

7 PROF. BENGT SUNDELIUS: As I said before, industry would  
8 like to be part of the answer, but a number of obstacles  
9 that make it difficult. We need to create incentive  
10 structures, understand the logics how business works in  
11 order to encourage them, facilitate for industry in  
12 various ways to contribute to the joint effort. So in a  
13 sense we continue the discussions from the previous  
14 session. We have a number of presentations now. The  
15 first one is dealing with the U.S. experience on the  
16 U.S. Safety Act, and towards the end of the session we  
17 will have a European proposal, some thinking that's  
18 going on on the European Security Label. And one of the  
19 co-authors, minds behind this, will present this. So we  
20 start with Allison Jetton at the DHS counsel, who will  
21 tell us about the U.S. Safety Act please.

22 MS. ALLISON JETTON: Thank you, Bengt, and thank you to  
23 MSB for helping sponsor this conference, and thank you  
24 very much to all of the attendees.

25 I've been very impressed by all of the thoughtful

55

1 questions and the dialogue that we've had over the last  
2 day and a half, and I really hope that by sharing the  
3 U.S. perspective in our legislation we can continue that  
4 dialogue and improve our understanding. I'm going to  
5 sort of segment my part of the panel into two parts.  
6 First directed towards companies, because the U.S.  
7 Safety Act is not limited in who can apply for  
8 protection. And, secondly, speaking more towards the  
9 government perspective, because the Safety Act is  
10 limited in who it's intended to protect. First a little  
11 of the general background. The Safety Act, or Support  
12 Antiterrorism by Fostering Effective Technologies Act of  
13 2002, was actually passed as part of the Homeland  
14 Security Act. It took us a little while to get the  
15 regulations implementing the Safety Act finalized, but  
16 we've seen really robust numbers of applications since  
17 the act came to be. Basically it's intended to foster  
18 the development and wide deployment of effective  
19 antiterrorism technologies through a dual system of risk  
20 mitigation and litigation management. It provides  
21 important liability protections for manufacturers and  
22 sellers of antiterrorism technologies, but it's  
23 important to note that the protections only apply to  
24 claims arising out of or related to an act of terrorism  
25 as defined by the act and declared by the secretary.

1 We'll get into that a little bit.

2 For industry, it's important to understand that it's  
3 really designed to remove barriers and create market  
4 incentives for the development and deployment of  
5 antiterrorism technologies. In terms of what is an  
6 antiterrorism technology under the act, it is any  
7 technology that is developed, designed, modified,  
8 procured for specifically preventing, detecting,  
9 deterring, responding to an act of terrorism or  
10 otherwise limiting the harm that such an act might  
11 cause. In terms of who is eligible to apply what kinds  
12 of technologies we look for, it's a really wide field.  
13 Products, services, software, other types of  
14 intellectual property including standards are all  
15 eligible, and it's really across all industries. Cyber  
16 security, critical infrastructure protection, blast  
17 mitigation, vulnerability assessments and other  
18 services, security services, and similar types of  
19 technologies that follow in the antiterrorism field.

20 In terms of who is eligible, the Safety Act liability  
21 protections are available to a seller as defined in the  
22 final rule which is basically anyone that sells or  
23 otherwise provides an antiterrorism technology. And the  
24 "otherwise provides" language is significant because it  
25 also means that services provided internal to an

1 organization or by quasi-governmental entities are also  
2 eligible. In terms of the types of protection, there  
3 are basically three levels, and the levels are  
4 significant because they determine the amount of legal  
5 liability protection that you get. The highest level is  
6 certification. We look at seven criteria and then three  
7 additional conditions. Basically what certification  
8 means is that this is a highly effective technology that  
9 we believe will continue to have long-term effectiveness  
10 against terrorism. It provides a statutorily created  
11 government contractor defense, which means that in the  
12 event of an act of terrorism your liability is  
13 potentially zero.

14 The next act of Safety Act protection is designation,  
15 which is an evaluation for seven criteria, technical  
16 criteria, and your liability is essentially your  
17 insurance amount. We do both a technical and an  
18 economic evaluation of the technology and the company  
19 portfolio, which helps us set cost realism based  
20 assessments of insurance. Basically an amount that  
21 would not unreasonably distort the price of the  
22 technology based on currently available terrorism risk  
23 insurance and the market value.

24 The third type of protection is a developmental test and  
25 evaluation designation, and this is specifically

1 designed for prototype technologies that haven't yet  
2 been tested operationally or perhaps we only have  
3 limited operational test data. And the goal is to  
4 further test them and gain that data so we can look at  
5 them for a full application for either designation or  
6 certification.

7 In terms of the legal provisions, it's definitely  
8 focused on kind of the American style of litigation, but  
9 it provides numerous protections, not only to the seller  
10 of the antiterrorism technology, but also to upstream  
11 manufacturers or component parts and downstream users,  
12 meaning that if for example the technology was a  
13 product, all of the pieces that go into that technology,  
14 those manufacturers could not be sued. Only the seller.  
15 And in terms of those who purchase and use that  
16 antiterrorism technology, similarly they cannot be sued.  
17 It goes back to the seller. So it provides a wide range  
18 of upstream and downstream liability with the single  
19 seller concept.

20 Also there's a cap, as I discussed a little bit earlier,  
21 with regard to the different levels. For the  
22 certification level it's the government contractor  
23 (unintelligible) which means your liability is  
24 potentially zero. For designation and developmental  
25 test and evaluation designation, your liability is

1 capped at your insurance amount. In addition there are  
2 other legal liability mitigations and litigation  
3 management strategies, such as you have an exclusive  
4 federal cause of action in federal court which means  
5 that you don't have the kind of differing judgments that  
6 happen when you sue in Arkansas instead of New York in a  
7 state court. So we expect that the body of law  
8 supporting the Safety Act, if it's ever triggered, would  
9 be much more consistent than if it were tried at state  
10 court.

