PROF. BENGT SUNDELIUS: We have three speakers and we will start with Mr. Luigi Rebuffi, who will come up. I guess you will all come up. He's representing the European organization for security industry and (unintelligible) private sector. We have Claes Erik Frolund, who will proceed, who is the vice-president of BAE Systems, vice-president of security and resilience. And we have Dr. Thomas Cellucci that we met with yesterday. So, gentlemen, have a seat here and begin with Luigi. Give the presentation on what industry can do for us.

DR. LUIGI REBUFFI: Thank you, Bengt. So, ladies and gentlemen, Mme. Lindberg, thank you for the invitation to give me the opportunity to present the view of the industry, but bring also the private sector in this trans-Atlantic dialogue that you are establishing and that we have heard yesterday there will be an agreement between the European Commission and the DHS on research and development.

From the private point of view I think that this cooperation, trans-Atlantic dialogue, should be of course extended not only at the administrative public level but also to the private level. But this is my message at the end, so let's start first from the beginning. Quickly, I would like to introduce you briefly what is the European Organization for Security.

And we have been after four years of discussion, we have created this organization, which is a company but not for profit, with a number of major European stakeholders but also some research centers, some public organizations. You see, you recognize probably in this slide a number of well-known companies which are also present here in this conference. So we are tackling different sectors of security. Not only defense, but also civil security and transport, security for transport and so on.

Our objective is to create a sustainable European security model and develop the European security market. We have spent something like two years now with this what usually are called competitors. We manage to have them around the same table working different working groups and try to develop a common view. A common view which is given in a position paper that I mentioned there, European -- EOS priority for a future European security framework -- and now we are also issuing eight white papers in the major areas which are mentioned there like borders and so on. Big message there is that you should see the research and development not like an end per se, like an objective. For industry what we want is to develop the business, provide the administration, the citizens with best possible

technology and to have the economy running properly. And that's the reason why we are proposing to the next European Commission and the new European Parliament the creation of a major European security program: Border control, civil protection, service security and the protection of critical infrastructure. This maybe sounds evident to our American friends which are already quite well organized in the Department of Homeland Security, but this is still not the case in Europe. In Europe we have a situation which is relatively, well, quite fragmented. Let me put it that way. We have issues of national sovreignty. We have different legislation and regulation and standards. We have big variety of legacy systems. The perception of threat and the perception also we have seen of privacy is very different in Europe and in different countries. I mean in the UK we saw that they have so many CCTV, but they hardly accept an ID card. In France they don't accept CCTV, and they have everybody, also like in Sweden, ID cards. So how you can move on with a common approach, let me say. So how do we define common requirement to build up, let me say, a consistent, homogeneous market and homogeneous approach to security? That's the point. So that was my point. That's the definition of common operational needs and dialogue with the user and

operator. And also we have seen that only recently in the first communication from the European Commission there is a request for the definition of an internal security strategy. So we are just at the beginning of that story, and these should give us the guidelines how to go further in the development and the deployment of solutions which are following this security strategy. It seems that we are not doing today yet what we are developing -- there's no strategy. No, actually we are following national strategy. What we would like to have is a common strategy. And on top of that of course we have the agreement for the Lisbon Treaty with possible extent of an international role of Europe and the discussion on the civil-military role and the budget which is always lacking, let me say, for this kind of development. But I would like to go very briefly on this slide. These are according to us the main drivers of the security market especially in Europe where we have an evolution of the traditional threats into high level security threats. We see also, for instance, on civilian threats which is demanding a high level of research, and research and technology. We have to develop flexible capabilities in what we call a global approach, linking different application and also end-to-end approach. We need also a better strategy

from the public decision-maker, or as we said previously we need a strategy to have appropriate investment if the threat perception is changing, is the requirement changing every year or every two-year how we can invest on research. How we can have a return on this. And also top of that we see that statistics may be not correct the figure, not exactly, but we see that we estimate that there's a factor of roughly ten between the expenditure of research in Europe and the United States, which makes a big difference. And also we have seen that in Europe discussed a lot yesterday already about the privacy issues and to increase very sensitive in Europe different countries as we said previously, different perception, but to increase the citizen trust. This means that we have to manage this intrusive national security, and this means added cost. Maybe also an added value because at the end it will be easier to sell on the market, but nevertheless high investment in the beginning. And also a message we heard yesterday also from ESRIF is that we need a global security solution with enhanced interoperability across the member states and more security and privacy by design and less added on solution. Well, I added here now this chart that you probably for sure you cannot read. This I took it from my friend Tom, and this is the product

