kit. To be sure the application forms are clearer and more logically arranged and this will be a benefit to applicants. The amount of financial information that is required with the initial application appears to be minimized. But we do not believe that the request for information under this kit will be significantly less than the amount of information previously required. In fact, new to this version of the application for Designation under Chapter 4 of the kit, is the instruction relating to past sales and ongoing procurements; it requires that an applicant "attach a copy of any request for proposal or broad agency announcement that led to the award and a copy of the applicant's final proposal and statement of work."[15] In addition, while there is more information on how to properly and fully complete the application forms, we believe that the new kit places tougher standards for the Department to find an applicant complete.

---

[5] See 71 F.R. 33154 (June 8, 2006) column 2.
[6] See 71 F.R. 33151 (June 8, 2006) column 2 and Section 25.10 of the final regulations.
[7] See 71 F.R. 33156 (June 8, 2006) column 3 and Section 25.9(j) of the final regulations.
[8] See 71 F.R. 33156 (June 8, 2006) column 2 and Section 25.4(f) of the final regulations.
[9] See 71 F.R. 33149 (June 8, 2006) column 2.
[10] See 71 F.R. 33156 (June 8, 2006) column 3.
[11] See 71 F.R. 33154 (June 8, 2006) column 3.
[12] Available at: *https://www.safetyact.gov/DHS/SActHome.nsf/23158AD7D420AEDB852571C70056BE33/$FILE/Application%20Kit%20Version%202.pdf* .
[13] See 69 F.R. 72207 (December 13, 2004).
[14] See PSC February 10, 2005 letter to DHS and OIRA, available at: *http://www.pscouncil.org/pdfs/SAFETYActApplication2-10-05.pdf* .
[15] See the Instructions for Designation D6.2 at page 34-35.

Furthermore, we requested and expected a significantly streamlined application kit, particularly when seeking to match the application process with an on-going federal procurement. On September 6, 2005, PSC and four other associations jointly developed and submitted to DHS former Under Secretary McQueary, a proposed streamlined application kit and instructions.[16] In this 2006 version of the application kit, the Department makes a reference to a streamlined application process in connection with Block Designations,[17] but we do not view that single reference in one section as meeting our expectation.

We look forward to further discussions with the Department on our comments on this kit and moving toward a true streamlined application process.

DHS staff support for the SAFETY Act

On a related matter, we strongly recommend that the Department continue to provide the necessary infrastructure support for the Office of SAFETY Act Implementation (OSAI) and its activities. Our members have appreciated the responsiveness of the OSAI, Science and Technology (S&T) and General Counsels' offices to requests for information and to processing applications. We would hope that, in the near future, the OSAI would have a permanent director and be staffed with a sufficient number of federal employees to handle the expected increase in requests for information, growth in applications, and demands for being a resource to other federal agencies who need information on the Act and its processes, particularly in relationship to planned or on-going procurements.

Addressing the Procurement Processes

The SAFETY Act protections are relevant only when applied to a specific anti-terrorism technology. Thus, the relationship between the SAFETY Act and the procurement of those technologies is critical. Certain aspects of that relationship vest in the SAFETY Act regulations; other aspects must be addressed in the federal procurement regulations. Still other provisions must be covered in the procurement processes of other purchasers—state, local, or commercial.

Through September 6, 2006, the Department has already issued 62 Certifications and 22 Designations.[18]

To its credit, the June 2006 final SAFETY Act regulations recognize the importance of aligning the SAFETY Act process with planned and on-going federal procurement and the procurement processes of others.[19] For example, these final rules establish a flexible approach for coordinating consideration of a SAFETY Act application with the procurement process by allowing a government agency to seek a preliminary "Pre-Qualification Designation Notice" with respect to a technology to be procured, stating that the technology to be procured either affirmatively or presumptively satisfies the technical criteria necessary to qualify under the Act.[20] The regulations provide that selected vendors chosen to provide the technology will receive expedited review of their application for designation, be deemed to have satisfied the technical criteria for SAFETY Act Designation with respect to that technology, and be authorized to submit a streamlined application as set forth in the pre-qualification designation notice.[21] We strongly support this approach. Even though the information required to be submitted would vary on a case-by-case basis, we strongly recommend that this Pre-Qualification Designation Notice be incorporated into the application kit instead of being totally outside it.

In addition, the final regulations addressed the deference due to other federal or state regulatory or procurement officials.[22] As the background information and the regulations provide, the level of deference due to other government officials will depend on the nature of such officials' review.

Beyond the SAFETY Act regulations, we have long asserted that companion regulatory coverage must be included in the Federal Acquisition Regulation and, if necessary, in the Department's own Homeland Security Acquisition Regulations. For example, when the Department published its interim acquisition regulation on December 4, 2003, PSC's written comments on that rule specifically noted the absence

---

[16] See September 6, 2005 Joint letter from PSC, Aerospace Industries Association, Information Technology Association of America, National Defense Industrial Association and U.S. Chamber, available at: *http://www.pscouncil.org/pdfs/McQuearySAFETYActKitLetter.pdf* .

[17] See the Chapter 7 Block Designation Application at page 67.

[18] See SAFETY Act website: *https://www.safetyact.gov/,* last visited on September 6, 2006.

[19] See 71 F.R. 33156 (June 8, 2006) column 1.

[20] See 71 F.R. 33163 (June 8, 2006) column 3 and Section 25.6(g) of the final regulations.

[21] See the "Pre-Qualification Designation Notice on *www.safetyact.gov.* Section 25.6(g)(4)(iii) of the regulations provides that the Pre-Qualification Designation Notice will provide a list of the portions of the application information in Section 25.6(a) that the selected vendor(s) must complete and submit in order to obtain Designation.

[22] See 71 F.R. 33157 (June 8, 2006) column 2 and Section 25.4(viii) of the final regulations.

of any SAFETY Act coverage applicable to the Department's own procurement.[23] In the Department's May 2, 2006 final acquisition regulations, the Department acknowledged that SAFETY Act coverage is appropriate and will be considered when the Federal Acquisition Regulation is issued.[24]

We do not yet know the status or content of the Federal Acquisition Regulations (FAR). In 2003, PSC and other organizations wrote to the Office of Federal Procurement Policy urging the FAR Council to develop and publish for comment the necessary government-wide acquisition policy regulations. The FAR Council established a case number but took no action on the rule, awaiting the final SAFETY Act regulations. The FAR Council closed the prior case without action, but on August 23, 2006 opened a new case number (2006–023) based on the strawman draft submitted by the Department's Chief Procurement Officer.[25] This is an important next step to fully effectuate the SAFETY Act. Once the FAR rule is in place (or even pending that final rule), it may be necessary or appropriate to supplement the FAR with coverage in the Department's own acquisition regulation.

Once the final acquisition regulations are in place, the next critical step is to provide necessary training to the federal acquisition workforce and others. We believe both the DHS acquisition staff and the OSAI staff recognize the importance of such training and have indicated a willingness to initiate that training at the earliest opportunity. PSC, and I am sure my colleagues at the other associations that we have worked in partnership with over the years on the SAFETY Act, will offer our assistance wherever appropriate.

Fortunately, the Department has not waited for the final rule or for the acquisition regulations to begin applying the SAFETY Act protections to its own significant procurements. For example, the three DNDO Advanced Spectroscopic Program (ASP) awards that the Department made earlier this year include SAFETY Act coverage. The significant SBI.net procurement now under review by the Department includes specific provisions to address SAFETY Act coverage. Finally, to address the emerging challenges of liquid-based explosives, the Department issued a Request for Information for recommended technology approaches, with SAFETY Act coverage addressed as part of it.[26]

Regrettably, we do not have any visibility into the application of SAFETY Act coverage in other federal agency procurements. Even less visibility exists on the extent to which the SAFETY Act has been used in state, local or commercial applications. However, since the Department makes significant grants to first responders and state and local governments for a wide range of homeland security matters, we can well envision that many of the products and services acquired with these grant funds would be interested in and eligible for SAFETY Act coverage. We encourage the Department to share with the Congress and the public the extent to which the SAFETY Act is being used in these circumstances.

Conclusion

Mr. Chairmen, it has been almost four years since the Congress took the significant step in the Homeland Security Act to enact the SAFETY Act. In our view, the law is intended to be a "gas pedal" that is designed to accelerate the deployment of anti-terrorism technologies; the procedural issues relating to the SAFETY Act should not be a "brake" on the applicant. Over the past three years, we have seen interim regulations, and now a final rule, preliminary and then an interim and now a final application kit, and other related implementation actions. Those early SAFETY Act applicants helped test the process and the information required to be submitted to assist the Department in deciding appropriate coverage. We have significantly advanced that process in the last few weeks with the final regulation and application kit. Hopefully, over the next few months, we will see the final Federal Acquisition Regulation and any related DHS acquisition regulation coverage. Simultaneously, critical procurements are taking place where the SAFETY Act coverage could be the difference in a successful procurement.

PSC has been involved in the SAFETY Act process from the beginning and we intend to remain active in the future to make the process clear and its utilization as robust as possible. We particularly appreciate this Committee's bipartisan attention to the Act and to the Department's administration of the Act. Unquestionably your interest has helped to move this process forward.

---

[23] See PSC comment on the DHS interim procurement regulations, available at: *http://www.pscouncil.org/pdfs/ITAA-PSC%20IFR%20Comments.pdf* .

[24] See 71 F.R. 25759;65 (May 2, 2006)..

[25] See FAR Council Status of Cases, available at *http://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf,* as of September 1, 2006.

[26] See liquid explosive RFI available at: *http://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC%2DBAA%2D06%2D00063/SynopsisP.html,* last visited September 7, 2006.

Thank you again for opportunity to testify. I would be pleased to respond to any questions you have.

STATEMENT REQUIRED BY HOUSE RULES

In compliance with House Rules and the request of the Subcommittee, in the current fiscal year or in the two previous fiscal years, neither I nor the professional Services Council, a non-profit 501(c)(6) corporation,has received any federal grant, sub-grant, contract or subcontract from any federal agency.

Mr. REICHERT. Thank you, Mr. Soloway.

The chair recognizes Mr. Finch, who heads the homeland security practice for the law firm of Dickstein Shapiro LLP to testify.

STATEMENT OF BRIAN FINCH, ESQ., DICKSTEIN SHAPIRO LLP

Mr. FINCH. Thank you, Mr. Chairman. Chairman Rogers, Chairman Reichert, Ranking Member Meek, Ranking Member Pascrell and other distinguished members of the subcommittees, it is an honor to appear before you today to discuss my experiences with the SAFETY Act.

My name is Brian Finch, and I am the head of the homeland security practice group at the D.C. law firm Dickstein Shapiro. While I am here in my personal capacity, I am delighted to share with you my experiences over the past 3 years with the SAFETY Act.

I have helped prepare dozens of applications, including many of those that were the first approved. I have seen pretty much every type of application submitted to DHS, and I have helped companies of all sizes file applications.

While it has not always been an easy process, it is my firm belief that DHS has made great strides to make the SAFETY Act process easier and more efficient.

Some of my SAFETY Act application experiences: As a starting point, this committee must understand that applicants must give DHS the sufficient information needed to make a determination that the technology at issue is, in fact, safe, effective and useful.

In my experience, however, what constitutes sufficient information has varied significantly. For some, a few dozen pages of documentation is sufficient, while for others a blizzard of information is not enough.

Also, there have been at times unnecessary additional requests for information that have often led to applications being held up for several months beyond the 150-day initial decision time frame.

For example, in one application we stated to DHS that guard dogs could detect thousands of different smells. In response, DHS asked us to provide a list of those thousands of smells. That seems excessive.

Applicant distress over the process has come about in part because at times there seems to be a significant disconnect between the senior management of DHS and the implementation staff. This disconnect can result in unnecessary delays and frustrations.

While it does not represent the majority, my experiences—and I do, in fact, applaud the work of the SAFETY Act office—I would be remiss if I did not mention these experiences.

The final rule and revised application kit. Although it has been fairly well covered, I believe there are a few elements of the final rule and the new application kit that are especially noteworthy.

Prequalification. The final rule spells out a prequalification designation process that should be warmly welcomed. Under the final

rule, federal, state and local government customers are now armed with a way to ensure that potential vendors will, in fact, receive SAFETY Act coverage.

Other changes to the application kit. The new kit is greatly simplified and adds useful new sections that recognize the importance of antiterror deployments to all governments as well as commercial entities.

DHS has gone to great lengths to provide a better vehicle for requesting an expedited review. DHS has also reduced the potential review time from 150 days to 120 days. And I applaud the undersecretary's comments that he views 120 days as the outside limit.

While there is always room for improvement, it should be perfectly clear that the final rule and the new application kit are, in fact, significant steps forward.

Suggestions for improvement. As DHS is aiming to create a robust and user-friendly application process, I would suggest some of the following improvements: Increased oversight by the science and technology leadership.

It is unrealistic to expect that Secretary Chertoff's senior staff can exert significant daily oversight over the SAFETY Act program.

I would urge Undersecretary Admiral Cohen to assign a senior member of his staff with the responsibility of being a kind of SAFETY Act ombudsman. This should be someone who has access to DHS policy makers and has the ability to interact regularly with the SAFETY Act office to ensure that policy decisions are, in fact, translated into action.