11 In terms of where the Safety Act applies, the act has no  
12 geographical restriction in the statutory language which  
13 means that the Safety Act applies as far as U.S. law  
14 applies. This could include acts on foreign soil, and  
15 specifically the act includes that it may be with a  
16 domestic United States air carrier, a United States flag  
17 vessel or other type of situation in or outside the  
18 United States. In the final rule the department  
19 provides further information and that the focus of the  
20 language is on where the effects of the act of terrorism  
21 are felt, where the harm is caused. It's important to  
22 think about this especially as we continue to identify  
23 challenges with protecting our citizens against cyber  
24 terrorism because, especially in those situations,  
25 identifying the place where the attack started could be

1 quite difficult.

2 So again foreign companies are eligible to apply. We've  
3 had a number that have in fact applied and received  
4 Safety Act protections. And also that the insurance,  
5 you can certainly have foreign insurance. We want the  
6 very best technologies for U.S. citizens, and it really  
7 doesn't matter where they come from. There are no  
8 geographical restrictions in the act.

9 Switching gears a little bit to focus on some of the  
10 benefits we've seen as a government, from a policy  
11 perspective, I'd like to share with you just a number of  
12 reasons why we feel the Safety Act has been so  
13 beneficial in the United States. There are five reasons  
14 basically that other governments may wish to consider  
15 the Safety Act. And first is enhanced global and  
16 national security through increased availability of  
17 effective antiterrorism technologies. Second is an  
18 increased size of viable industry for antiterrorism.  
19 Third is improved quality of antiterrorism technologies.  
20 Four is increased market diversity, basically the  
21 different types of companies that are entering the  
22 antiterrorism market. And fifth, increased innovation  
23 and market competitiveness. And I'll discuss each one  
24 in turn.

25 First, U.S. Government policy supports technology as a

61

1 front line defense against terrorism. Our Congress  
2 wisely after September 11 looked at what we could do,  
3 anything that would better protect the American public  
4 against the consequences of an act of terrorism. And  
5 there's kind of some anecdotal stories that have been  
6 passed around, but that numerous defense contractors had  
7 these technologies that they couldn't deploy because it  
8 was either too risky; it would be a business-losing  
9 venture if you were ever sued or that the terrorism risk  
10 insurance simply was not available. And so the Safety  
11 Act was intended to address those two situations. Some  
12 might say that it was intended to be a unique solution  
13 for a uniquely American problem, but what we've seen is  
14 in the other incidents after 9/11 in other countries  
15 that litigation continues to be an increasing risk for  
16 companies with antiterrorism technologies.

17 The incentivizing effect of the U.S. Safety Act, as I  
18 said before, extends only as far as U.S. law, which is  
19 not everywhere. Further, the Safety Act is only  
20 intended to prevent harm to U.S. citizens, U.S.  
21 institutions and U.S. interests. Other governments have  
22 to consider how they will protect their citizens from  
23 harm, and the effect of other countries considering  
24 similar types of legislation or policies that similarly  
25 incentivize the deployment of these antiterrorism  
62

1 technologies could help improve the security not only  
2 for their own citizens but globally. The intent by the  
3 Safety Act is to encourage the widespread availability  
4 of effective antiterrorism technologies, and again this  
5 is in the civilian sector where the impact of an act of  
6 terrorism is likely to be most severe. Companies may  
7 not deploy antiterrorism technologies if they believe  
8 the risks are too high. And a hypothetical example  
9 would be the London Olympics. Many perceived that the  
10 likelihood of an act of terrorism might be higher and  
11 may choose not to bid on contracts for antiterrorism  
12 technologies to be deployed there simply because it  
13 would be too risky for their business. Even in these  
14 trying economic times, it doesn't make sense to bet the  
15 business on one contract. And that's the exact type of  
16 situation that the Safety Act is designed to prevent, to  
17 help encourage and protect for those types of  
18 deployments. As a result governments without Safety  
19 Act-type protection may not have the benefit of having  
20 the best, most effective, widest field of antiterrorism  
21 technologies available. This is reasons two and three,  
22 that having the Safety Act or something like it may  
23 increase the size of viable industry at the same time it  
24 increases the quality of antiterrorism technologies that  
25 are available.

1 Reason four is that the impact of the Safety Act has  
2 increased market diversity. We're not talking about  
3 benefits to just large multinational companies. In  
4 fact, the greater majority of our Safety Act awards have  
5 been to small and medium size business. This is very  
6 important because the Safety Act, in setting the  
7 insurance premiums, takes into account the total  
8 corporate profits and the revenue generated from that  
9 particular technology. When you think about a small  
10 business that's just starting up, and they may derive  
11 their sole revenue from that one technology, the cost  
12 realism approach of setting the insurance value is of  
13 huge business impact for them because it means that they  
14 may be able to enter the market when without the Safety  
15 Act they could not. So reason four, that it increases  
16 the market diversity. And again this is true for larger  
17 businesses, but the impact is greatest for small  
18 businesses.

19 Reason five is increased innovation and competitiveness.  
20 After 9/11 we saw a number companies that came forward  
21 for the first few Safety Act technology applications,  
22 and in some cases they took existing technologies and  
23 adapted them or modified them for new commercial  
24 applications and antiterrorism. What we didn't expect  
25 at the time the Safety Act was passed was kind of the

1 impact that it would have upon new technologies and on  
2 the commercial world. We've seen a number of new  
3 technologies have been developed specifically for  
4 antiterrorism after 9/11, but the private sector is  
5 starting to require Safety Act in some instances in  
6 order to bid on its contracts. This is particularly  
7 true in New York and New Jersey, which has experienced a  
8 lot of the litigation after not only the 1993 World  
9 Trade Center bombings but September 11. As greater  
10 recognition and awareness of the Safety Act increases in  
11 the private sector, companies that are vulnerable to  
12 antiterrorism or to terrorism are looking at how they  
13 can increase their security posture, and requiring  
14 Safety Act in order to bid on those contracts is  
15 becoming increasingly more common.