realization chart that many of you know is already from the DHS. This is the chart where the DHS is developing, although Tom will explain much better than me, from the needs on the left to basic research to technology development and to, let me say, deployment on the right side. And why I put this here is that because in Europe with the European Commission we stop the process in the middle more or less. Don't get me to the letter. But we stop the process in the middle. We still have to build on all the phases like, for instance, mentioned there you have U.S. Safety Act, you have the certification procedure? We are still envisaging something there, but we are still far away from that. We are still a little bit -- we are just talking now about making some demonstration project, pilot project, now starting being accepted, but no more than that, and it's tough. It's tough to go to the market.

So also other issues concerning the regulation. Regulation is very important for shaping the market, but in Europe we have not sufficient guidelines from the European Commissions on a clear regulation on different areas. Even where we have regulation they are not sufficiently detailed. For instance, in the civil aviation, with the liquids and all, in general all the regulation concerning airport security, we do have

regulations since 2002, updated in 2008, but still they're very not sufficiently detailed to allow one level of investment and also homogeneous level of security across the different countries. You well know that when you go -- I don't know. Maybe when you're traveling from the States, when you visit, you go to Rome, you have to take off the belt. When you go to Paris, you have to take off the shoes. Why for that? What's the difference? It's just an example. But we have hard -- hard time to understand why there is so different treatment, different procedure and different technology sometimes used across Europe. So then also we don't have a common validation and certification of the solution and the procedure. Each country has their own accreditation system, their own certification system, but we don't have something in common. Now there is a proposal coming up from discussion in Brussels that there is a need for a European network for test and validation of innovative security and solution and services to try to help this deployment. But still we cannot have and we will hardly have in the short time some European certification, because to have an harmonization of the different countries on these topics will be quite difficult in a short time. In U.S. you have the U.S. Safety Act, which really helps you in

providing liability limitation. We do not have this in Europe. And still it's under discussion in Brussels if we do need this. Well, in EOS we have developed the suggestion. This will be tackled in the following -- well, maybe discussing the U.S. Safety Act will be tackled in the following round of speakers, but I'm sorry I have to leave very quickly after so I cannot stay in the discussion. I have to go to the ministry. But what we are suggesting, if they could be also in Europe, a limitation of liability for the technology and services, but not like in U.S. on a product basis but on an event basis. When there is a terrorist act then you apply this suggested regulation. And what you apply is not global European, but the rule -- we apply the rule where the security technology or the services are of a national accreditation. So you apply the rule of the country where have been sold according to a value limited -- the liability limited to a value given according to the security services or technology supplied. So I don't want to go more on this discussion, just to say that we have discussed this. We are proposing something, but we do think that we do need to help the result of the innovation of the research to be deployed also via this also in Europe. And what we are proposing is that we don't have to see, as I said,

at beginning research as an objective per se, but it should be part of a clear implementation of the policies, European policies driven not only by political discussion but also economic and societal needs. So we see this, the research, like in the frame of the public-private, what we call public-private end-to-end security programs that I mentioned before. End to end from policy and regulation standards, pilots, procurement, deployment and services. I mentioned before that the four security program, the four areas, the border, civil protection, the cyber security and the CIP, now we have to see the four -- these are the four major areas. Now to give some priorities and actually thinking about this, it was discussed yesterday, I changed some of my presentation overnight because I want to see this is the point in Europe. What can we do if we want to really have a cooperation between industry and the cooperation with the administration? Because it's nice to say, okay, we go for R&D, but first message we want to go beyond R&D. We want to have a dialogue of cooperation public-private with the administration, and third we have to start on priorities. We have a list of four major themes, and if I get the last slide, so first point is, okay, we could set up a kind of public-private advisory group to define this, concrete priorities for