Better utilization of the SAFETY Act inside and outside of the federal government. Homeland security is not the sole responsibility of the Department of Homeland Security. Many other members of the federal family, including the Department of Defense, Health and Human Services, Department of Agriculture, all play a vital role in defending the nation.

DHS should do its part to help ensure that other federal agencies understand the SAFETY Act and how it can be best utilized to our nation's advantage.

DHS should also use the National Infrastructure Protection Plan, or the NIPP, as much as possible, as it itself explicitly encourages the use of SAFETY Act-approved products to help protect the nation's critical infrastructure and key resources.

Given that the NIPP is the DHS blueprint for protecting the nation's critical infrastructure in partnership with the private sector, that encouragement makes plain sense.

Allow for better-defined marketing of SAFETY Act approvals. Driven by concerns about the misuse of its seal, DHS has barred its use in conjunction with the promoting of SAFETY Act approval.

I would ask the department to create a special logo that only SAFETY Act-approved technologies and services could use. There is ample precedent for such a logo—the USDA's national organic program comes to mind—and it would go a long way to resolve what has become an unnecessary impediment to allowing SAFETY Act-approved technologies to be better utilized.

This is important to note, because SAFETY Act-approved technologies can, in fact, be used by any customer, including private-sector customers.

And to Mr. Dicks's comments earlier, I have seen a number of applications that are intended to be used solely by the private sector and helped get those through the review process.

Better-defined time frames. No one is still quite sure what it means to receive an expedited review. DHS needs to give applicants a better sense of what exactly an expedited review means so they can better plan in the application process.

Despite the bumps in the road, from my perspective, the SAFETY Act program is one of the stars of the Department of Homeland Security. There are still improvements to be made, but I believe that we are now in the realm of fine-tuning and not major overhauls when it comes to the SAFETY Act.

That concludes my prepared remarks, and I am delighted to answer any questions.

[The statement of Mr. Finch follows:]

PREPARED STATEMENT OF BRIAN E. FINCH

Chairman Rogers, Chairman Reichert, Ranking Member Meek, Ranking Member Pascrell, and other distinguished members of the Subcomittees, it is an honor to appear before you today to discuss my experiences in assisting applicants in obtaining liability protections under the Support Anti-Terrorism By Fostering Effective Technology Act of 2002 (the SAFETY Act).

My name is Brian Finch, and I am counsel at the law firm Dickstein Shapiro LLP, where I also serve as the head of the firm's Homeland Security Practice Group. While I am here in my personal capacity, I am delighted to share with you my many experiences over the past three years with the SAFETY Act. It has not always been an easy process, and there have been times of great frustration for both myself and the companies that I have represented. However, it is my firm belief that the SAFETY Act implementation process has been steadily improving and that the Department of Homeland Security has made some great strides over the past few years to make the process easier and more efficient. Given the many challenges that DHS faces on a daily basis, it is my opinion that DHS has given an extraordinary amount of attention to improving the SAFETY Act process, and that it should ultimately be commended for its efforts.

I have been involved in the SAFETY Act process for the better part of the last three years. Over that time frame I have helped to draft dozens of SAFETY Act applications, including the very first two applications to receive Certification and Designation under the SAFETY Act. I have helped prepare a wide variety of applications. I have for instance helped draft applications for non-intrusive detection devices, explosive detection equipment, decision support software, maintenance services, systems integration services, vaccines, and vulnerability assessment methodologies to name but a few.

The size of companies for which I have provided SAFETY Act assistance has ranged from the exceptionally large to small ventures generating just a few million dollars annually. I am currently working with well over a dozen companies that have applications in various stages of review, and those companies range from large defense conglomerates to smaller security contractors, as well as trade associations.

Experiences With SAFETY Act Application Review Procedures

With that wide range of clients and applications, I have encountered any number of scenarios in the SAFETY Act application process. My involvement typically starts with the decision making process on what applications to submit all the way through to counseling on ways to utilize the receipt of a SAFETY Act approval. I have handled some very straightforward applications that passed through review with relative ease, and I have been involved in some applications that entailed painstaking reviews and immense amounts of effort. This has allowed to me see both patterns and aberrations in the review process.

In that vein, I would like to start with my basic views about the SAFETY Act application process. As I inform all potential applicants, the process will involve some significant thought and effort as we must present to the Department a thorough overview of the technology or service in question. Applicants have a responsibility to present evidence demonstrating that their technology is safe, effective, and has a usefulness as anti-terror technology. At the same time, they must be aware that the Department has a responsibility to conduct a fair and meaningful review.

DHS must have at its disposal sufficient information to make a determination that technology or service at issue is in fact safe, effective, and useful.

In my experience, what constitutes "sufficient information" has over the past three years varied significantly and been somewhat of a mystery. Some applications have moved swiftly through the review process with dozens of pages of documentation. Others have submitted literally thousands of pages of backup documentation, and yet applicants will receive numerous additional requests for information. These additional requests for information have often led to applications being held for several months beyond the 150 day decision timeframe.

The applicants who have run into the continued requests for information or have had their applications under review for months beyond the prescribed timeline are the ones that typically talk about the SAFETY Act process being akin to a "mini-FDA" process. Based on my work, I can say that the application review process has at times been unnecessarily involved. While the majority of my application experiences have not been negative, there certainly have been occasions where the level of documentation requested and the delays in the process could be deemed excessive. For example, one application informed DHS that guard dogs—including those used by the applicant—could detect over 20,000 different smells. In response, DHS asked us to provide proof of that statement, including a list of the 20,000 smells. That seemed excessive.

Given the number of applications where I have been involved, I have grown accustomed to those types of information requests and can warn applicants about the level of detail that must be provided. Clients who are not used to that experience, however, are more than a little surprised and frankly disappointed by how much information must be provided. Applicants are always quite willing to provide the information needed as they are committed to successfully pursuing coverage, but at the same time they are baffled as to why DHS would demand so much information. That, if anything, has been the source of much consternation.

Part of that distress has come about in part because at times there seems to be a significant disconnect between the senior management of DHS and the implementation staff. While DHS leadership has always seemed to have grasped the importance of a smooth running SAFETY Act application process, that message seems not to always flow down consistently to the implementers and the reviewers. Instead of a unified theme of quick and efficient reviews of applications one is left with the impression that review staff are more committed to microscopic reviews of applications, leading to reviews getting bogged by details of an application. This results in unnecessary delays and frustration at the process.

Again, this does not represent the majority of my experiences. Indeed for most applications I have encountered personnel at all levels that are committed to the success of the SAFETY Act program and who would like to see applications succeed. I generally applaud the efforts of the DHS staff at all levels. However, I would be remiss if I did not mention that the heightened scrutiny of applications has occurred on more than one occasion and has led some applicants to express significant frustrations.

Despite the less than perfect experiences, I have found that an ever increasing number of companies are willing to pursue SAFETY Act protections. While the pace of approvals was generally considered to be slow, the recent uptick in the number of approved technologies has galvanized a number of companies to start the process. Even more important is the fact that we are starting to see an increasing number of customers who have decided that potential vendors should have either obtained or be seeking SAFETY Act approval. The fact that customers have recognized that SAFETY Act coverage is a valuable tool and accordingly believe it that they should be using SAFETY Act approved products and/or services is a strong indicator that the process is working. If there were no value in it, no would even think twice about it—particularly on the customer side.

I should also note that when the SAFETY Act was first brought online, a strong misperception existed that it would apply only to cutting edge "widgets," and not existing solutions or services generally. This misperception, which existed despite the best efforts of DHS, in my opinion contributed to the relatively small number of applicants at the beginning of the process.

To its credit, DHS has invested significant energy to dispel those myths. A significant number of approvals have been issued to service providers, and issuing those approvals has proven to be the best remedy for any concerns about the potential breadth of approvals that can be issued. And I would like to particularly note that DHS has gone out of its way to help ensure that applications encompassing less obvious but vitally important anti-terror services received a fair review.

These applications, which include engineering services, security guidelines, and professional certification programs, may not have the visceral appeal of an explosive

trace detection device or an anthrax detector, but they play just as an important part of the nation's anti-terror efforts as any other widget or service. DHS should be lauded for such approvals because it will make it easier to attract similar innovative applications.

THE FINAL RULE AND REVISED APPLICATION KIT

Ever since the Interim Final Rule and the initial Application Kit were released in the Fall of 2003, industry and commentators have been pointing out its flaws and asking when they would be supplemented or replaced. After years of questions and promises of "imminent" release, DHS finally released both the Final Rule and a Revised Application Kit this last summer.

DHS itself admits these documents are not the final say on all things SAFETY Act, which is both appropriate and welcome. Yet before the inevitable discussion begins about how both the Final Rule and the new Kit go far enough, I would like to note to the Committees what I believe are several very welcome new developments. While both the Final Rule and the Kit contain many improvements, I believe the following are especially noteworthy:

Pre-Qualification of Procurements: Since the SAFETY Act was enacted, potential applicants have been searching for ways to better ensure a guarantee that if they submitted a bid on a particular procurement they would obtain SAFETY Act coverage. Many procurement officials (particularly those outside of DHS), in light of the lack of an official vehicle for doing so, could do nothing more than offer to support an applicant's package to do DHS. While such support is always welcome, no one had the confidence that it would be sufficient to ensure a particular application's success. Under the Final Rule, customers are now armed with a way to help ensure that potential vendors will in fact receive SAFETY Act coverage. The Final Rule spells out a "Pre-Qualification Designation Notice" process that should be warmly welcomed. Agencies now have a method by which they can submit their potential procurement to DHS for review. If DHS finds that the potential procurement would merit SAFETY Act approval, vendors who are ultimately chosen to provide the specified technology will receive an expedited review, either affirmatively or presumptively be deemed to satisfy the criteria for a SAFETY Act Designation, and can submit a streamlined application. This is truly a step forward, as now procuring agencies are armed with a methodology that will allow them to guarantee SAFETY Act approval. That in turn should help bring forward more potential vendors, increasing choice and the potential that the proper technology will be deployed.

Developmental Testing & Evaluation Designations: In the development phase of any technology, including those to be used to combat terrorism, it is quite normal for an unfinished or unproven product to be field tested or deployed in limited circumstances. Such preliminary deployments are necessary in order to finalize testing or verify the value of the technology. In the context of anti-terror technologies such deployments can be extremely problematic given that terrorist activity could realistically occur during the deployment. SAFETY Act protections would obviously be ideal to limit liability concerns, but the Interim Final Rule did not contemplate offering protections for such deployments. The Final Rule has significantly addressed those concerns, however, by creating a heretofore unavailable liability protection method. DHS has made available a limited set of SAFETY Act protections for technologies that are being developed, tested, evaluated, modified or are otherwise being prepared for deployment. The SAFETY Act protections offered under a Developmental Testing & Evaluation (or DT&E) Designation will last for no more than 36 months, shall apply only to limited deployments, and could have other restrictions imposed as determined by the Under Secretary for Science & Technology. While a DT&E Designation is far more limited than a full SAFETY Act Designation or Certification, it provides a measure of liability protection that otherwise was not available. Given that many technologies need an operational deployment in order to be finalized, this category of application will allow such deployments to proceed without fear of crushing liability.

Changes to the Application Kit: One of the more regularly maligned facets of the process has been the SAFETY Act Application Kit. The initial version of the Kit was criticized by many as confusing, overly repetitive, and lacking guidance on what it would take to receive an "expedited review". The new Kit addresses many of those concerns. First and foremost, DHS has drastically toned down the "Pre-Application" section of the Kit. Applicants no longer have to fill out a confusing form that often resulted in grand misconceptions about a particular technology. DHS now makes clear that a Pre-Application consultation is

strictly voluntary, and has gone to great lengths to make that process easier for potential applicants to undertake. DHS has also added a section asking directly what entities have been procuring the technology in question. Importantly included in that section are categories for commercial organizations and foreign governments. That inclusion recognizes the importance of anti-terror deployments not only to Federal, state and local governments but also to foreign governments and commercial entities, all of whom are vital partners in the fight against terrorism. DHS has also gone to great lengths to provide a better vehicle for requesting an expedited review. A specific section has been set up to address this issue, which should make it easier for an applicant to explain what pressing deadlines they are facing and why DHS should issue a decision in less time than typically required. In that vein DHS has also reduced the potential review time from 150 to 120 days.

While there are many other changes in the Final Rule and Application Kit that could be discussed, it should be sufficient to note that the Department has gone a long way to address many of the concerns expressed by applicants. There will always be room for improvement, as discussed in part below, but one should be absolutely clear that the Final Rule and Kit represent significant steps forward and that the Department should be applauded for its actions.

SUGGESTIONS FOR IMPROVEMENTS TO THE SAFETY ACT PROCESS

Even in light of the great strides taken by the Department, there are other steps it could undertake in order to ensure that the SAFETY Act realizes its full potential. An overarching goal for the Department should be to create a robust and user friendly process that is well known inside and outside of the Department, and whose use is considered a high priority by all entities. To that end, I would suggest the following operational steps in order to better implement the SAFETY Act.