16 In closing, the Safety Act has been successful in  
17 achieving its aim of incentivizing the development and  
18 deployment of antiterrorism technologies. We have over  
19 250 technologies now that have been either designated or  
20 certified under the Safety Act, and the market benefits  
21 that we've seen alongside the Safety Act have been  
22 exciting to watch. These benefits aren't just unique to  
23 America. I think that they can be easily generalizable  
24 and achievable elsewhere. As we work to increase our  
25 global security, this is something that foreign

1 companies and foreign governments may wish to consider.

2 So thank you.

3 PROF. BENGT SUNDELIUS: Thank you very much for that

4 introduction. Now we welcome back Mr. Speaker.

5 Mr. Finch will join later. The persons that were

6 instrumental in shepherding this through, very

7 complicated legislation, I'm sure. Tell us your

8 thinking and your processing.

9 SPEAKER DENNIS HASTERT: Thank you very much. Again

10 it's great to be with you this morning, and if you were

11 here for the earlier session, we kind of laid out what

12 happened in 2001 after the 9/11 incident and our markets

13 were down, we couldn't do business in the United States,

14 nobody could fly. And if you're familiar with the

15 United States, you can't hardly get to one end of the

16 country to the other without use of airplanes. And so

17 we were just basically paralyzed. Our problem was how

18 do you get things back to -- how do you get the planes

19 back in the air? How do you guarantee American Airlines

20 and United Airlines that just had their plans destroyed

21 and all these pending legal cases that were piling up

22 outside their door, how do you get them incentivized or

23 give them protection to get their planes back in the

24 air? So these were problems that we had to face in the

25 Congress. And let me take you back eight years before

66

1 9/11 in February of 1991 when the first World Trade  
2 tower attack happened. The ensuing lawsuits that came  
3 out of that, the courts in New York held the terrorists  
4 33 percent liable and the landlord 68 percent liable.  
5 So when you start to think about that, who would want to  
6 be a landlord? So the incredible liability or risk that  
7 somebody took building a building or owning a building  
8 that was liable to be a focus of terrorism. If you're  
9 in downtown Manhattan or Chicago or Los Angeles or New  
10 Orleans, or wherever you happened to be, you were  
11 vulnerable to this type of liability. But the real  
12 problem happened after 9/11. Only a month after 9/11, a  
13 month and three days, to be exact, on October 15, the  
14 U.S. Capitol became the focus for an anthrax attack. So  
15 this piled on top of 9/11 said that we needed to find  
16 new innovations, new ideas, and as we were starting to  
17 put the act together to try to bring all the departments  
18 under one head and trying to unify the whole national  
19 security issue or homeland security issue, we had people  
20 coming in literally lined up outside my door saying, I  
21 have this device, I have this widget, we can detect  
22 anthrax. Well, why don't you do it. We don't want to  
23 do it because we have a liability. If for instance our  
24 product is 98 times in a hundred successful, what's the  
25 liability if it's not successful two times or doesn't  
67

1 detect that two percent? What is our liability? And we  
2 found that we couldn't get American companies to come  
3 forward with new ideas, new technologies, new R&D to  
4 protect our people. So we had to find some solution to  
5 protect those companies and entities from basically our  
6 court system. And so the Safety Act, that was the  
7 purpose of the Safety Act. That's exactly what we did.  
8 You heard the young lady giving the technical side, the  
9 lawyer's side, but on a very practical side, I guess on  
10 a politician's point of view, we did two things. First  
11 of all, we allowed people to go forward and to invent  
12 and to bring forward and to create the implements to  
13 create a safer environment, to be able to find something  
14 you put on the ceiling in a subway station so if there  
15 was some detection of a gas or anthrax or whatever it  
16 happened to be, you could find it. There was a  
17 detection. And, secondly, you started to create an  
18 environment that you not only brought these ideas  
19 forward, but those people that implemented these  
20 protections were also protected. So not only within the  
21 confines of the United States, but if you're a United  
22 States entity that has a hotel or a market overseas, you  
23 can protect yourself at least from the U.S. courts,  
24 which are probably the most -- the toughest to deal  
25 with, because you have implemented this regimen of  
68

1 either protections or devices to protect your people.  
2 If you are the NFL and have 100,000 people in a football  
3 stadium every weekend or you're the NCAA, National  
4 Collegiate Athletic Association, you have events in  
5 basketball games and football games across the country,  
6 and you're the end user or you're the person who  
7 sponsored it, it gives you some protection if you follow  
8 a certain regimen. So that's what this is all about.  
9 The tricky thing is how do you qualify, how do you  
10 interface with Homeland Security to make sure that you  
11 are qualified, that you do meet those responsibilities?  
12 And I'm going to defer to my colleague Brian Finch to  
13 talk about this issue and basically how that happens.  
14 Brian?

15 MR. BRIAN FINCH: Well, thank you and, first of all, I'd

16 like to deliver my appreciation to our hosts today for  
17 inviting us to be here. It's a real pleasure and an  
18 honor to be able to join you and address some of the  
19 very important issues confronting us, particularly  
20 incentivization to continue to persist in the security  
21 market as well as talk about the ways to manage your  
22 liability protection. I think it's also important to  
23 recognize, too, as a private sector practitioner who  
24 deals with the Department of Homeland Security, to  
25 acknowledge that the Science and Technology Directorate  
69

1 has done an excellent job over the past six years of  
2 administering the Safety Act, and thanks to people like  
3 Ms. Jetton and Undersecretary Buswell and his  
4 predecessors that they have done yeoman's work with  
5 respect to getting knowledge out with respect the Safety  
6 Act and making sure the process flows well. And if you  
7 visit the Safety Act website, you'll see some of the  
8 awards the program has won, which is a real credit to  
9 their ability to outreach to the private sector and  
10 encourage the utilization of this program.

11 As part of my role it has been to work with companies to  
12 not only educate them about the Safety Act but as well  
13 to move them through the process and help to explain it  
14 to them, because they often come to us as lawyers  
15 saying, what do we do if we come into this marketplace  
16 in order to mitigate our potential liability and better  
17 ingratiate ourselves with the security marketplace?