dialogue and cooperation. But then I said, okay, maybe I could suggest something more to be provocative with you and say, okay, border control is maybe sensitive. Cyber security for sure it's common, we have common problem across the Atlantic on cyber security, but it's still difficult to define the -- profile the area and so on. So maybe there's an area where it could be maybe easier and more interesting to start to get a real dialogue and cooperation could be civil protection, the protection of the citizens, kinds of natural disasters, for instance, which is valid in the country, internal in our countries, but also abroad as we see these days with the earthquake and the tsunami in the Pacific. And on top of that also we could work on some standardization issues in a different domain we mentioned before. So this is just a suggestion to you, but I would say please, and playing with the word of industry, "thrust" with an H, please trust in industry thrust. Thank you.

PROF. BENGT SUNDELIUS: Thank you very much. Good proposals and a wish list. Now we have the vice-president for security and resilience, Claes Erik Frolund.

MR. CLAES ERIK FROLUND: Thank you very much and good morning. Mr. Rebuffi took the role as representing the whole industry of Europe and painted a big picture, so I

will take the role of a single entity of the industry struggling with the day-to-day operations including R&D questions, cash flow and what to do tomorrow. Someone yesterday mentioned the difference between the military business -- military industry arena and the civil security arena and said that the military was reasonably easy. And I can agree, I have experience from that. I also have some experiences from consumer products and business to business, and they are also reasonably easy to navigate in. In this new homeland security and civil security arena it seems to be, and it is, much more complicated. And I think the reason for that is that this is something in between the military and the consumer product. We don't have any clear doctrines. We don't have any clear standards, and we don't have any clear customers for comprehensive solutions. But I will start to give an example of -- a good example of how we could work. And this is a very specific example that started in 1999 when the BAE Systems in Sweden received a contract from the Swedish armed forces that was a contract to develop a joint operation simulation-based training tool for a peacekeeping operation. And that was the result of a memorandum of understanding between the DOD of the United States and the Swedish DOD. We received the contract, and it was to develop the system,

and it was a government-funded contract as it used to be in the military business. And we developed it, and it was used, and it was used -- and it still is used actually for ten years now every second year in the Viking exercises. This is a good example when the industry and the government in very close cooperation and interaction develop a product. When it came to the civil security we saw that there was a demand for a similar type of systems across organization, command training for crisis management, and we tried to -- we began to migrate this concept, these systems, from the military arena to the civil arena. But it was a little bit different because there was no clear funding for such immigration that it was in the military arena. So we started up with the internal funding for this project, and we also find some governmental funding within the 7th Frame Project within EU. And that was a project named COPE. COPE was a project to use cots which our minister of defense yesterday told that it was a very useful way to go, not to invent the world from the very beginning, but use what you have and integrate it. So that's what COPE project was about. It was to integrate cost product to produce a common operational picture for agencies within crisis management. And this migration from the military and civil area was based on

internal funding and governmental funding from the EU program. And everything went well and right now -- and I will present that later on in one of the breakout sessions, present this project. And we also have it in our demonstration room for anyone that is interested. But then there is a little bit of a problem because there is no clear customer for a comprehensive solution. The civil security market is extremely fragmented, and it's extremely hard to sell a comprehensive complex solution to a single fire brigade station or single police station. There needs to be some more overall approach even when it came to the customer side. And that is what I think is one of the most important issues to address, and I will address that issue to the panel and the rest of you that in the civil security arena, even if we come to very comprehensive solutions and we have a very common understanding on the R&D programs, we need funded customers for those solutions.

And I will make a statement that is of course the industry, including ourselves, are very committed, and we can and we have the capability to develop whatever is needed within the civil society to secure the world. But we need clear guidance in what direction we shall go, and I know there's a lot of work going on on the arena, but in the day-to-day business it's still quite

hard to navigate into this area. I will also address a few concerns. IP rights is a very big issue actually. When we have these multinational and multicompany research and development programs, openness is a very, very natural -- it's a must actually to get to any good results in such research projects. But on the other hand companies are competitors also, and when we came to a certain point it goes from openness to more to protect your own company's IP rights to the results. And it's nothing wrong with that because it's a part of the system. It's a part of how it works. But it is an issue that I will address that could cause some problem, and I'm quite sure that the efficiency in the R&D programs is a little bit decreased because of that question.