Increased Oversight By Science & Technology Leadership

From the moment he was sworn in, Secretary Chertoff has made clear that getting the SAFETY Act right was one of highest priorities. In numerous speeches the Secretary has underscored the importance of the Act and his commitment to improving the process. As a regular participant in the SAFETY Act process, his dedication to the success of the program has been plainly evident. This commitment has also been demonstrated by a number of other DHS offices, including most prominently the General Counsel's office.

However, as we are all aware, the SAFETY Act is not the only priority for the Department. The very mission of the Department requires it to be focused on any number of emergencies or emerging threats at any given point. To a large extent that has resulted in an unfortunately reality where the Department operates "out of the in-box," reacting to the crisis of the day. Because of that reality, it is unrealistic to expect that senior staff in the General Counsel's Office or in the Secretary's Office can exert significant oversight on the SAFETY Act program.

A more appropriate level of oversight can be exerted however by the Science & Technology Directorate, which is entrusted with administering the SAFETY Act. The new S&T Under Secretary, Admiral Jay Cohen, is in a prime position to strike a balance between the high level of policy direction and operational supervision. Under Secretary Cohen has at his disposal the personnel necessary to ensure that the policy directives of the Department are properly implemented by the Office of SAFETY Act Implementation (OSAI), including any contractor who conducts a review. To date, no one person has been able to fill such a role, with the result being an unfortunate disconnect between policy directives and implementation. In order to bridge that gap, I would urge the Under Secretary to assign a senior member of his S&T staff the responsibility of being a kind of "SAFETY Act Ombudsman," someone to who has access to and can regularly interact with policy makers within the Department, but at the same time has the ability to interact regularly with OSAI to ensure that policy decisions are translated into action. The creation of such a position, potentially within the Under Secretary's immediate office, will significantly reduce the communication disconnect that has, frankly, hindered progress for the SAFETY Act program.

• Better utilization of the SAFETY Act inside and outside of the Federal government

Homeland security as a mission is not the sole responsibility of DHS. Numerous other members of the Federal family, ranging from the Department of Defense to the Department of Health and Human Services as well as the Department of Agriculture, all play a vital role in defending the nation from terrorist threats. Because of the shared responsibilities, each department procures its own anti-terror goods

and services and also helps promote their use on a state and local level as well as in the private sector.

For those and many other reasons, DHS should do its part to help ensure that other Federal agencies understand the SAFETY Act and how it can be best utilized. This can take many forms, including encouraging other Federal agencies to prequalify procurements for SAFETY Act approval. For example, it makes plain sense to have the Department of Defense utilize the SAFETY Act when procuring technologies to conduct force protection operations at its facilities. Similarly the Department of Health and Human Services should not be shy about promoting the use of the SAFETY Act when procuring technologies and services that will be used when a mass casualty event occurs. DHS should work with other Federal agencies to encourage the use of SAFETY Act approved products by private sector partners. This could take the form, for instance, of the Department of Agriculture encouraging companies to use SAFETY Act certified companies to perform security services in order to help reduce the risk of agro-terrorism. The bottom line is that DHS should work actively with other agencies involved in homeland security to increase their knowledge and utilization of the SAFETY Act.

One vehicle in particular that DHS should use to promote the use of the SAFETY Act outside of the Department itself is the National Infrastructure Protection Plan (the "NIPP"). The recently released final version of the NIPP explicitly encouraged the use of the SAFETY Act approved products to protect critical infrastructure and key resources. This was a very smart move by the Department and should be utilized as fully as possible. Given that the NIPP is the DHS blueprint for not only protecting the nation's critical infrastructure but also partnering with other Federal, state and local agencies as well as the private sector to do so, it only makes sense to use that vehicle to help promote the SAFETY Act. Protecting the nation's critical infrastructure is a daunting and extremely expensive task, and helping to ensure that SAFETY Act approved items are used will help mitigate costs and provide a measure of assurance that properly vetted items are being employed.

- **Allow for better defined marketing of SAFETY Act approvals**

One question that companies constantly face when they receive SAFETY Act approval is how they advertise their hard won victory. Initially DHS encouraged as much marketing as possible, including not objecting to the use of the official DHS seal in materials promoting an applicants receipt of SAFETY Act approval.

Over the past year DHS has altered that policy. Driven by major concerns about the misappropriation of the DHS seal generally, the Department has made clear that the official DHS seal may be used by non-Federal agencies only in very limited circumstances. This means that the use of the DHS seal in conjunction with promoting a SAFETY Act approval is no longer permissible.

One can understand the Department's rationale in these circumstances. It wants to control the use of its seal and wants to avoid the appearance of endorsing a particular technology or service. Neither are unrealistic motivations, but successful applicants should be allowed some measure of latitude in promoting the receipt of SAFETY Act protections. Currently many applicants are without significant direction on how to appropriately market their SAFETY Act approval.

Recognizing that a core purpose of the SAFETY Act is to promote the widespread deployment of anti-terror technologies, DHS should do what it can to help encourage that goal. In order to strike a balance between that objective and the Department's legitimate concern about the misappropriation of the official DHS seal, I would ask the Department to seriously consider the creation of a special logo that only SAFETY Act approved technologies and services could utilize. There is ample precedent for such a logo (including recently from the Department of Agriculture's National Organic Program), and its use would go a long way to resolve what has been an unnecessary impediment to successful applicants.

- **Better define time frames for expedited reviews**

Even after all the progress that has been made, one issue that continues to be of concern for applicants relates to expedited reviews of SAFETY Act applications. More specifically, no one is quite sure what it means to receive an "expedited" review. For some time the Department has maintained that if an application is granted an expedited review, it means that it will be moved to the top of the review pile. However, knowing that the number of applications received is still fairly low, and given the tendency of reviews to get mired in details, that has offered little comfort to applicants.

If, as the Department predicts, there will soon be a significant upswing the number of applications received, receiving a high priority review will likely be more meaningful. Similarly, the reduction by 30 days of the amount of time DHS is given to conduct a review (assuming the DHS does not grant itself numerous extensions,

as it has been known to do) could be helpful here. However, there are still going to be times when parties could be significantly aided with a start to finish time frame that runs closer to 60 days than 120. DHS certainly needs and must be given time to conduct a meaningful review of an application, but it also needs to give applicants a better sense of what exactly an expedited application means. This could take the form of agreeing upon a target date for an decision to be issued or window in which an application should be returned.

CONCLUSION

Chairman Rogers, Chairman Reichert, Ranking Member Meek, Ranking Member Pascrell, and other distinguished Members of the Subcomittees, from my perspective the SAFETY Act program is one of the shining stars of the Department of Homeland Security. Its implementation has not always been the smoothest, and there are still improvements to be made, but on the whole I firmly believe that the Department should be applauded for the hard work it has put in to the program. I feel comfortable in stating that DHS has addressed many of the pressing concerns that legitimately faced applicants, and we are now in the realm of fine tuning and not major overhauls when it comes to the SAFETY Act.

This concludes my prepared remarks. I am delighted to answer any questions.

Mr. REICHERT. Thank you, Mr. Finch.

The chair recognizes our last witness today, Mr. David Bodenheimer, who is a partner at the law firm of Crowell & Moring here in Washington, D.C.

STATEMENT OF DAVID BODENHEIMER, ESQ., CROWELL & MORING LLP

Mr. BODENHEIMER. Thank you. Mr. Chairman and members of the committee, I thank you for holding these hearings today on the SAFETY Act implementation on the fifth anniversary of September 11th. We all appreciate the vital role of the SAFETY Act in unleashing lifesaving technology to protect us against terrorism.

I am David Bodenheimer, a partner in the law firm of Crowell & Moring here in Washington, D.C., where I specialize in government contracts and have a particular passion for homeland security and the SAFETY Act, about which I have been busy lecturing, writing, advising clients and co-chairing the American Bar Association homeland security committee. I appear today in my personal capacity, and my comments are my own.

This year Secretary Chertoff and his team have made great strides in implementing the SAFETY Act. However, the terrorists are not resting, and neither can we.

The SAFETY Act has a very clear congressional purpose, saving lives through antiterrorism technology. With the same urgency that we mobilized the industrial base for World War II, we need to supercharge the SAFETY Act so that we can build the world's greatest arsenal of technology against terrorism.

I would like to summarize four points from my testimony.

Number one, we must assure the confidentiality of SAFETY Act data. DHS agreed that successful implementation of the SAFETY Act depends upon protecting trade secrets. To do so, DHS must have a sound information security program.

Industry concerns expressed during the 2003 hearings have been magnified by some hard knocks this year on DHS information security, including failing scores on the FISMA report, delays in appointing the assistant secretary for cybersecurity and continuing criticisms by OMB, GAO and the DHS inspector general.

Quite simply, the capability and credibility of DHS commitments to protect SAFETY Act data hinge upon a robust information security program.

In addition, DHS must issue confidentiality procedures promised in 2003, procedures addressing the who, what, when, where and how of data protection, who can see the SAFETY Act data, what controls protect that data, and how will DHS enforce the rules.

As the focal point for the security of cyberspace, DHS should showcase its leadership role by establishing best practices for guarding the most valuable technologies and secrets of SAFETY Act applicants.

Number two, we must encourage development of breakthrough technologies. The new rules recognize that new and developing technologies may indeed qualify for SAFETY Act coverage, but these items have been given second-class status, burdened with limitations on use and deployment, approvals terminable at will by DHS and restrictions on the duration of coverage generally to 36 months.

These rules send the wrong message. We must encourage breakthrough technologies revolutionizing the war on terror. Just stopping terrorist attacks with conventional bombs does not make us safer when the terrorists have moved on to common household products to build bombs in midair.

Thus, the DHS rules should welcome both developmental and breakthrough technologies so there will be no penalty to companies submitting breakthrough technologies for review and approval.

Number three, we must assure the full duration of SAFETY Act protection. The DHS rule imposes a mandatory sunset period upon approved antiterrorism technology, thus requiring renewal every 5 years to 8 years.

The DHS mandatory sunset period cannot be squared with the express terms or purpose of the SAFETY Act. Indeed, the SAFETY Act offers protections without any term limits, consistent with the statutory purpose of encouraging more technology more rapidly to our front line defenses.

Number four, we must establish an appeals process. An appeals process is consistent with the legislative intent favoring liberal approval, not rejection, of liability protection for antiterrorism technology.

In addition, an appeals process is the rule, not the exception, in the federal arena for everything from pharmaceuticals and pesticides to federal contract awards. The right time for an approvals process is now, not after a terrorist incident causes us to regret the unavailability of a technology.

Thank you for your time. I welcome your questions.

[The statement of Mr. Bodenheimer follows:]

PREPARED STATEMENT OF DAVID Z. BODENHEIMER

Introduction

Mr. Chairmen and Members of the Committee. Thank you for holding these hearings today on the Department of Homeland Security's implementation of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). On the fifth anniversary of September 11th, we all understand and appreciate the vital role of the SAFETY Act in unleashing our technology to combat terrorism and protect the Homeland.

I am David Bodenheimer, a partner in the law firm of Crowell & Moring LLP in Washington, DC where I specialize in Government Contracts and Homeland Security. As part of this practice, I have advised clients, published articles, and lectured extensively on Homeland Security and SAFETY Act matters. In addition, I serve as Co-Chair of the ABA Science and Technology Section's Special Committee on Homeland Security. However, I appear before your Committee today in my personal capacity and the views that I express are my own.

This year, Secretary Chertoff and his team at the Department of Homeland Security (DHS) have made real progress in implementing the SAFETY Act by issuing final regulations in June, revising the application procedures in August, and approving SAFETY Act technologies at a more rapid pace. DHS deserves praise for these advances that bring the SAFETY Act closer to realizing its potential to expedite the development and deployment of anti-terrorism technology. However, the terrorists are not resting and neither can we. More remains to be done to better align the DHS implementation of the SAFETY Act with the Congressional intent to accelerate the availability of anti-terrorism technology by providing statutory protection from liability lawsuits arising out of terrorist acts. As discussed below, implementation of the SAFETY Act would benefit from the following enhancements:

- Assuring the Confidentiality of SAFETY Act Data
- Encouraging the Development of Breakthrough Technologies
- Synchronizing Procurements and SAFETY Act Approvals
- Extending the Duration of SAFETY Act Protection
- Establishing an Appeals Process

The SAFETY Act's Purpose to Promote Anti-Terrorism Technology

The DHS implementation of the SAFETY Act must be measured against the statutory purpose established by Congress. The SAFETY Act has a purpose that is both simple and clear—save lives through anti-terrorism technology. To clear the path for such technology to move from the drawing board to the "Nation's front-line defense," Congress created protections against liability lawsuits:

> The Select Committee [on Homeland Security] believes that technological innovation is the Nation's front-line defense against the terrorist threat. Unfortunately, the Nation's products liability system threatens to keep important new technologies from the market where they could protect our citizens. In order to ensure that these important technologies are available, the Select Committee believes that it is important to adopt a narrow set of liability protections for manufacturers of these important technologies.[1]
>
> * * *
>
> Briefly, the SAFETY Act ensures that U.S. companies will be able to develop and provide vital anti-terrorism technologies to help prevent or respond to terrorist attacks—without the threat of crippling lawsuits.[2]

This purpose rests upon a fundamental, Congressionally recognized premise—anti-terrorism technology is essential to Homeland defense.[3] Quite simply, we cannot secure over 100,000 miles of land and sea borders—much less our cyber borders—merely with guns, guards, and gates.[4] Only with technology can we tackle the gargantuan tasks of defending our vast borders and infrastructure against terrorism, while maintaining the flow of commerce, as mandated by the Homeland Security Act of 2002. Pub. L. No. 107–296, § 402(8), 116 Stat. 2178. Consequently, the appropriate question is whether the DHS implementation of the SAFETY Act fully and effectively serves this objective of fostering more anti-terrorism technology, more quickly, and more efficiently for Homeland Security.