18 Both Ms. Jetton and Speaker Hastert indicated quite  
19 clearly that this is a liability protection process,  
20 that this is a process where if you take your product or  
21 service and you bring it forward and you run it through  
22 the Safety Act process, you will be given what is  
23 essentially a unique level of protection that is found  
24 nowhere else within federal law, which is the ability to  
25 either cap or eliminate any of your potential liability

1 following a terrorist attack. There are some similar  
2 programs that exist in courts of law and limited other  
3 examples in other territories of the federal government.  
4 The Safety Act is a very unique tool, and thanks to the  
5 foresight of Speaker Hastert and his colleagues back in  
6 2001-2002, it was a recognition that without something  
7 like this companies were not going to come forward with  
8 new technologies in order to meet and defeat the anthrax  
9 possibilities or the next wave of suicide attackers.

10 Just as importantly from the private sector, and why a  
11 lot of companies find themselves moving through the  
12 process, is that it's also a recognition that if you go  
13 through this Safety Act process, which is a fairly  
14 rigorous one -- not unduly onerous but it is rigorous,  
15 and the Department of Homeland Security does do its  
16 homework when reviewing an application -- that it sends  
17 a powerful message to the community of customers who  
18 need to acquire security technologies that by the nature  
19 of the law that this is a useful and effective  
20 technology. It in no way, mind you, represents an  
21 official endorsement from the Department of Homeland  
22 Security and never should be misconstrued as such, but  
23 at the same time if you have that Safety Act approval it  
24 sends a message to the educated customer community that  
25 this is a technology, a product or a service that has

1 been thoroughly examined by the department and is found  
2 to be in compliance with the regulation within the law  
3 which states that it must be useful and effective  
4 against terrorism. And so educated customers will look  
5 at the Safety-approved services and products and say to  
6 themselves this is something I can have confidence in  
7 that it will help defend me and the public citizens  
8 within the United States and even outside the United  
9 States against terrorism. So this may well be a wiser  
10 investment than potentially another technology. They  
11 both could work well, but I have a level of confidence  
12 associated with this product or service having been  
13 through the application process and earning the  
14 appropriate accreditation.

15 Another important point to mention, which Ms. Jetton  
16 covered in small part but I think is very important to  
17 understand particularly for European and other companies  
18 that are looking to expand their presence in the U.S.  
19 marketplace, is that when you think of the Safety Act  
20 you have to think of not only what it can do for you,  
21 but you have to think about how do my customers examine  
22 it and what do they think about it and are they aware of  
23 it. And as I just mentioned, some view it as a very  
24 powerful tool and you see that. It pops up a lot in  
25 procurements these days, but I've seen many procurements

1 where the procuring entity has said in no uncertain  
2 terms, if you are not a Safety Act-approved provider of  
3 services or products for security, you may not even  
4 submit a bid to compete in this process. And while it's  
5 certainly not widespread, it is certainly increasing.  
6 And without a doubt you're going to see that becoming  
7 more and more of a regular presence or at the very least  
8 you must apply for Safety Act protections as part of the  
9 bidding process. Potentially even being Safety Act  
10 approved. In another lane of the Department of Homeland  
11 Security, there's a law being administered known as the  
12 Chemical Facility Anti-Terrorism Standards law or CFATS.  
13 What that functionally is is that any facility in the  
14 United States that possesses or utilizes certain  
15 chemicals has to impose a wide range of security  
16 measures, from vehicle barriers to access control to  
17 inventory control, cyber security requirements, et  
18 cetera. And a lot of the facilities that are regulated  
19 by this process are very large, heavily invested  
20 companies, petrochemical, large chemical refineries, et  
21 cetera. And they're spending 20, \$30 million per  
22 facility, and they'll oftentimes have 10, 12 facilities  
23 initial in security upgrades. These are the educated  
24 customers that I was alluding to. So they look at the  
25 marketplace, and I've been speaking with a number of  
73

1 their chief security officers, and they've all said the  
2 same thing. When we look now for a new truck barrier or  
3 an interoperable communication system so our internal  
4 security services can communicate with others in  
5 addition to law enforcement, we're looking to buy only  
6 Safety Act-approved products. So this is not just a  
7 process that applies to sales to the Transportation  
8 Security Administration, Coast Guard, FEMA, et cetera.  
9 It's all customers within the United States,  
10 particularly those that are going to be buying large  
11 amounts of security equipment. And when you get into  
12 critical infrastructure, I think everybody in this room  
13 knows enough to know that's a lot of dollars being  
14 expended by the private sector, where you're going to  
15 see Safety Act coming to the forefront. And even I  
16 think one other area to mention here as well is that  
17 when we're talking about innovation, along the lines of  
18 the CFATS program, one of its potential requirements  
19 that was just announced yesterday is the use of  
20 inherently safer technologies or ISTs, and these are  
21 chemicals and other processes that pose less danger to  
22 the public should they be released into the atmosphere  
23 or they be ignited whether due to accident or terrorist  
24 activity. And these are the types of innovative  
25 products and services that scream out for Safety Act

1     protections.  For instance, we actually assisted one  
2     company that makes a fertilizer that's less detonable.  
3     And it's a product that when fuel oil is added to it or  
4     other types of accelerants are added to it, it doesn't  
5     carry the same explosive force as traditional ammonium  
6     nitrate.  And as I think people who are familiar with  
7     terrorism now, ammonium nitrate is a favorite tool of  
8     terrorists.  Well, this is a product that again was  
9     exactly what we were thinking of when it came to the  
10    Safety Act.  It's a product that carried a lot of  
11    security benefits, would help out reduce the risk to the  
12    public, and while there were some potential liabilities  
13    associated with it, the company said to itself, this is  
14    exactly what we need to use for the Safety Act because  
15    we want to manage our liability, get this great product  
16    out and encourage wider utilization.  And now, thanks in  
17    part to the Safety Act process, it is going into full  
18    production and being more widely used.  So it's a  
19    tremendous success story thanks in part to the  
20    utilization of the Safety Act.  And again I mentioned  
21    earlier the distinguishing characteristic.  One of the  
22    more widespread utilizations of the Safety Act is in the  
23    services area when it comes to security guards.  A lot  
24    of armed and unarmed security guards throughout the  
25    United States, their parent companies are Safety Act