Cash flow is a very important day-to-day issue. And together we have quite a heavy administration and bureaucracy in the European research and development program that could cause a problem for the single entity, the single company. I'm representing a big company, but it still is a problem. And I can imagine that for small companies that this is a killer. I mean, there is no lack of ideas, but I'm sure that it's very -- must be very, very hard for a small company to take deal of these big frame programs. So that was two

small concerns that I will address to you. Thank you very much.

PROF. BENGT SUNDELIUS: Thank you very much for pointing those important problem areas.

Now, Tom, come and give us some guidance from your many years of experience at DHS and in private industry.

DR. THOMAS CELLUCCI: Good morning. As we promised yesterday, today we're going to talk in more detail about some of the things we're attempting at Homeland Security in the area of commercialization. By way of background, it didn't take literally more than two days after joining the department to find out that there were literally thousands upon thousands of private sector entities, national labs, universities, trying to push solutions onto DHS. In other words, people had solutions looking for problems. And very early on I had the opportunity to work closely with the secretary, the deputy secretary, and what we call the gang of seven, the leaders of the seven operating components. I said, now, I know I'm just this person from the private sector, but it would seem to me, because I like to keep things simple and make them easy, as I mentioned yesterday, that it would be much more effective for everyone involved, and efficient, if we took the time to write detailed requirements and then put that out to the

private sector. And a lot of the senior executives of the department said, you mean we're not doing that today? And it was very interesting to me. This -- what we're going to talk about is now used as a case study. We get invited by more business schools and government schools than you can imagine on a weekly basis. For those of you in the audience and in our internet audience, if you go to the DHS website, you will see two very detailed presentations that involve effecting change in government. And let me just tell you in a forthright manner that it's not easy, and I'll comment on that. But I think some of the issues that we just heard from my colleagues in Europe are being addressed by the commercialization model and the innovative public-private partnership programs that we've developed. I'm very proud to say they were developed in science and technology, but they are now being mandated not only through the Department of Homeland Security, but I now work with President Obama's chief technology officer to talk about how this could be spread across the federal government in the United States.

So to continue with the story, I also, as my friend just commented, was dealing with a lot of frustration from the private sector who said, we don't need your money. We just want to know exactly what you want and what are

the opportunities. So basically commercialization started out with a simple premise, that the private sector would be ready, willing and able to assist the department if we gave them two things. Neither of them were money. The first were detailed operational requirements. Now, we talked yesterday about what I would call high level requirements in a requirements hierarchy, which are generated from the capstone integrated product teams. And those were capability gaps. But if you've really dealt with requirements, these tend to be very broad. Detailed operation requirements tend to be things that take some time to develop. If you look on our website you'll see that our typical operational requirements documents are 40 to 50 pages in length, compared to capability gaps which may be a sentence or two long. And basically, if one really wants to develop a product or a service, many people will argue, and I think quite effectively, that you need these detailed requirements. So the first thing we needed to do is to develop the capability within DHS to articulate our detailed needs. That is to say, to articulate detailed requirements. The second thing that would be of value to the private sector would be a conservative estimate of the potential available market. As we said yesterday, it's been my experience that the

majority of applications for the Department of Homeland Security are for widely distributed products. We talked about the three major stakeholders for DHS: The operating components which are funded; the large base of first responders, who by the way get funding from FEMA, about 3 billion U.S. a year; and the critical infrastructure key resource owners and operators within the private sectors, 18 sectors that comprise the economy. So by offering both pieces of information the private sector would have the information it needed to make a business case. And basically what we found is that indeed the private sector, and as you'll learn even the university community's national labs, very much want to help, and they'll do it with their own resources to share in the imprimatur of the DHS, as you'll see, as well as being able to look at medium and long-term opportunities. So I'd like to give you a brief overview of commercialization, talk about the initiatives at DHS in a case study format, and hopefully you can see what we have learned so far in this experiment.