In its final rule, DHS recognizes the purpose underlying the SAFETY Act: "The purpose of this rule is to facilitate and promote the development and deployment of anti-terrorism technologies that will save lives." 71 FED. REG. 33147 (June 8, 2006). While both the DHS final rule and revised application kit represent considerable improvements over their predecessors, further revisions must be made to assure that neither the spectre of crippling liability lawsuits nor the hurdles of the DHS review process foreclose or delay our access to the most robust arsenal of anti-terrorism tools.

DHS Enhancements for Opening the Anti-Terrorism Technology Pipeline

The following enhancements would serve the SAFETY Act's purpose by encouraging more companies to accelerate the pace of bringing the widest array of technology to our battle against terrorism.

Assuring the Confidentiality of SAFETY Act Applications & Data

In its earliest proposed rules on the SAFETY Act, DHS acknowledged "that successful implementation of the Act requires that applicants' intellectual property in-

terests and trade secrets remain protected in the application process and beyond." 68 FED. REG. 41423 (July 11, 2003). In the latest rules, DHS has taken commendable steps to maintain the confidentiality of SAFETY Act application data by: (1) treating "the entirety of the application" as "confidential under appropriate law"; (2) recognizing the applicability of various trade secret laws to the application information; and (3) committing to "utilize all appropriate exemptions from the Freedom of Information Act." 71 FED. REG. 33151, § N and 33168, § 25.10 (2006). However, DHS needs to take additional steps to assure SAFETY Act applicants that their most valuable technologies and secrets will be secure. Two key steps are: (1) establish a sound information security program; and (2) provide transparency and controls for any sharing of SAFETY Act data.

Information Security Program. A sound information security program is critical to avoid disincentives for companies to share SAFETY Act data about their most valuable technologies with DHS.[5] The new rules encourage electronic applications, but still do not address the concerns raised during the 2003 hearings on SAFETY Act implementation:

> 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 . . . . 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.[6]

These concerns have been magnified by cybersecurity issues that continue to challenge DHS, including: (1) failing scores on information security for the past two years on the Federal Information Security Management Act (FISMA) report card;[7] (2) continuing delays in filling the Assistant Secretary for Cybersecurity position;[8] and (3) various information security concerns identified by the Office of Management and Budget (OMB), GAO and the DHS Inspector General.[9] While the SAFETY Act regulations include DHS commitments to protect the confidentiality of applicant data, DHS needs to roll out a FISMA-compliant information security program built around the standards published by OMB and the National Institute of Standards and Technology (NIST).[10] With sound information security, DHS can better achieve the SAFETY Act purpose of encouraging more applicants to offer a broader array of technology due to their confidence that DHS will protect their confidential data.

Transparency & Controls for Information Sharing. In 2003, the interim SAFETY Act regulations stated that DHS "shall establish confidentiality protocols for maintenance and use of information submitted to the Department under the SAFETY Act and this part." 68 FED. REG. 59703, § 25.8 (2003). The final SAFETY Act regulations offer little more transparency or detail, stating that DHS "shall establish confidentiality procedures for safeguarding, maintenance and use of information submitted to the Department under this part." 71 FED. REG. 33168, § 25.10(a) (2006).[11] These latest SAFETY Act regulations do not address industry concerns lingering from the 2003 SAFETY Act hearings regarding with whom DHS may share data, under what conditions, and with what controls in place. In both their testimony to Congress and comments to DHS, the major industry trade associations requested greater transparency and protection:

> 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.[12]

As the "focal point for the security of cyberspace" under Homeland Security Presidential Directive (HSPD) 7 (Dec. 7, 2003), DHS can demonstrate its leadership role in this area by establishing "best practices" for guarding the confidential information of SAFETY Act applicants. In particular, DHS should adopt SAFETY Act regulations that not only incorporate the industry requests above (notice, consent, and review), but should also include technical and management controls (e.g., digital audits and watermarks) capable of tracking who received the data, which recipients signed non-disclosure agreements, what copies have been made, and when audits and training have been conducted. By publishing and implementing such rules governing SAFETY Act data, DHS will greatly enhance both its capability and credibility to protect this confidential information.

Encouraging Development of Breakthrough Technologies

The new regulations properly recognize the eligibility of developmental technology (*i.e.,* technology that is being developed, tested, evaluated, modified or is otherwise being prepared for deployment") for SAFETY Act protection. 71 FED. REG. 33161, § 25.4(f) and 33156, § R (2006). However, these regulations and new Application Kit appear to establish an undue preference for existing technologies. At least six times, the Application Kit repeats the following statement emphasizing past or current sales as a critical factor in the approval process: "It may be very important and could significantly expedite your application if your Technology has been acquired or utilized (or is subject to an ongoing procurement) by the military, a Federal agency, or a state, local or foreign government entity." Application Kit at 21, 23, 27, 34, 35, 40 (July 2006). More worrisome, the new regulations create a second-class status for developmental technologies, imposing "limitations on the use and deployment" of such items, making approval "terminable at-will" by DHS, and generally restricting the duration of the designation ("presumptively not longer than 36 months"). 71 FED. REG. 33156, § R (2006).

The new SAFETY Act regulations and Application Kit send the wrong message, and create the wrong incentives, for companies building the anti-terrorism arsenal. Due to the heightened uncertainties in the SAFETY Act approval process for such breakthroughs, companies have greater incentive to invest their research dollars in anti-terrorism technology ready to be fielded now, rather than in breakthrough technologies that may revolutionize the war against terror. We cannot afford to focus the SAFETY Act approvals solely upon today's technologies (i.e., detecting conventional explosives) when the terrorists have moved on to nail polish and peroxide to build bombs in mid-air.[13] Furthermore, approvals burdened with "limitations" and "terminable at-will" conditions undermine the certainty needed to foster new anti-terrorism technologies, as the DHS rules acknowledge: "The Department is aware of this concern and understands that undependable or uncertain liability protections would not have the desired effect of fostering the deployment of anti-terrorism technologies." 71 FED. REG. 33152, § D (2006). As the purpose of the SAFETY Act is to provide "critical incentives for the **development** and deployment of anti-terrorism technologies" (71 FED. REG. 33147 (2006) (emphasis added)), development of such technologies should not be shortchanged.

In any event, the effort to distinguish between developmental and existing technologies may be illusory, as most technologies have elements of both:

> 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.[14]

Indeed, nearly all of the major Homeland Security programs include ongoing, evolutionary design and development work in parallel with other program activities.15 As the president of one trade association explained, companies need to know during the design phase whether SAFETY Act protection is available:

> 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.[16]

Thus, the DHS regulations and Application Kit should make clear that the SAFETY Act approval process will welcome both developmental and existing anti-terrorism technology and that companies will not be penalized in the application process for presenting breakthrough technologies for review and approval.

Synchronizing Procurements and SAFETY Act Approvals

In its latest regulations, DHS "recognizes the need to align consideration of SAFETY Act applications and the government procurement process more closely." 71 FED. REG. 33156, § P (2006). In addition, DHS has identified several procedures that should assist in accomplishing this objective, including (1) the option for agencies to seek "a preliminary determination of SAFETY Act applicability," (2) the use of "Block Designation or Block Certification," and (3) the potential that DHS "may expedite SAFETY Act review for technologies subject to ongoing procurement processes." 71 FED. REG. 33156, § P (2006). These procedures represent positive steps towards the critical objective of synchronizing procurements and SAFETY Act approvals. However, more needs to be done, as discussed below.

For companies selling anti-terrorism technology, the parallel track of procurements and SAFETY approvals presents substantial risks and uncertainties:

- *Disqualification:* Company is disqualified because it conditioned its bid upon receiving timely SAFETY Act approval;
- *Delay:* Company receives award prior to SAFETY Act approval, thus "betting the company" during the interim; or

• *Default:* Company receives contract award—but not SAFETY Act approval—forcing company either to default or to perform at risk.

According to an NDIA survey, "25 percent of the respondents had 'no bid' over 50 procurements because the company would be unable to obtain SAFETY Act protection in time for the procurement." [17] While such "no bid" actions may be less common with the accelerated pace of SAFETY Act approvals, the risk of losing opportunities for major technological advancements and breakthroughs must be carefully weighed in light of the purpose of the SAFETY Act.

In particular, DHS can foster the development and deployment of anti-terrorism technology by accepting the risk of delayed SAFETY Act approval. For example, DHS could offer indemnification under Public Law No. 85–804 or authorize bids contingent upon SAFETY Act approval.[18] By shouldering approval risks that fall almost entirely within its control, DHS would expand the field of competition and the array of anti-terrorism technologies available to both DHS and the public.

In addition, the approval process should benefit from a new position for a SAFETY Act technology advocate tasked with breaking bottlenecks, resolving impasses, and expediting critical applications. Such a technology advocate would reduce the risk of approval delays that plagued a similar process in the 1960's and 1970's when a small part of the Food & Drug Administration (FDA) review staff occasionally delayed life-saving drugs with excessive information demands.[19] In addition, a SAFETY Act technology advocate would help DHS to avoid the type of pitfalls encountered by the pharmaceutical industry when the FDA review staff found it easier to deny, than approve, applications.[20] With this technology advocate, the DHS objective would be directly aligned with Congressional intent that the SAFETY Act "Support" and "Foster" anti-terrorism technologies to save lives.

Extending the Duration of SAFETY Act Protection

Without identifying any support in the statute itself, the DHS final rule imposes a mandatory sunset period upon approved anti-terrorism technology, thus requiring renewal every "five to eight years" to maintain protection. 6 C.F.R. 25.6(f), (h); 71 FED. REG. 33163–4 (2006). Since the time that DHS initially proposed this "five to eight year" period in 2003, industry consistently opposed it.[21]

DHS seeks to justify this rule based upon the assumption that the approval depends upon factors such as "a specific threat environment, the nature and cost of available insurance, and other factors all of which are subject to change." 71 FED. REG. 33155, § N (2006). However, the factual basis for this assumption is unclear, as some technologies—like blast-proof glass and bomb-sniffing dogs—will change at glacial paces, if at all. If either the technology or the insurance requirements change, the DHS rules already impose reporting requirements that assure continued DHS supervision. 6 C.F.R. §§ 25.5(g), (h), 25.6(l), 71 FED. REG. 33162, 33165 (2006). If the threat environment changes, new technologies will replace the old. Thus, this agency-imposed restriction on the statute appears neither justified nor necessary.

In any event, the DHS mandatory sunset period cannot be squared with the express terms or purpose of the SAFETY Act. First, the SAFETY Act establishes statutory protections without any term limits. For example, the Act states that "No punitive damages . . . may be awarded," rather than that "No punitive damages . . . may be awarded for **five to eight years.**" 6 U.S.C. § 442(b)(1). If Congress intended to limit the duration of statutory protections, the SAFETY Act surely would have said so. Second, the limited shelf-life for approved technologies will create a bow wave of renewals in five to eight years, burdening industry and DHS alike with paperwork and distracting both from the more important task of seeking and approving new technologies. Unless the review is a mere formality (in which case it is unnecessary), the additional burden and risk undermine the incentives for technology investments. Accordingly, the DHS renewal requirement runs counter to the statutory purpose of encouraging and facilitating the development and deployment of more technology more quickly.

Establishing an Appeals Process

Even for an arbitrary or unreasonable denial of a SAFETY Act application, the DHS rules cut off any opportunity for an administrative or judicial appeal. 6 C.F.R. § 25.9(c)(2), 71 FED. REG. 33167 (2006) ("Under Secretary's decision shall be final and not subject to review"). Instead, DHS suggests that an "interactive process" in which an applicant may "provide supplemental information and address issues" is "sufficient recourse." 71 FED. REG. 33155 § O (2006). Since 2003 when DHS proposed an "interactive process" without any appeal, the major trade associations expressed the need for an appeals process.[22]

This DHS policy of unreviewable denials is contrary to legislative intent favoring liberal approval, not rejection, of liability protection for anti-terrorism technology: "it is Congress' hope and intent that the Secretary will use the necessary latitude

to make this list as broad and inclusive as possible, so as to insure that the maximum amount of protective technology and services become available."[23] Furthermore, this "no appeal" policy sends the wrong message, shielding the DHS reviewers from scrutiny or accountability for denying applications and discouraging companies from pursuing applications that may be denied without recourse. Finally, while DHS has accelerated the pace of approvals in the past year under Secretary Chertoff's leadership, the DHS rules do not include any procedural safeguards that would prevent a return to the period when DHS approved just six technologies in sixteen months.[24] Given the SAFETY Act's purpose to "save lives" through technology (71 FED. REG. 33147 (2006)), the right time for an appeals process is now, not after a terrorist incident causes us to regret the unavailability of a technology that could have protected us.