1 approved. I see Securitas on a lot of the buildings  
2 around here. They're an example of a Safety Act-  
3 approved company within the United States. And again  
4 you're seeing their customers demand that they be Safety  
5 Act approved. It may be a little surprising to you, but  
6 in the United States large shopping centers where lots  
7 of families and young children spend their time on the  
8 weekends and evenings, most of the owners of those large  
9 shopping centers require that their security guard  
10 vendors be Safety Act approved because they know it's  
11 one of the few ways that they can manage their  
12 liability. By their very nature they're an open system,  
13 easily accessible. You can't conduct very much  
14 screening. So what you need to rely upon are guards who  
15 have a proven process for oversight, management,  
16 training, ongoing quality control. And going through  
17 the Safety Act process helps validate the fact that they  
18 in fact have those processes in place.

19 Another reason why we often see companies going through  
20 the Safety Act process as well was mentioned earlier:

21 The liability situation. I don't have a phone book in  
22 my room, but if you go to your average American hotel  
23 and you look at the back cover, you will see an  
24 advertisement for a personal injury lawyer. And that's  
25 just indicia of how litigious the United States is.

1 When there is an accident, it's obviously not my fault.  
2 It didn't matter that I was drunk and stole a bulldozer.  
3 Somehow it was the construction yard's fault, not mine,  
4 so I'm going to sue. And you see that regularly.  
5 Unfortunately, particularly following the course of  
6 terrorist events. It so happened that pre-9/11 those  
7 claims generally weren't allowed. There were a number  
8 of claims that followed the 1993 attack on the World  
9 Trade Center, the Oklahoma City bombing in 1995, where  
10 the manufacturers of the products used in the bombings  
11 were sued, saying they manufactured an inherently  
12 dangerous product. They had a responsibility to the  
13 public at large. Their product was defective and they  
14 knew it. And in those instances the court claims were  
15 dismissed, where the courts basically said, look, nobody  
16 knew that this was going to be transformed into a  
17 terrorist weapon. You didn't owe any specific duty to  
18 the plaintiffs in these cases, the victims. In part  
19 because why are you responsible for terrorists coming  
20 and taking your product, doing something to it and  
21 turning it into a weapon? That's not your  
22 responsibility, manufacturer. That's the responsibility  
23 of the terrorists. And that, dare I say, is common  
24 sense and good judgment on the parts of those courts.  
25 Well, post 9/11 that situation entirely flipped. You  
77

1 had a number of claims arising out of the 9/11 attacks  
2 against the security providers, against the airport  
3 owners, against the manufacturers of the airplanes. And  
4 they tried to assert those claims. If the U.S.  
5 government writ large couldn't envision hijackers  
6 turning airplanes into suicide weapons, why should it be  
7 the responsibility of the airframe manufacturer? Why  
8 should it be the responsibility of the building owners  
9 to anticipate such an event and to design their  
10 buildings against a low hard strike by a fuel laden  
11 airplane? Seemed like reasonable defenses, common  
12 sense. Unfortunately, common sense didn't necessarily  
13 prevail in those claims, and courts of law allowed those  
14 claims to proceed. And they said you should have known;  
15 there has been a pattern of terrorist activities. You,  
16 airframe manufacturer, should have known that a  
17 hijacking in the cockpit could lead to disastrous  
18 results. So we're going to potentially hold you liable.  
19 And that's a very dangerous precedent, and that's in  
20 part what led to Congress pushing forward the Safety Act  
21 and the aggressive utilization and implementation by the  
22 Department of Homeland Security, by the Safety Act. If  
23 you think about it from a pure numbers perspective,  
24 people who participate in the victims compensation fund  
25 that was established by the U.S. Government post-9/11

1 for families of victims of 9/11, they're getting paid on  
2 average \$2 million from the U.S. taxpayer system. If  
3 you sued the airlines, which a number of people did --  
4 some of those claims are still going forward and  
5 actually settled -- the average compensation was  
6 \$5 million per victim, so far more than double what you  
7 could expect from the government. And I think the  
8 speaker would probably agree with me here that we're not  
9 likely to see another victims' compensation fund if  
10 there should be another unfortunate terrorist event. I  
11 think the national treasury simply wouldn't support it  
12 at this point nor would there be a willingness  
13 necessarily to bail out companies who should have known  
14 better. So it's a dangerous situation, and again the  
15 speaker clearly mentioned the 1993 case where the  
16 terrorists were only held a third liable and the Port  
17 Authority of New York-New Jersey was held two thirds  
18 liable for a truck bomb that almost devastated the World  
19 Trade Center. That's the type of precedent companies  
20 are living with at this point. That's the situation  
21 they face, and that's what's encouraging the greatest  
22 utilization of the Safety Act. Finally, it's important  
23 to note there are no limitations on who can apply. And  
24 just as importantly, there are no limitations on who can  
25 take advantage of the Safety Act. Again, it's important  
79

1 to note, if you are a Swiss company selling to a Houston  
2 football franchise or to an amusement park in Florida,  
3 you can still take advantage of the Safety Act. Even if  
4 you sell or utilize the scanning technology here in  
5 Europe for cargo that's in transit to the United States,  
6 if something bad happens and there are claims made in  
7 the United States and our cargo was destroyed, lives  
8 were lost, business was interrupted, those claims can  
9 still be protected under the Safety Act so long as they  
10 are litigated under U.S. law. So it's a very broadly  
11 applied law, there's a tremendous amount of potential,  
12 and if you are looking to develop technologies, continue  
13 deployment of technologies or expand into new markets  
14 particularly related to the United States, I would urge  
15 you to take a strong look at the Safety Act, not only to  
16 protect yourself, to protect your shareholders and the  
17 future of the business, but also to give yourself an  
18 understanding of what your customers look at and what  
19 they need. Just like they want a user-friendly product  
20 that's effective, they also want to know that this  
21 product has some liability protections in place that you  
22 can take advantage of and that has been through a  
23 process that helps provide indicia of effectiveness, and  
24 that is the Safety Act. Thank you.