In the federal realm of agency actions, administrative or judicial review is the rule, not the exception. More than 50 years ago, agencies contended that rejection of a contractor's bid was too discretionary for external review, but the Court of Claims disagreed, instead recognizing a disappointed bidder's right to judicial review for breach of an agency's implied duty "to give fair and impartial consideration" to bid and proposal submissions. *Heyer Prods. Co. v. United States,* 135 Ct. Cl. 63, 69 (1956). In addition, agencies themselves have acknowledged the need for administrative or judicial review by establishing procedures for appeals and protests for everything from pesticides and pharmaceuticals to radio frequency (RF) devices and federal contract awards.[25] For SAFETY Act anti-terrorism technology designed to save lives, the case for a review or appeals process is at least equally compelling—if not more so.

Conclusion

Under Secretary Chertoff's leadership, DHS should be commended for bringing the SAFETY Act much closer to achieving its statutory purpose. With additional enhancements described above, the SAFETY Act can reach its full potential of facilitating the development and deployment of technologies essential to our fight against terrorism. I am available to answer your questions.

Endnotes

[1] H.R. REP. NO. 107–609, Pt. 1, at 118 (July 24, 2002).

[2] 148 CONG. REC. E2079 (daily ed. Nov. 15, 2002) (statement of Rep. Armey).

[3] *Border Technology: Keeping Terrorists Out of the United States: Hearing Before the Senate Subcomm. on Terrorism, Technology & Homeland Security and Subcomm. on Immigration, Border Security and Citizenship of the Comm. on the Judiciary,* 108th Cong., 1st Sess. 1–8 (Mar. 12, 2003) (statement of Sen. Kyl: "people can't possibly patrol the entire area, and therefore we are going to have to continue to enhance the application of technology") (statement of Sen. Feinstein: "technology is not the sole answer . . . but it is an essential element"); (statement of Sen. Kennedy: "We know that a great deal more has to be done in this area not only in getting the best technology, but also having it interoperable").

[4] "The old security paradigm in this country of guns, gates, and guards is changing fast. And technology is going to replace it all." *Fiscal Year 2004 Homeland Security Appropriations: Hearings Before House Subcomm. on Homeland Security of Comm. on Appropriations,* 108th Cong., 1st Sess. (Mar. 20, 2003) (statement of Rep. Wamp).

[5] With respect to critical infrastructure information, the Government Accountability Office (GAO) has documented instances in which industry does not share information with DHS due to concerns about "potential release of sensitive information" and uncertainty about how such information "will be used or protected from disclosure." GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 14 (July 19, 2005) (GAO–05–827T).

[6] *Implementing the SAFETY Act: Advancing New Technologies for Homeland Security: Hearings before House Comm. on Government Reform,* 108th Cong., 1st Sess. 44 (statement of Mr. Miller) (hereinafter the *"2003 House SAFETY Act Hearings"*).

[7] Rep. Davis, "No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards," House Comm. on Government Reform (Mar. 16, 2006) *(http://reform.house.gov/UploadedFiles/TMD%20FISMA%2006%20Opener.pdf).*

[8] Krebs, "A Year Later, Cybersecurity Post Still Vacant," *Washington Post* p. A21 (July 13, 2006); "Democratic Senators, Industry Coalitions Urge DHS to Fill Still Vacant Cyber-Chief Slot," *BNA Privacy Law Watch* (July 14, 2006).

[9] OMB, *FY 2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* at 39 (Mar. 1, 2006) (43% of DHS systems certified and accredited; 52% of security controls tested); id at 40 (DHS IG gave rating of "Poor" to DHS) (*http://www.whitehouse.gov/omb/inforeg/reports/2005*_fisma_report_to_congress.pdf); GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 9–10 (July 19, 2005) (GAO–05–827T) (identification of DHS cybersecurity responsibilities and problem areas).

[10] OMB Circular No. A–130; OMB News Release, "OMB Reinforces Strict Adherence to Safeguard Standards" (June 26, 2006); OMB Memo to Department and Agency Heads, "Protection of Sensitive Agency Information" (June 23, 2006) (M–06–16) (*www.whitehouse.gov/omb/memoranda/fy2006/m06–16.pdf*); NIST Special Publication 800–53A (2nd Public Draft) (Apr. 2006) (*http://csrc.nist.gov/publications/drafts.html#sp800–53–Rev1).*

[11] The DHS commitments to require non-disclosure agreements and to check for potential conflicts of interest are not new, as both the interim regulations in 2003 and the final regulations in 2006 address these issues. 68 FED. REG. 59687 (2003); 71 FED. REG. 33151 (2006).

[12] *2003 SAFETY Act Hearings* 54 (statement of Mr. Miller); *id.* at 150 (comments of Information Technology Association of America (ITAA), the Professional Services Council (PSC), the Aerospace Industries Association (AIA), and National Association of Manufacturers (NAM).

[13] "Technology isn't available to detect potentially lethal liquids hidden in sports drink bottles or other containers. The foiled airline attack from the U.K. highlighted the merits of good intelligence, which stopped the liquid bomb scheme before it reached a critical point." Alva, "Billions of Dollars Buy Tighter Security But Work Remains," *Investor's Business Daily* A1 (Sept. 11, 2006).

[14] *2003 House SAFETY Act Hearings* 58 (statement of Mr. Soloway).

[15] GAO, *Homeland Security: Progress Continues, but Challenges Remain on Department's Management of Information Technology* 30–31 (Mar. 29, 2006) (GAO–06–598T) (discussing challenges relating to requirements definition and development for major Homeland Security programs).

[16] 2003 House SAFETY Act Hearings 65 (statement of Mr. Soloway).

[17] NDIA and PSC letter to DHS Under Secretaries Hale and McQueary dated Feb. 3, 2005.

[18] For the Secure Border Initiative (SBI) Net program, the DHS Request for Proposals specifically recognizes that the procurement should be covered by the SAFETY Act, but warns offerors that "Proposals in which pricing or any other term or condition is contingent upon SAFETY Act protections of the proposed product(s) or service(s) will not be considered for award." In a number of other procurements, contractors have been disqualified for conditioning their proposals upon SAFETY Act approval.

[19] For example, in 1969, one FDA reviewing officer repeatedly demanded more data on the efficacy of aspirin in preventing heart attacks (including submission of all prior literature on aspirin), ultimately forcing E. R. Squibb & Sons, Inc. to abandon the research initiative. Wardell, "Rx: More Regulation or Better Therapies?" *Regulation* at 25–6 (Sept.–Oct. 1979). Five years later, studies by the National Institute of Health (NIH) confirmed substantial reductions in heart attacks attributable to aspirin, thus demonstrating the costs of unnecessary delays in the drug approval process. *Id.; see also* Elwood & Sweetnam, "Aspirin and Secondary Mortality After Myocardial Infarction," *The Lancet* 1313 (1979).

[20] The former FDA Commissioner described the incentives for FDA staff to take "negative action on new drug applications" as "intense" during the late 1960's. Grabowski, Drug Regulation and Innovation 76 (quoting speech by former FDA Commissioner Schmidt before the National Press Club in Washington, DC on Oct. 29, 1974).

[21] DHS does not explain why "five to eight years" represents an appropriate period of time. During hearings in 2003, the president of the ITAA objected to the "arbitrary timeframe for designation," adding alternatively that "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." *2003 House SAFETY Act Hearings* 48 (statement of Mr. Miller). Similarly, the PSC president testified that "there is no public policy reason to impose any fixed period of time on the useful life of the Designation period of a QATT [qualified anti-terrorism technology]. Indeed, in some cases, a contract performance period can extend beyond five or eight years." *Id.* at 65 (statement of Mr. Soloway).

[22] *2003 House SAFETY Act Hearings* 55 (statement of Mr. Miller). In comments on the DHS proposed regulations in 2003, the ITAA, PSC, AIA, and NAM all requested an appeals process. Id. at 149.

[23] 148 CONG. REC. E2080 (daily ed. Nov. 15, 2002) (statement of Rep. Armey).

[24] "Shortly after being sworn in, Secretary of Homeland Security Michael Chertoff stated: 'There is more opportunity, much more opportunity, to take advantage of this important law, and we are going to do that.'" 71 FED. REG. 33148 (2006). During the earlier phase of SAFETY Act implementation "from October 2003 to February 2005, six technologies were designated Qualified Anti-Terrorism Technologies under the SAFETY Act." *Id.*

[25] C.F.R. § 152.118(e) (2006) (right to hearing for denial of application for insecticide, fungicide or rodenticide); 47 C.F.R. §§ 1.106, 1.115 (2006) (petition for reconsideration by Federal Communications Commission (FCC) staff or for review by the FCC Commissioners for denial of RF equipment authorization); 21 C.F.R. §§ 201,235 (2006) (hearing or judicial review for denial of a new drug application); Federal Acquisition Regulation (FAR) § 33.103 (agency review and alternative dispute procedures for disappointed bidders for federal contracts).

Mr. REICHERT. Thank you, Mr. Bodenheimer.

I will first go to Ms. Jackson-Lee for her questions.

Ms. JACKSON-LEE. Thank you very much.

And I do appreciate the witnesses and thank you for your understanding of our schedule. I want to raise a concern that looms over the heads of the traveling public.

Obviously, the recent finds or discoveries, if you will, law enforcement—a combination of intelligence authorities just the past couple of weeks with the British busting of a potential terrorist act.

That then sent, of course, the summer travel schedule spinning, as well as the thoughts and minds of travelers, and then, of course, the determination decisions that have to be made by the industry.

You have a traveling public that now is forbidden from taking toothpaste onto their carriers on the basis of safety. But certainly, as Americans and many times as travelers, we are used to convenience.

That is an element, if you will, for technology, either how you detect it, how you use the sophistication of the screening system to ensure that you are able to secure but also that you are able to provide the traveling public with the conveniences that they understand and expect, not deflecting the importance of homeland security.

So let me ask Mr. Bodenheimer, because you mentioned the words best practices, you mentioned breakthrough, developmental, et cetera, which are words that are music to me, what is thwarting this new department and the SAFETY Act to do meaningful technology and research? That is something that we need.

We are being delayed and detained. So let me just pose that question to you, and I don't know if you reviewed the department structure, but you have heard Secretary Cohen. What more do we need to do?

And this is urgent. And I would imagine that the traveling public—but America believes that homeland security and technology is urgent. What do we need to do? I yield to the gentleman.

Mr. BODENHEIMER. I fully agree with you that this, in fact, is urgent. We are talking about not only lifesaving technology but, as you point out, technology which will provide the flow of commerce so that we don't choke our economy through lacking the type of technologies to keep us not only safe but also economically viable.

I think DHS needs to put the resources in here as a top priority. I believe that in terms of staffing they need not only additional staffing but, in addition, a lack of turnover.

One of the comments that I have heard is when an application goes in, you never know whether you are going to be dealing with the same person today that you deal with tomorrow and next time.

I believe that they need to bring in the necessary expertise to be able to push the applications through rapidly. I think they also need to take the steps of assuring confidentiality of the information, of encouraging the breakthrough technologies so that the message gets out to industry that they know that they are welcome and they are protected when they provide their information.

Ms. JACKSON-LEE. Let me yield back to the distinguished—unless there is someone desiring to—I will take a quick response.

Mr. HOWELL. I think that one of the most interesting parts of the reorganization plan that Vice Admiral Cohen has put together is he has reoriented the Science and Technology Directorate so that it serve the needs of its customers, its customers as he has defined them in his reorganization plan as being the directorates within DHS.

Therefore, he will be more responsive and directly responsive to the needs of TSA and what it sees as the threats, and therefore put science and technology research dollars toward those threats. That

was not the case prior to his reorganization plan. We think that is critically important.

We also have or would argue that his additional set of customers is the owners and operators of the critical infrastructures and finding a way to integrate their needs, their desires, their views on threats and research and development priorities based on those threats is absolutely essential.

And then once you have an understanding of the priorities of both the public-and private-sector customers that he responds to, have a SAFETY Act process that prioritizes and expedites those is appropriate in our view.

Ms. JACKSON-LEE. Thank you.

Mr. Soloway, I think you had—it looks like I am getting a lot of—if I can get Mr. Soloway and if you can do yours in seconds, and then Mr. Meldon. Thank you.

Mr. Soloway?

Mr. SOLOWAY. Thank you, Ms. Jackson-Lee. I would just suggest that in this discussion we can't divorce the discussion of the S&T organization with sort of the broader procurement regime of the federal government, which does involve Congress. It does involve the Office of the Chief Procurement Officer.

And two quick analogies. In the Clinton administration I served in the Defense Department in a senior acquisition position, and one of our great challenges was opening up our acquisition processes to cutting-edge technologies, be they very small firms out in the hinterlands or very large firms who would not do business with the government because of so many of the unique rules and requirements that we layered on them.

More recently, in the aftermath of Katrina, I traveled to Mississippi with Mr. Thompson to talk to four or five dozen small businesses in his district that wanted to participate in the cleanup process. And we spent a whole half day with them walking through all of the requirements associated with doing government contracting.

So part of this is an organizational challenge for S&T. Part of it, I think, is a broader discussion of do we have the right procurement regime in place to attract those firms in a way that they can afford to do business with the U.S. government. And that would involve the Congress as well as the department.

Ms. JACKSON-LEE. Thank you, Mr. Soloway.

Mr. Meldon?