25 PROF. BENGT SUNDELIUS: Thank you for this information

1 about a very important piece of legislation that  
2 obviously has effects far beyond the United States. I  
3 imagine many Europeans in the room now are thinking  
4 about what are the fine print and what are the  
5 consequences for European businesses and industry. And  
6 I welcome you to formulate some questions for a little  
7 while here. Also I invite the global viewing audience  
8 to think about some questions about the consequences  
9 worldwide of the U.S. Safety Act.

10 As you heard yesterday when the ESRIIF report was  
11 presented by the chairman, it also became clear that  
12 under the auspices of the ESRIIF work some thinking had  
13 been done on a so-called European Security Label. One  
14 of the persons doing part of this thinking is Mr. Mark  
15 Miller. He will explain to us a bit about the thinking  
16 behind the European Security Label proposal.

17 MR. MARK MILLER: Thank you. Delegates, distinguished  
18 guests, ladies and gentlemen, first of all I'd like to  
19 say a thank you to Director General Lindberg for the  
20 invitation to speak and to discuss the European Security  
21 Label initiative. When I was asked to speak about the  
22 European Security Label I thought of all the efforts  
23 that have been undertaken and all of the people that  
24 have been involved in this. In fact, it's totally  
25 impossible to name all of those involved, so I'm not  
81

1 even going to begin to try. The other comment I should  
2 make very early in this discussion is that despite my  
3 American accent, I'm representing the European side on  
4 this and the European Security Label.

5 While the idea of the European Security Label may have  
6 begun earlier, clearly the steps forward and the  
7 development of the European Security Label came during  
8 the European Security Research and Innovation Forum work  
9 under Working Group 9. Under the guidance of our  
10 esteemed chairman Dr. Alois Sieber and more specifically  
11 within the Security Label subworking group led by Roger  
12 Warwick, we developed some of the early thoughts and  
13 early processes and early approach to the label.

14 Quite significantly, as was mentioned just a moment ago,  
15 the ESRIIF report itself mentions the European Security  
16 Label. And I'm going to specifically quote just very  
17 briefly from the executive summary. New initiatives and  
18 programs should include evaluating the applicability and  
19 efficacy of the numerous initiatives available to the EU  
20 and its member states such as a lead market initiative,  
21 trans-European networks for security, the creation of an  
22 internal security fund or a European Security Label.

23 However, it must be noted that we are very much in the  
24 very, very early times of the development of the label,  
25 so there are important aspects that are still to be

1 addressed. And whilst we've reached a general agreement  
2 as to what the label should be, could be and could do,  
3 we are very far from an answer as to how it can  
4 accomplish its goals. Dedicated resources, funding,  
5 research and testing are required to fully achieve this.  
6 Also it must be mentioned that third party liability is  
7 an issue that has to be addressed within this context as  
8 well. Thus during our short time together today I'm  
9 going to cover the following key issues: What is the  
10 European Security Label, why the European Security  
11 Label, what is the scope of the European Security Label,  
12 some very brief background and examples, and finally a  
13 challenge for all here in the room.

14 Please bear with me for a short time while I quote from  
15 some of the results of our Working Group No. 9  
16 innovation under ESRIIF. What is the European Security  
17 Label? The European Security Label is intended to be an  
18 instrument to facilitate and support access to the  
19 European security market, essentially serving as a  
20 common reference point for suppliers, for end users, for  
21 customers and for society to ensure confidence that the  
22 systems processes and services have gone through an  
23 approval process in a transparent, auditable and  
24 sustainable approach. One of the key points of all of  
25 this is that this common reference point enables

1 suppliers to be able to say my service, my product, my  
2 solution, my system has actually gone through a process  
3 of evaluation, a process of testing, and the result has  
4 been the awarding of a security label. This can be used  
5 as a way of being able for the company to have a unique  
6 selling proposition for its approach to the different  
7 users and customers which may be interested in that  
8 technology. Currently one of the issues in Europe is  
9 the fragmentation of the security industry. And this  
10 fragmentation essentially forces a lot of suppliers to  
11 go through a number of processes in different EU member  
12 states, and there is not one common reference point.  
13 That brings me to the point of harmonization.  
14 Harmonization itself is also a requirement within this  
15 concept. Now, again, this has not been fully developed  
16 so we are still very early in the early stages. For end  
17 users one of the key points is the claims of the  
18 manufacturer and the claims of the solution provider:  
19 Are they backed up with real test results? Currently a  
20 manufacturer can provide a data sheet, can provide many  
21 different proofs that his technology or solution or  
22 service meets the requirements of the customer. But  
23 what is the testing behind that? Therefore one of the  
24 aspects and one of the beneficiaries are the end users  
25 who can use the label as a way of saying, yes, this

1 technology has gone through a test process. It does  
2 meet the requirements for use that the manufacturer is  
3 claiming, and it does meet the specifications that the  
4 manufacturer is mentioning in the data sheet.

5 Additionally, for the citizen and society one of the  
6 points is that it can be used as a way of reassuring the  
7 citizen and informing the citizen that the security  
8 measures which have been undertaken and provided in the  
9 public environment are compliant with and use  
10 exclusively products that respect European criteria, and  
11 the European Security Label can be the mark that  
12 represents this. Also that an adequate level of  
13 recognized level of security has been established for  
14 their protection and well being.