Mr. MELDON. I would add the following, Ms. Jackson-Lee. Number one, I think that what needed to be done was done. I.e., once the problem was identified, there was a sense of urgency and industry responded. Remember, industry is also part of this equation, as is the Department of Homeland Security.

Number two is that in Undersecretary Cohen's remarks, he mentioned dual-use technology. We can't assume that we know what the next terrorist's use of some technology for a benign purpose is going to be for the wrong purpose.

Therefore, what industry is looking for from the department is prioritization of future R&D development for dollars to be spent on what the next threat is going to be.

Who would have imagined that a Coca–Cola or Gatorade could be used to blow up an airplane, okay? Well, now we know. Now we are responding. The government and industry is responding.

But how do you prioritize that? That is something that I think needs to be considered.

Ms. JACKSON-LEE. It is a good question to leave on, Chairman Reichert. Thank you very much for your indulgence.

And on our side, let me simply say the word "urgent" should be the word resounding out of this room. And I think there is some good instruction from these individuals on small businesses, on cutting-edge technology, on industry.

And, Mr. Chairman, maybe we can work on getting this, I guess, infant sector of the Homeland Security Department—Secretary Cohen; we are glad he is there—to give priorities, because I think that is going to be key.

We can't be constantly in the back side of the issue. We have got to be in the front side. Now we are trying to find out about Gatorade and Coca–Cola and everything else. I know all of us would have hoped that maybe intelligence and otherwise could have gotten us 6 months out at least. And how do we counter these?

So I hope maybe this committee can help focus on that priority. Thank you, Mr. Chairman.

Mr. REICHERT. Thank you, Ms. Jackson-Lee.

I want to maybe just make a couple of comments first before I ask my questions. Maybe some of you know I was sheriff in Seattle for a number of years, 33 years in law enforcement. My last 8 years, I was the sheriff of King County in Seattle, Washington.

Part of my duties, of course, was to come before the county council—it was a 13-member committee—and testify. And every now and then I would show up and there would be one or two people sitting in the chair. And I would be a little bit offended, because I thought what I had to say was important.

I just want to remind you that because you have two members sitting here does not mean your testimony is not important. This is critical for us to hear. Your testimony is critical.

The number of people sitting on the dais here doesn't apply to the importance of your input.

One of the things that we have done in our subcommittee is we have taken every statement by every witness, since I took the chair of Science, and Technology, Emergency Preparedness back in October of last year, and evaluated each one of those statements as if I were investigating a murder case, looking for commonalities positive, looking for commonalities negative.

And then you base your legislation upon the information that you provide in your statements. So I don't want you to leave here today thinking that your presence here was not appreciated and is not important, because your testimony, your statements, will all be reviewed and thoroughly examined so that we can begin to work with you.

This isn't a job, as someone said in their testimony, just for Homeland Security, but for a number of other departments, and for businesses that you represent across this country and for members of Congress. So all of us are in this together.

And since there are only two of us, I will take just a little bit more time to say that I really understand this progression of science, not because I have any real background in science, but because in my experience in investigating one of the most horrendous crimes ever committed in this country, a series of murders in Seattle where 80 people were killed, and we were able to convict someone for 50 of these murders. The science was the key.

The science will be the key in homeland security. And I know that the undersecretary is keenly aware of that and has presented a plan.

But in 1982, having a Rolodex file, no computers, no AFPIS—automated fingerprint identification system—no idea that DNA was on the horizon, but only a blood type is what we were looking for. And years later, DNA arrives and a fingerprint identifying the man responsible for the death of at least 80 people.

So we know where this is headed, and we know that we have the right man in charge of this effort, and we know that we have a great dedicated group of people like yourselves representing businesses across this country involved in this process.

So my first question is what is the most common criticism you hear from businesses about the SAFETY Act. And anyone on the panel can—what is the most common criticism? Is it the process, the application process, or what is the most common criticism?

Mr. Finch?

Mr. FINCH. Mr. Chairman, I would say in my experience, among the most normal criticisms that we get is that the application process to date has been overly involved and has required too much detail in terms of the amount of information that must be provided.

Everybody understands the responsibility of the Department of Homeland Security to conduct a meaningful review and to have faith in its determination that the technology at issue is, in fact, safe, effective and useful.

But over the past years, as I mention in my testimony, what constitutes sufficient information has fluctuated up and down. It has varied from application to application. If you submit enough applications, you can see patterns. But if you are relatively new to the process, it can catch you a little bit by surprise.

And I think the department has taken that to heart, and I believe Secretary Chertoff, from the moment he assumed his position, understood that improvement needed to be made to the process and that it had to be a quicker, leaner and more efficient process. Not to say that it would be a rubber stamp; nobody would ever expect that. Nobody would ever agree to that.

However, they do understand that it may not necessarily require drilling down to the subatomic level on some of these applications. Applicants sign their name to this application saying that everything is truthful that is included. And if they don't do that, then they suffer consequences at a later date.

Mr. REICHERT. Thank you.

Mr. Soloway?

Mr. SOLOWAY. Yes, if I could just add on to that, and I second Mr. Finch's comments, I think first of all the emergence of the final rule has eliminated some of the more common comments that we have had over the last several years.

But a number of us made reference in our comments to a streamlined application kit. And I want to be clear—and I think Mr. Finch made the point that no one is suggesting a rubber stamp here, but leaving aside for a moment the amount of information the department determines it needs, there is also a staggering of timing of information.

How much does the department need at various stages of this process? And to load it front end all the way oftentimes requires levels and degrees of information that either you can't even get at that moment, are not necessarily relevant to that moment in time.

So part of the point of the application kit that this coalition of groups created was really to define a staggering so that you are not staggered at the very front end by this total volume that you don't really need to get through that level of process at that time.

So there is also a timing issue for the volume of information as well as a definition of the total volume that you need.

Mr. REICHERT. Mr. Meldon?

Mr. MELDON. In keeping with your question about commonality of themes, Mr. Reichert, I would say that as Undersecretary Cohen mentioned in his remarks, there is a supposed 120-day to 150-day period by which these applications are to be reviewed and passed on.

And the problem with that is that if the department comes back with questions for the seller of the technology within 90 days or 100 days, the clock starts all over again, so it is not a flat 120 days. It is a flat 120 days after the final submission of all of the information that has been requested by the department relative to the certification and designation of the technology.

Mr. REICHERT. Any other comments?

Mr. Bodenheimer?

Mr. BODENHEIMER. It depends in part upon the size of the business. One of the things that I have found is that the small-and medium-sized businesses have been completely terrified by the process of going through the application, trying to comply with the regulation.

I still have heard from even the large businesses that the new application demands a very large amount of information, and they anticipate that the burden will not be substantially lessened.

The most common complaint I hear from the large companies is this issue of synchronizing the procurement process with the SAFETY Act approval process that several of the panel members have identified.

There are a number of companies who simply will not bid on government procurements out of fear that they will not get the SAFETY Act approval in time.

Mr. REICHERT. Because of the length of the process and the complications of the process, there is a cost involved to the companies that are looking at completing the paperwork and going through this process, besides the time of the employees involved in trying to research and fill out the paperwork, is that—

Mr. BODENHEIMER. Yes. There is a huge burden in filling out the applications. I believe Mr. Soloway in 2003 identified a burden of about 1,000 hours to fill out the applications, and some of the large

businesses are telling me that still they anticipate the burden will be in the same range.

Mr. REICHERT. Mr. Finch?

Mr. FINCH. I would like to comment on that a little bit, again, given my experience in working with companies both large, small and in between. Your experience depends on the company you are dealing with.

I would say, actually, in a number of instances where I have dealt with smaller companies, the process has actually been somewhat easier for them, if for no reason other than they are a little bit more nimble than the larger companies.

There is less people who retain the information that is necessary for the SAFETY Act review process. So it can vary from time to time and from company to company.

And you know, on a related note, when we were talking about the marriage of procurement and the SAFETY Act, again, I think it cannot be overstated that one of the great successes of the new rule and the new application kit is this prequalification process.

You talk about, you know, companies not willing to bid upon a particular procurement because they are concerned they won't get SAFETY Act approval. The department has heard that criticism, heard it from some of the largest municipalities in the country, who said we need these technologies, but we need to also guarantee that they will receive SAFETY Act approval.

By virtue of the prequalification, there is now a process in place to assure that whoever wins that particular procurement—and it doesn't have to be a particular company; it can be whoever wins, one of five companies, 10 companies, 15 companies that bids—they will be assured by virtue of the prequalification process they will ultimately receive SAFETY Act approval.

And that is an important aspect that I think cannot be understated. And the department should, frankly, again, be applauded for that.

Mr. REICHERT. Thank you.

Any other comments?

Mr. Howell, in your testimony you remarked that DHS needs to strengthen its procurement and acquisition process in order to achieve coordination with antiterrorism procurements and the SAFETY Act.

Do you have some performance metrics in mind?

Mr. HOWELL. Candidly, I think it comes down to the issue of performance metrics. One of the largest challenges that I think Ms. Duke and others in the DHS procurement office have identified is coming up with effective performance metrics for antiterrorism procurements.

One of the biggest challenges in measuring things like responses to SBInet proposals is the lack of performance metrics in that request for proposal.

It is designed to be a very open-ended process where vendors come forward with unique solutions, yet at the same time that creates a challenge. How does one define the efficacy of a technology and therefore determine its efficacy in a SAFETY Act review and as part of the procurement process?

And you know, a lot of it gets to the challenges that DHS procurement officials face, and I would defer part of this to Mr. Soloway, because he is much more expert in this area than I am. But the procurement staff, as we all know—the sense of urgency has been discussed here repeatedly.

There is an extraordinary sense of urgency in the DHS procurement staff, in that they must perform probably under compressed time frames from what they might otherwise be used to in going through an orderly process of conducting market research, planning a procurement strategically, building out their performance metrics, and then actually putting their procurement on the street.

All of those time frames are extraordinarily compressed, and finding a way to incorporate liability issues and SAFETY Act concerns in that process, I would argue, has been a tremendous challenge, as has been the whole issue of identifying performance metrics.

And I would invite Mr. Soloway to add some additional meat onto those bones.

Mr. SOLOWAY. I would just make two very quick comments. Number one, I think performance metrics are critical, but I don't think we can hold people accountable for performance metrics until we give them the tools to meet the performance we expect and are asking.

And that is really a training and education challenge for the department, and I think the Congress can be very helpful here.

Our office has worked with Mr. King and Mr. Thompson on prospective legislation to help essentially close off or closet off some funds to ensure that the office of procurement has adequate funds to train its workforce, because, as you know, in tight budgets, some of the first things to get cut are training and travel.

So we have to give the people the tools first before we hold them accountable, though I agree fully with Mr. Howell.

I think the second thing is to have a lot more engagement between DHS and this committee and others so that as people are trying to do things innovatively, particularly in a compressed time frame, particularly when a new threat emerges and we need action quickly, that we don't have a lot of after-the-fact second-guessing when people have acted in good faith, whether or not they have done everything absolutely right.

There can be mistakes made, and try to separate that out, and so the workforce knows that it is supported both in their department and on the Hill and elsewhere to be innovative and go out and react quickly to challenges as they emerge.

Mr. REICHERT. Well, I want to thank all of you for your testimony today and your patience. And we have a short month of work here, so everyone is running off to other hearings here and there.

But I recognized a few things that I want to mention very quickly. One, we are, I think, very encouraged that communication that we talked about here today is in existence, and people are working on that, and it is absolutely the key to our success.

The undersecretary recognized that. As soon as he took office, he opened communication with our staff on both sides and personally sat down and had discussions with them. And I know that he will

be doing that with you if he hasn't done that already, and he has been seated behind you the entire time listening to your testimony.

So I think there is a lot of encouraging things happening in our efforts.

The three things I hear that need to be improved upon, though, certainly is the application process. We need to really make sure that we encourage new technology and break through those bureaucratic rules and regulations that hinder the development of new technologies.

And, of course, the last thing we just talked about was the acquisition process. And I know all of you are working hard on that.

I certainly appreciate, again, you taking time to be here today. Thank you all for your testimony.

And this hearing stands adjourned. Thank you.

[Whereupon, at 12:35 p.m., the subcommittees were adjourned.]

APPENDIX

QUESTIONS FROM REPRESENTATIVE PETER KING FOR ELAINE DUKE RESPONSES

Insurance Related Questions

1. The Department's August 15, 2006 revised Application, the question is presented if insurance purchased for SAFETY Act claims can be paid for non-Safety Act claims. Would the Department approve an insurance program where the full liability limits could be exhausted by non-SAFETY Act claims? If so, what insurance funds will be used for the SAFETY Act claims?

Response: The issue of erosion of available insurance proceeds was taken into consideration when an applicant's insurance program was considered. It depended on the amount of insurance that was available relative to the likelihood of claims associated with the deployment of that technology. The Under Secretary of Science and Technology would not allow erosion in which there is a small insurance policy associated with the particular technology. If large corporate general liability policies are pledged by the sellers, the tendency had been to allow erosion of those large policies for non-SAFETY Act related claims. It is our intention to move away from erosion to single non-erodable limit.

2. In cases where the Department allows a company to self-insure for certain technologies or services, will the amount of self-insurance required be equal to the amount of insurance required? How will the Department ensure that an applicant has the financial solvency to fulfill its self-insurance commitment?

Response: In the event of self-insurance, the Department of Homeland Security weighs a number of factors, including, non-transfer of risk to an insurance company, cost of capital, financial health of the company, company assets, management, etc. We also conduct a benchmark analysis to determine the amount of insurance normally carried by similar companies selling similar products or services. Furthermore, we have subject matter experts conduct a 'risk based' analysis based upon the characteristics of the product or service utilizing a standard template developed with the assistance of the world's largest insurance broker. All of these factors are considered in setting the appropriate amount of insurance. However, the use of self-insurance is rare and never mandated.

The Department may require any company permitted to self-insure to either obtain a financial instrument to guarantee coverage (e.g., letter of credit from a bank) a pledge of assets, or a certification from the seller that it possesses sufficient assets to satisfy the insurable amount. Because of the small number of cases in which there has been self-insurance, it would be inappropriate to make broad generalizations about the methods employed to ensure that the seller is solvent. Each seller's situation is examined on a case by case basis.

The Department keeps abreast of available and affordable commercial insurance products for the smaller applicants with low revenue, but effective, anti-terrorism technologies. In these instances, the Department will also require periodic reports from the applicant concerning revenues from their SAFETY Act technology, so the Department will be able to re-visit the insurance affordability issue over time.

3. Does the Department support "self-insurance" even if there is SAFETY Act insurance available in the world market at prices that would not unreasonably distort the sales price of the approved technology? In what cases does the Department support such self-insurance?

Response: The Department will generally require applicants to acquire (or maintain in force) a contract of insurance to satisfy the insurance requirement, although the Department will entertain requests to self-insure and allow self insurance on an exceptional basis. In the event of self-insurance, the Department weighs a number of factors, including, non-transfer of risk to an insurance company, cost of capital, financial health of the company, company assets, management, etc. We also conducted a benchmark analysis to determine the amount of insurance normally

carried by similar companies selling similar products or services. Furthermore, we have subject matter experts conduct a 'risk based' analysis based upon the characteristics of the product or service utilizing a standard template developed with the assistance of the world's largest insurance broker. All of these factors are considered in setting the appropriate amount of insurance.

4. If an insurance policy only provides terrorism coverage for acts deemed to be a terrorist attack under the Terrorism Risk Insurance Act (TRIA), does that policy qualify as "sAFETY Act insurance" under the Department's interpretation of the Act; especially since the definition of an Act of Terrorism is very different between the two laws?

Response: The Department of Homeland Security's practice has been to accept a Terrorism Risk Insurance Act (TRIA)/Terrorism Risk Insurance Extension Act (TRIEA) endorsement for acts of terrorism without requiring a company to purchase additional insurance since that requirement would most likely unreasonably distort the price of the anti-terrorism technology. We are also sensitive to not require insurance coverage that is not reasonably available on the worldwide insurance markets.

The Department keeps abreast of sources of available insurance that are affordable and which will provide an adequate level of protection in the event a SAFETY Act technology is involved in a loss caused by an act of terrorism.

QUESTIONS FROM REPRESENTATIVE MIKE ROGERS (AL)

1. Can you please describe the training that procurement officials receive about the SAFETY Act? Are there plans to revise such training to reflect the recent changes? Response: The procurement community has received and will continue to receive SAFETY Act training and guidance through multiple venues, including formal briefings/training, workshops, and on-line training.

Training accomplished thus far has included:

- In 2005, Science and Technology (S&T) and the Office of the Chief Procurement Officer (OCPO) prepared and posted to the Defense Acquisition University (DAU) virtual campus web site training material that provides an overview of the SAFETY Act, including the vendor application process.
- In June 2006, in collaboration with S&T, the OCPO briefed the heads for each of the eight DHS contracting activities (HCA) on the SAFETY Act and the procedures for implementing SAFETY Act considerations into DHS procurements.
- In August 2006, S&T and OCPO issued a joint memorandum to the heads of the DHS HCAs, the component Offices of General Counsel (OGC), and the DHS Program Management Council (PMC) discussing the implementation of the SAFETY Act in acquisition planning.
- In September 2006, S&T and OCPO also briefed the DHS Program Management Council on the SAFETY Act and related processes and procedures. The Program Management Council is a component of the Program Management Center of Excellence, which works to develop the policies, procedures and other tool sets needed for DHS Program Managers to succeed.

With the final publication of the SAFETY Act program rule, and the development of a federal government-wide procurement regulation on the SAFETY Act, future training plans include:

- Familiarization training to acquaint DHS contracting professionals on the SAFETY Act in general and how and when it applies to DHS procurements.
- Development and delivery of a workshop for the purpose of developing a subject matter expert within each of the contracting Components on the SAFETY Act and its application to DHS procurements. The subject matter expert would then assist contracting professionals within each Component on evaluating the need for SAFETY Act coverage on applicable procurements and the procedures for implanting coverage.
- Development of an on-line training course that provides just-in-time training to contracting professionals as needed.

In addition to training, OCPO is currently working to further revise the Department's current acquisition planning guide, which is contained in the Homeland Security Acquisition Manual (HSAM) (a document describing DHS' internal procurement policies and procedures) to incorporate guidance and procedures on how to apply and implement the SAFETY Act to applicable procurements. Last, OCPO is preparing a source selection guide, which will also include information on the SAFETY Act.

2. What specific procurement process changes has your office made to ensure greater coordination between the SAFETY Act approval process and the procurement process?

Response: To effectively integrate SAFETY Act considerations in the procurement process, the OCPO works closely with S&T to facilitate open communication and align processes. OCPO and S&T personnel collaborated in developing a proposed FAR case to implement the SAFETY Act. They are also developing a case for revising the Homeland Security Acquisition Regulation (HSAR) to include DHS-specific policy related to SAFETY Act implementation. OCPO personnel revised the Homeland Security Acquisition Manual (HSAM) to alert both requirements and contracting personnel of the need to address SAFETY Act applicability early on in the acquisition process and document the consideration in the acquisition plan. OCPO is currently preparing an additional revision to the acquisition planning guide to provide additional procedures on how to apply and implement the SAFETY Act to applicable procurements.

3. At what point in the procurement process does the SAFETY Act become a factor? Is it at the outset of the procurement or at some other point?

Response: For those requirements potentially involving anti-terrorism technologies, SAFETY Act concerns should be addressed as soon as possible after identifying the mission need. However, absent the ability to make that identification, the requirement for SAFETY Act protections may be identified later in the process (e.g. at the solicitation or proposal phases). In order to preclude impacting the acquisition cycle time, early identification is crucial.

4. Ms. Duke, in your testimony you discuss how you will expedite the SAFETY Act process with certain procurements such as with Radiation Portal Monitors (ASP) and the Liquid Based Explosives Detection Technologies. However, the industry is concerned about all procurements, specifically if they are not particularly high profile.

- What steps can your office take to expedite the process and eliminate duplicative paperwork for all procurements?

Response: DHS remains dedicated to ensuring that consideration for SAFETY Act coverage is addressed in all appropriate procurement actions. In addition to the various educational formats envisioned, the final program rule provided a number of tools that will be used to expedite SAFETY Act processes. Among these are block designations, block certifications and the prequalification designation notice (PQDN). Use of these instruments allows contractors to submit streamlined SAFETY Act applications. Use of the streamlined SAFETY Act application results in expedited processing by the OSAI. Additionally, DHS maintains the SAFETY Act website at *https://www.safetyact.gov/,* which includes a list of technologies that have been granted "Designations" and another list of approved SAFETY Act products. These two resources can be helpful to potential offerors in developing proposals for requirements that could employ those technologies.

5. What is the method and level of communication that occurs between the procurement officials and the Office of SAFETY Act Implementation? For instance, is the communication formal such as weekly meetings or less formal? Does communication only occur at the upper management level of each component or can a procurement officer pick up the phone and have a discussion with Science and Technology about a specific technology?

Response: Project managers/requirements personnel and contracting officers are encouraged to discuss requirements for potential anti-terrorism technologies with OSAI representatives as early as possible in the acquisition process. OSAI personnel are available to assist anyone involved in the acquisition, from upper-level management to working-level requirements development personnel.

There is regular interaction between the Chief Procurement Officer and the Acting Director of the Office of SAFETY Act Implementation. Additionally, strong relationships are being built by the senior management of the Directorate. As part of assigned duties, the Director of Transition has been actively reaching out to other agencies to inform and educate them about the SAFETY Act and its possible role in their procurements.

6. What actions are being taken to develop and pursue the companion Federal Acquisition Regulation and any necessary DHS acquisition regulation or instructions? When can we expect that such regulations will be issued?

Response: As mentioned in September 2006, DHS requested that the FAR Council, composed of representatives from the General Services Administration (GSA),

National Aeronautics and Space Administration (NASA), Department of Defense (DOD) and the Office of Federal Procurement Policy (OFPP), initiate a proposed Federal Acquisition Regulation (FAR) case to establish uniform federal procurement policy implementing the SAFETY Act. The FAR Council accepted the DHS request to initiate the rulemaking case. Both OCPO and S&T personnel participated with the FAR law team in drafting a FAR case. The proposed case was sent to both FAR councils, i.e. the Defense Acquisition Regulations Council (DARC) and the Civilian Agency Acquisition Council (CAAC), for consideration on November 1, 2006. OCPO and S&T continue to be involved as the case progresses through the DARC and CAAC, by attending meetings where the case is discussed. The timeframe for taking a case from its beginning to publication depends on such factors as complexity, urgency, and whether the case is determined by OMB to be a significant case. Every effort is being made to expedite the process as much as possible. Agency-specific policy and guidance will be included in revisions to the DHS acquisition regulation and manual as appropriate.

7. The final program regulations say that all information on the program, including who has applied, will be kept confidential. While that makes sense for an individual applicant, there is no information on overall SAFETY Act activity except final actions. **While protecting proprietary information, what plans does the Department have for providing some transparency to the process? Would DHS commit to publicly reporting on a regular basis information such as the number of registrations filed and the status of such applications?**

Response: The Office of SAFETY Act Implementation (OSAI) seeks to have the process as transparent as possible to both applicants and the public. However, one of the key components in ensuring that the number of applications continues to rise is protecting applicants and their technologies. Revealing which companies have applied and the exact status of their applications would result in revealing SAFETY Act confidential information without their permission. OSAI will continue to provide program updates on the number of applicants and awards issued as the SAFETY Act program continues to grow.

OSAI is committed to ensuring the confidentiality of SAFETY Act matters. To ensure that applicant confidentiality is maintained, we have recently had the Department of Homeland Security's Office of the Inspector General (IG) perform an inspection of our computer systems used for the storage and transmission of proprietary information. The system was certified and accredited.

8. There are several references in the final rule and the revised application kit to a "streamlined" application kit, but there is no other information in the material. What is the DHS plan for a "streamlined" application process?

Response: The Department of Homeland Security has refined the SAFETY Act application kit and the application process more generally to reduce burdens and to focus more precisely on collecting the information necessary for the review of a particular anti-terrorism technology. The revised kit was posted on the SAFETY Act website (*www.safetyact.gov*) on August 21, 2006.

The Department had recognized that the initial SAFETY Act application kit was overly burdensome and the application process could be streamlined and made less bureaucratic. Utilizing an intensive internal and external 'lessons learned' process, as well as all public comments, we implemented improvements in the application kit to make it more applicant friendly; we have received positive feedback on the improvements. For example, the amount of information required has been significantly modified to remove unnecessary burdens on the applicants without compromising the needed data required by our staff and reviewers. In terms of streamlining the application kit, the Department has dramatically decreased the number of financial questions. In particular, since the program is forward looking, we have eliminated questions concerning past sales and insurance history. To better protect company confidentiality, we have removed questions that delve into cost of production and unit costs. The revised kit requests significantly less technical information from the applicants. In addition, the workflow software has been modified to make it easier to track and respond to applicant questions. The Office of SAFETY Act Implementation will continually work to improve the process.

9. What is the status of current discussions within the Federal government about whether other sellers of Anti Terrorism Technology throughout the Federal government will be eligible to apply for SAFETY Act designation and certification? Are products and services procured through DHS grants being considered for SAFETY Act coverage?

Response: All sellers of anti-terrorism technologies are eligible to apply for SAFETY Act protection. The Office of SAFETY Act Implementation (OSAI) is reaching out to other agencies, monitoring fedbizopps.gov and working with the procurement and grant officers to inform them about the benefits of SAFETY Act protection. It should be emphasized that there are no limitations on availability of SAFETY Act protections to the sellers of anti-terrorism technologies that might be associated with any government funding agreement, including grants. The Department of Homeland Security has issued internal guidance and has initiated a Federal Acquisition Regulation (FAR) case to address whether sellers of various technologies are eligible for SAFETY Act designation or certification.

Q04420: 10. Testimony from Panel II experts includes the suggestion that the duration of SAFETY Act protection once a technology receives designation or certification should be extended beyond the five to eight year time period. Is the Department currently reviewing the duration of protection and if so, what modifications to the current policy are under consideration?