15 Next I want to mention a bit about the scope of the  
16 European Security Label. The initial discussions that  
17 we had within the Working Group 9 defined the European  
18 Security Label as applicable to systems, processes and  
19 services with the security application either stand  
20 alone or as part of a complex integrated system. The  
21 label is not for specifically technology but rather is  
22 very much so application and task driven. Issuing the  
23 label indicates compliance of the proposed solutions  
24 with the specific task it's designed for. It also  
25 confirms respecting the 70 criteria referred to by the  
85

1 label. Now I'll go into just very briefly some  
2 background and some examples. This European security  
3 initiative has been an effort involving European  
4 industry, the European Commission, European security  
5 systems users including government agencies, European  
6 stakeholders and European Standards Organizations. As  
7 part of the efforts to define the security label, a  
8 number of different approaches have been investigated,  
9 including looking at examples of certification and of  
10 systems and solutions such as the accreditation of  
11 qualified antiterrorism technology under the Safety Act,  
12 as you have previously heard. With the 27 EU member  
13 states having different requirements and regulations for  
14 certifying equipment for use, a common approach is  
15 necessary. As I've mentioned earlier, harmonization of  
16 requirements is thus also a very important element to be  
17 considered when developing the label. Interestingly  
18 enough, there is a current European Commission FP7  
19 project which is going to be live-testing this concept.  
20 We're talking about Creative, the setup of a network of  
21 security technology and solution test centers across  
22 Europe. Please stay tuned for more information as this  
23 develops, and I can provide some discussion on this if  
24 you'd like to know more after this session.

25 And, finally, let me get to the challenges. I leave you

1 all in the room with a challenge. First for the  
2 European Commission, the European Union member states,  
3 the European Standards Organizations, the European User  
4 Organization and European industry, I challenge you to  
5 convert the European Security Label initiative into a  
6 real structure and program enabling all of the  
7 objectives mentioned previously. This also implies the  
8 allocation of specific resources and dedicated funding.  
9 I challenge you to ensure that there are benefits for  
10 the suppliers, for buyers and for end users. This  
11 requires that EU agencies and EU member states will  
12 agree starting at some point in the future to use only  
13 technologies, systems, processes and solutions that have  
14 received a European security designation. And, finally,  
15 I challenge you to commit to working with U.S. and other  
16 counterparts in developing an approach which will enable  
17 an eventual mutual recognition of certification.  
18 Second, for the U.S. Department of Homeland Security and  
19 other U.S. officials and representatives here present  
20 today, I challenge you to share openly with your  
21 European counterparts the experiences in certifying  
22 technologies, processes and systems, and solutions under  
23 the current U.S. Safety Act and within the context of  
24 its testing. I challenge you to work together with your  
25 European counterparts as early as possible in preparing  
87

1 to set up the mechanisms for future recognition of  
2 security certification, and finally I challenge you to  
3 commit fully to the process of supporting these efforts  
4 with the objective to ensure the global development of  
5 security technologies, processes, systems and solutions  
6 which can make the world a more secure place.  
7 Security is the objective for all in this room. We do  
8 want to achieve the same goals. Therefore I urge you, I  
9 urge you all, to work together and to share knowledge.  
10 The future of security for the global citizen and  
11 society lies in your hands. Thank you.

12 PROF. BENGT SUNDELIUS: Thank you very much for that

13 strong statement. Now I invite some comments or  
14 questions about these two -- one act and one proposal.  
15 And while you think about this, maybe I will address --  
16 there are microphones around. Mr. Furla (SP?), is this  
17 good for your company? What are the consequences for  
18 your company with the U.S. Safety Act? What will be the  
19 implications for your company, looking at your company  
20 now, of a security label if it came about? Is this a  
21 good thing or not such a good thing? Please.

22 AUDIENCE ANSWER: I should be very honest and answer  
23 very honestly because I really don't know. I am working  
24 very focused on the European branch of our company and  
25 my colleagues over in the U.S. are focused on U.S.

1 branch. What I heard from the discussion, it seems to  
2 be absolutely necessary to come beyond this type of  
3 total stupid suing regarding liabilities. So from my  
4 point of view I think it's a step in the right  
5 direction. Thank you.

6 PROF. BENGT SUNDELIUS: Thank you.

7 Allison, you heard the presentation about the European  
8 Security Label. Do you have any reflection and  
9 thoughts? Does it make any sense at all? You have a  
10 mic there.

11 MS. ALLISON JETTON: We have one of the most open  
12 processes, and the Office of Safety Act Implementation,  
13 which directly handles the processing of applications  
14 for the Safety Act within the Science and Technology  
15 Directorate, has a robust dialogue, and we would welcome  
16 the opportunity to share with our European colleagues  
17 how we've structured our process, how we've structured  
18 our review. And indeed with individual applicants there  
19 is a robust back and forth process about the information  
20 that we look at -- the information that's required for  
21 the technical review as well as for the economic  
22 evaluation. There are extensive frequently asked  
23 questions on our website [www.safetyact.gov](http://www.safetyact.gov). There's  
24 even a 1-888 help desk number, and you may be surprised,  
25 but they are very proactive in getting back to people.

1 Usually it's in a matter of days. So we would welcome  
2 the opportunity to share with you our experiences.

3 PROF. BENGT SUNDELIUS: Questions out there?

4 AUDIENCE QUESTION: (Unintelligible) participated in the  
5 ESRIF work on the Working Group 3, and I've been  
6 wondering about this with the European label done for  
7 security equipment and so on. Where would the actual  
8 testing take place? In Europe as a central place or in  
9 the various countries? Would there be -- what would the  
10 procedure be then? Have you any ideas about this? And  
11 what about the United States? Will you have central  
12 testing facilities or would you have the testing all  
13 around the States or how would you organize it?

14 MR. MARK MILLER: Briefly, just to respond to your  
15 question, first of all, in terms of how the approach is  
16 going to be, we haven't actually developed all of the  
17 details of the security label. We do have one example  
18 as I mentioned, the Creative project, which is actually  
19 the setup of a network of test centers to test security  
20 technology across Europe. Of course there are a lot of  
21 issues to get to this label. The harmonization of  
22 requirements across the EU member states is a very key  
23 issue that has to be addressed. Also the mutual  
24 recognition of the security label across the EU member  
25 states so that if one testing laboratory and one member

1 state does the testing, awards the label, is it  
2 recognized by all the other member states? That's  
3 another aspect that is required to be worked out.  
4 Under Creative we have a pure example because we have  
5 laboratories in Austria, we have laboratories in Sweden,  
6 we have laboratories in the Netherlands, we have  
7 laboratories in Germany, we have laboratories in France.  
8 We also have the European Commission itself, which is a  
9 member of this project, and in essence we're in the  
10 early days of testing how this would work. We're  
11 looking at common test protocols. We're looking at  
12 standardization of and harmonization of requirements.  
13 So there are a lot of steps that have to take place. Of  
14 course we have 27 member states.

15 As for the approach of the United States, I leave it to  
16 our U.S. colleagues; however I would say this. One of  
17 the parts of the European Security Label that we have  
18 very much oriented ourselves toward is to looking at how  
19 to have a mutual recognition in some way with some of  
20 the U.S. requirements. And that hasn't yet developed as  
21 we're still in early days. But that is definitely a  
22 goal and an objective of the orientation of how we  
23 develop this.

24 MS. ALLISON JETTON: In terms of the U.S. perspective,  
25 we have over 400 subject matter experts in different

1 areas that do a paper study of operational test data  
2 regarding a technology including an analysis of  
3 predicate technologies. We do not actually take the  
4 technology itself and test it. We rely upon prior  
5 operational test evaluation. We look at the results  
6 from other government agencies' testing and use. Prior  
7 government use is a criteria for designation. And we  
8 also look at statements from state, local and federal  
9 agencies on their experience using the technology.

10 Given the rigorous analysis that's done on paper, we're  
11 not anticipating moving towards an actual  
12 laboratory-based testing. But that's our experience,  
13 and certainly the European perspective will have to  
14 consider its approach to the process as well.

15 PROF. BENGT SUNDELIUS: We have a final question from  
16 the audience.

17 AUDIENCE QUESTION: Yes, George (unintelligible) from  
18 the European Commission. It's both a reaction to the  
19 challenge and also a question. Perhaps also an element  
20 of translation. We have heard these cryptic comments  
21 about the citizen being reassured by the label that the  
22 solution is compliant with requirements. From a very  
23 practical point of view, and for our American friends,  
24 what this means is, as my director was saying yesterday  
25 on behalf of Vice-President Barrot, without citizen

1 acceptability in Europe, in European markets, there will  
2 be no regulatory environment. There will be no budgets,  
3 there will be no markets, that's it. The European  
4 citizen is extremely worried about data privacy,  
5 fundamental rights requirements in solution for  
6 security. More than in other markets. It is the  
7 reality here. And basically, when we are talking about  
8 this compliance, the label giving something to the  
9 citizen, that is basically it. The label would tell the  
10 citizen this solution is compatible with the law as it  
11 stands and therefore respects data privacy requirements  
12 and others. And therefore, if you are a parliamentarian  
13 and you vote the budget allowing this solution to be  
14 widespread in Europe, you are not going to have to face  
15 political penalties for having voted this. So it's an  
16 exercise of we are extremely good in being cryptical  
17 about things in Europe, but sometimes you have actually  
18 to make it available so that our politician friends from  
19 the other side understand what we are talking about.  
20 The question on the challenge the European Commission  
21 will adopt in the coming weeks, formal communication  
22 giving its initial reply to the ESRI final report,  
23 obviously this is still being debated. From the vantage  
24 point of Vice-President Barrot and the justice home  
25 affairs side of my house, it is clear that we find the

1 European Security Label initiative to be extremely  
2 interesting. And we argue strongly for the Commission  
3 to follow the advice of ESRIIF and to look into it in a  
4 determined manner allowing the necessary scrutiny,  
5 because a lot of questions are still to be answered, as  
6 you have pointed out.

7 On the question on insurance, we do not have the  
8 marvelous litigation tradition you do have in the United  
9 States, but we do have the insurance problems. So the  
10 question is, have you already engaged with insurance  
11 industry? Have you looked at the ways of transforming  
12 the label into guarantees for access to insurance and  
13 how you can mortgage the label in other forms in sort of  
14 accelerated throughputs, facilitation systems and other  
15 ways for the industry that buys solutions that are label  
16 guaranteed to be able to somehow mortgage back that  
17 investment through, on the one hand, insurance solutions  
18 and on the other other forms of facilitation and  
19 commercial improved conditions? Thank you.

20 MR. MARK MILLER: Thank you for your explanation of the  
21 fact that this communication is going to respond to some  
22 of the challenges that I had mentioned in my discussion.  
23 And I must say that we very much support from the  
24 industry side that approach. Obviously, yes, we have  
25 talked with the insurance industry, but again it's very

1 early days. Part of the Working Group 9 work involved a  
2 number of different sessions in which we had insurance  
3 industry presentations and feedback. However, that also  
4 being said, there is also another element to all of  
5 this, which is we also see the potential for the link-up  
6 with the European Organization for Securities effort  
7 toward a third party liability limitation communication,  
8 directive, essentially to support a recommendation to  
9 move forward in such a way that not just the security  
10 label or the security certification or that approach is  
11 developed, but also so that there is some liability  
12 limitation associated with it. So from that standpoint,  
13 yes, there are -- there is a quite a bit of dialogue  
14 going on. In fact, earlier today you may have heard the  
15 CEO of the European Organization for Security, Luigi  
16 Rebuffi, mention the third party liability limitation  
17 initiative. I'm also the vice-chairman of the European  
18 Organization for Security, so I already have a direct  
19 connection with that, and in that respect we are very  
20 much so interested in developing how these two pieces  
21 can move forward together. Of course it will require a  
22 lot of effort. This is not something that's going to  
23 happen overnight. And as was mentioned, with 27 member  
24 states the harmonization requirement is also quite  
25 extensive. So in that respect I think we do have a lot

1 of potential for this, but it does require a lot of  
2 dedicated resources, a lot of dedicated funding and  
3 orientation to move forward. And I appreciate very much  
4 your comments. Thank you.

5 PROF. BENGT SUNDELIUS: Thank you all. Obviously,  
6 extremely important subject, well worth more discussion.

7 But we close the session now.