Response: The qualification for SAFETY Act coverage depends on a combination of the ability of the technology to be effective in a specific threat environment, the nature and cost of available insurance, and other factors, all of which are subject to change. Since the expiration of SAFETY Act Designation and Certification would impact only future sales of the subject qualified anti-terrorism technologies (QATT), the Department of Homeland Security believes that mandatory reconsideration of technologies after five to eight years provides a fair balancing of public and private interests while providing the certainty required by Sellers. Sellers may apply for renewal up to two years prior to the expiration of their SAFETY Act Designation to provide for continuity of coverage.

The Department is cognizant of the need for a sufficient period of protection for successful SAFETY Act applicants to achieve the main goal of the Act, which is to facilitate the deployment of the needed technologies. Therefore, the Office of SAFETY Act Implementation looks for opportunities to maximize the length the awards are given, consistent with the range set forth in the Final Rule

11. Under Secretary Cohen, in September 2006 you unveiled your plan to restructure the Directorate of Science and Technology. Where does the Office of SAFETY Act Implementation fit into the proposed restructuring to ensure it receives the appropriate attention and stature?

Response: The Office of SAFETY Act Implementation has been placed under the authority of the Director of Transition, who reports directly to the Under Secretary. This has been done because the Director of Transition is responsible for the deployment of all advanced technologies. This structure provides increased visibility for the SAFETY Act. Additionally, all proposed awards are examined for consistency with the ongoing development of DHS standards by senior staff assigned to the technology testing and evaluation office.

12. The Committee has some concerns about whether the Office of SAFETY Act Implementation has sufficient resources to ensure successful implementation of the recent changes-to the rule and application kit-that will increase the efficiency and timeliness of the process.

- **When will a permanent director for the Office of Safety Act Implementation be appointed beyond the current Acting Director?**

Response: We are currently searching for a permanent director for the Office of SAFETY Act Implementation and believe we will have a person placed in that position in the near future.

- **How many additional Full Time DHS Employees do you plan to add in order to meet the expected increased demand for applications and other actions?**
- **Response:** The Science and Technology (S&T) Directorate will continue to monitor the Office of SAFETY Act Implementation (OSAI) to ensure proper Federal oversight. We intend to meet expected demand by bringing on contract staff and Federal personnel as appropriate. To that end, the Department has hired a Deputy Director for the OSAI and expects to hire an Outreach Coordinator and a permanent Director in the near term.

13. One of the overriding concerns that industry has expressed to the committee is that the SAFETY Act process has lost its focus and gotten bogged down in government bureaucracy.

- **How will the changes made in the final rule and the revised application kit support the vision of congress that the SAFETY Act protections for in-**

dustry would help bring innovative homeland security technologies very quickly to the field?

Response: The Final Rule and the new application kit are vital to improving how the SAFETY Act process works and increasing the number of technologies that are granted SAFETY Act awards. The Department of Homeland Security has done analysis of the entire process and has eliminated, consolidated, and improved the Office of SAFETY Act Implementation (OSAI) to make the process more efficient with no loss in the quality of the application reviews. OSAI has also developed consistent policies and procedures.

The Final Rule reflects the many comments and suggestions that were made while the program operated under the Interim Rule. Significant progress has been made over the last several years and the Final Rule will allow the program to be more efficient and hospitable. Of the many changes made, there are a number of key provisions that will help applicants. For example, the Final Rule establishes a program to extend certain liability SAFETY Act protections to certain anti-terrorism technologies that are still in the process of undergoing developmental testing and evaluation to validate their safety and efficacy.

The Final Rule also incorporates provisions that establish a flexible approach to align consideration of SAFETY Act applications and government procurement processes more closely. The Department will, on an on-going basis, provide guidance for effectively coordinating government procurements and consideration of SAFETY Act Applications.

In addition, the preamble to the SAFETY Act Final Rule stated that the Department would soon publish a new SAFETY Act application kit which would account for the changes contained in the Final Rule and which would state with greater specificity the information required to properly evaluate a SAFETY Act application. The Department had recognized that the initial SAFETY Act application kit was overly burdensome and the application process could be streamlined and made less bureaucratic. The Department has refined the SAFETY Act application kit and the application process more generally to reduce burdens and to focus more precisely on collecting the information necessary for the review of a particular anti-terrorism technology. The revised kit was posted on the SAFETY Act website (*www.safetyact.gov*) on August 21, 2006.

Finally, the Department recognizes that each SAFETY Act application is different. Our aim is to have an interactive and flexible application process and to focus the SAFETY Act application kit on soliciting essential information that may be supplemented as necessary with individual applicants on a case by case basis.

With the Final Rule and the new application kit in place, we are confident that the number of applicants will continue to increase along with the technologies being given liability protection.

QUESTIONS FROM REPRESENTATIVE BENNIE THOMPSON

1. According to the rule, the Department "may expedite SAFETY Act review for technologies subject to ongoing procurement processes." This applies to procurements on any level—Federal, state, or local. As part of the Committee's recent authorization, we required the Secretary "to ensure coordination of the Department's efforts to promote awareness and utilization of the litigation and risk management provisions of the SAFETY Act in the procurement of qualified anti-terrorism technologies at the Federal, State, and local levels.

- **What kind of outreach is currently underway at the Department to inform procurement officials on the state and local levels on the significance of the SAFETY Act as they consider technologies to purchase?**

Response: The DHS public website includes links to the Office of SAFETY Act Implementation (OSAI) where state and local procurement officials can obtain information related to the SAFETY Act. The OSAI web page includes links to a large amount of information describing SAFETY Act procedures as well as lists of products and services that have received SAFETY Act designation or certification. The OSAI attended many targeted conferences to let state and local officials know about the SAFETY Act. The OSAI has given workshops and presented on panels so more state and local officials can be aware of the program and work to integrate it into their own practices and procurements.

2. In this Committee's recent authorization, we required the Secretary to issue a Departmental management directive requiring appropriate coordination between Department procurement officials and the Department officials responsible for implementing the SAFETY Act in advance of any Department procurement involving a qualified anti-terrorism technology.

• **Though this legislation may not go to the floor, what efforts are underway to write and deliver such a directive?**

Response: Both OCPO and S&T are dedicated to promoting awareness and utilization of SAFETY Act protections in contracting for qualified anti-terrorism technologies. While this relationship has not been formalized in a Departmental management directive, we have developed a collegial liaison though our combined efforts in delivering briefings/training and in preparing the strawman FAR case for the FAR Council.

3. In this Committee's recent authorization, we required the Secretary to include SAFETY Act instruction for all acquisition employees and their representatives.

• **What kind of SAFETY Act procurement training is underway at the present, and what are your efforts to include such instruction in the future?**

Response: The Defense Acquisition University (DAU) virtual campus web site provides an overview of the SAFETY Act, including the vendor application process. In June 2006, in collaboration with Science and Technology (S&T), the Office of the Chief Procurement Officer (OCPO) briefed the component HCAs on the SAFETY Act and procedures for implementing SAFETY Act considerations into DHS procurements. In August 2006, S&T and OCPO issued a joint memorandum to the component HCAs, the component Offices of General Counsel (OGC), and the DHS Program Management Council (PMC) discussing the implementation of the SAFETY Act in acquisition planning. The Program Management Council is an element of the Program Management Center of Excellence, which works to develop the policies, procedures and other tool sets needed for DHS Program Managers to succeed. In September 2005 S&T and OCPO briefed the DHS Program Management Council on the SAFETY Act and related processes and procedures.

With the final publication of the SAFETY Act program rule, and the development of a federal- wide procurement regulation on the SAFETY Act, OCPO's future training plans include: general SAFETY Act training for DHS contracting professionals to acquaint them with how and when it applies to DHS procurements; workshops to develop Component SAFETY Act subject matter experts to assist contracting professionals in evaluating the need for SAFETY Act coverage; development of an online training course to provide just-in-time training to contracting professionals. In addition, to training, OCPO is currently working to revise the Department's current acquisition planning guide, which is contained in the Homeland Security Acquisition Manual (HSAM) (a document describing DHS' internal procurement policies and procedures) to incorporate guidance and procedures on how to apply and implement the SAFETY Act to applicable procurements. A source selection guide is also in process that will include a discussion of the SAFETY Act.

4. In 2005, the security company Wackenhut was granted SAFETY coverage, which at the time was the first and only such Designation and Certification for a contract security service provider. This coverage would allow Wackenhut—if its protective service plan failed during a terrorist attack—to assert affirmative defenses to liability for third-party claims. According to Wackenhut, the services it received SAFETY Act coverage for "are designed to envision and defend against possible terrorist scenarios, deny terrorists access to secured facilities, and to respond to terrorist related security breaches." Unfortunately, as you're no doubt aware, Wackenhut fell out of favor with the Department, which recently solicited a new contract for security personnel. This stemmed in part from a poorly handled situation in which Wackenhut employees failed to properly handle an anthrax-type situation. One Wackenhut guard told the press "I had never previously been given training . . . describing how to respond to a possible chemical attack." Many news outlets have reported Wackenhut's failings in securing energy plants.

• **How can the Department comfortably issue liability waivers for services that apparently are providing less than adequate coverage?** Under your recent rule, applicants must notify the Department when they make modifications to technologies that would go outside the scope of the designation or certification. **How will this work for services?**

Response: The rules and procedures are the same for technology producers and service providers. Like technology producers, service providers have a continuing obligation under the Final Rule to notify the Department of Homeland Security of any significant modification of a qualified anti-terrorism technology (QATT) that causes the QATT to no longer to be within the scope of the original Designation or Certification (See § 25.6(l) of the final rule). Also, if there is a significant change that negatively impacts the seller or the QATT, this might affect insurance coverage (i.e. insurance company may withdraw or significantly reduce coverage). As part of the seller's continuing obligations, it must report any material change in insurance cov-

erage required by the Designation. This will also be taken into account when the applicant submits its request for renewal of the QATT's Designation/Certification.

5. In July 2006, this Committee passed as part of its authorization bill a section on the SAFETY Act. Included were provisions to add additional FTEs to the SAFETY Act Office, which we understood to be lacking an adequate number of staffers.

• Can you provide us with update numbers—how many contractors and FTEs are currently employed at the SAFETY Act office? Would the authorization recommendations be sufficient to achieve your goals for SAFETY Act implementation in 2007 and beyond?

Response: Currently, there are two full-time equivalents (FTE) working as the Acting Director and the Deputy Director for the Office of SAFETY Act (OSAI). There are four contractors supporting the Federal oversight personnel. In addition, there are three senior personnel providing technical, legal, and administrative oversight. This staffing has been sufficient; however the Department of Homeland Security will continue to evaluate the need for additional staff.

6. The final regulations for information sharing state that DHS "may use information that has been submitted to the Department under the SAFETY Act."

• Who is the Department planning on sharing this information with? What regulations have been established to guard this confidential information? What efforts are underway to safeguard the interests of applicants?

Response: Protecting the privacy of sensitive applicant data is one of the Department of Homeland Security's top concerns. There is no plan to share any SAFETY Act information. The Department is committed to taking all appropriate steps to protect the proprietary information of applicants consistent with applicable Freedom of Information Act (FOIA) exemptions, the Trade Secrets Act (18 U.S.G. 1905), the Privacy Act of 1974 (5 U.S.C. §552a), and other applicable law. As an example of this commitment, those engaged in evaluating applications are required to enter into appropriate nondisclosure agreements. In addition, prior to being granted access to any proprietary information associated with an application or its evaluation, each potential evaluator is examined for potential conflict of interest. Finally, the Department's conflict of interest and confidentiality policies apply to everyone associated with SAFETY Act implementation. In addition, the SAFETY Act IT System—Technical Evaluation System for SAFETY Act (TESSA)) has been certified and accredited. Additional IT security elements have been deployed to add a greater level of protection to all applicant materials.

7. According to the recently published rule, "the Department shall establish confidentiality procedures for safeguarding, maintenance and use of information submitted to the Department under this part."

• When will the Department publish these rules and/or management directives?

Response: On August 22, 2006, the Office of SAFETY Act Implementation (OSAI) published applicable rules and procedures to implement the requirements of Department of Homeland Security, 6 CFR 25 (the Final Rule) in an OSAI Memorandum entitled: "Office of SAFETY Act Implementation Procedures for Marking, Storing and Destroying SAFETY Act Confidential Information Documents and Electronic Media". The document supplements the requirements and procedures contained in Department of Homeland Security Management Directive 11042.1 "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated January 6, 2005. The Department will continue to assess whether additional guidance is necessary.

8. According to the Department, an appeals process to challenge Safety Act determinations is unnecessary because "the interactive process [between evaluators and applicants during the application process] will provide sufficient recourse to applicants." But while the Department has accelerated the pace of approvals in the past year, the Department's rules do not include any procedural safeguards to prevent a return to a time when the Department approved only 6 technologies in sixteen months.

• Has there been any consideration given to the establishment of an administrative review process for the SAFETY Act similar to the kinds available to applicants that received denials from the EPA, FCC, or the FAR bidding process?

Response: Yes, the Office of SAFETY Act Implementation (OSAI) has developed a strict administrative review process to ensure timely consideration of all cases by the Under Secretary.

9. The final rule mentions a "rapid system for prospectively reviewing significant modifications."

• **What efforts are underway to create this system?**

Response: There is currently an expedited process in place to evaluate modifications that do not fundamentally alter the approved technology. The goal of this process is to reduce the response time by 50 percent.

○