The commercialization office is involved in four primary activities. The first is a requirements development initiative. I did not come to the department to write the five books we have in the last year, and I wouldn't have believed that unless I lived there, but we did need

to learn a lot about defining, generating and vetting detailed operational requirements. You know, I thought everyone was Italian at DHS like me, because when I would ask people what do you mean by interoperability, they would do this (gesturing). What do you mean by situation analysis? Depending who you talked to on what day of the week, you would not get a similar answer. And we'll talk a little bit about that because this involves the need to measure things and to look at performance measurements, and I learned a long time ago, if you can't measure it, you can't manage it. And as I mentioned yesterday, not an excuse for the Department of Homeland Security, but just an observation: It's a young organization. It just celebrated its sixth anniversary. And just like when a child is starting primary school, things get a little harder. We expect the child to go home with homework and do it, et cetera. Well, this is what is happening at DHS. We developed a commercialization process and, simply stated, I loved what the Minister of Defense for Sweden said yesterday. He said sometimes the answer is right in front of you. And it was so clear to us at Homeland Security that when you talk about widely distributed products, that begs the discussion for commercialization versus the acquisition model that is typically used in the

Department of Defense, used by other government agencies. The acquisition model is quite useful when you're building one-off custom systems. And we all can agree the total potential available market in terms of units of any given year of an aircraft carrier is quite small. In that case government needs to pay the private sector to divert its valuable resources to make that one-off custom product. But when you're talking about thousands, if not millions, of potential units across all of these stakeholders, this gets the private sector excited. And it is true that it's fragmented, but we have now built segmentation maps to guide the private sector to help them navigate the waters, which we'll talk about. How do you take these commercialization models and make them real? This is through our innovative public-private partnerships. And finally we do global private sector outreach, which has been quite successful. There has been a lot of attention paid to commercialization, as I mentioned. It is working. Of the eight detailed operational requirements that we have now on our website, there are 43 companies building products and services for DHS at no cost to DHS. This saves the taxpayer money. It creates a speed of execution for the department. And it makes the private sector happy. And, again, I learned a long time ago, if

all participants in a program or a model or a system have the benefit to succeed, the probability of success goes up rampantly and rapidly. This is a typical chart that you don't see in government. This is what you call a market potential template, and what you can see is that if we segment DHS into the seven operating components, further segment into major applications and put dollar signs and unit symbols next to these, we can build potential market maps. And this is exactly what we do. And as I said, one of the largest stakeholders for DHS is the seven operating components: TSA, Customs/Border Protection, the Secret Service, Coast Guard, et cetera. We've added science and technology because we buy prototypes, et cetera, and then we put in a catch-all other category, but realize that we are conduits from a marketing standpoint to the first responder community through FEMA, through nongovernmental markets through the office of infrastructure protection. We talked about the 18 sectors comprising our economy. And just as an example, this is a market segmentation of the first responder community, so it is fragmented, but you have to understand the fragments. And some of these fragments alone are very enticing to the private sector because they can be quite large. So these are the major

segments and subsegments of what we call the first responder community.

Not to make you dizzy, but to make a point, these are the sectors comprising the key infrastructure and key resource owners and operators. So there are the 18 sectors and the major segments within those sectors. When you build these market maps you will see quite readily that the numbers get large. This is very exciting. So I'm very proud to say that the private sector has not been positive, they've been ecstatic about coming to us. Our issue today at DHS is we have so many people waiting to see more detailed operation requirements being added. We currently have 40 more detailed operation requirements that are being generated and vetted. As I said, the first eight, we have 43 companies now developing products and services for the department.

So the idea, to use the word of the Minister of Defense, is right in front of you. Keep it simple. Make it easy. So we publish in an open and transparent way solution-agnostic detailed requirements with potential available market. We say to the private sector, you are solution providers. You provide solutions from what we consider technology readiness levels five or above, which Luigi showed in the product realization chart.

And we will sign -- let me repeat this -- we will sign a one-page agreement that our lawyers have developed. I always have to thank the Office of General Counsel. It doesn't need to be a 5,000 page document. And in that way this cooperative research and development agreement allows us to work with the private sector or other entities to develop products and services and technologies as you'll see. And this increases the speed of execution. This increases the net realizable budget for the Department of Homeland Security. And another interesting story, Secretary Napolitano talks about three operational thrusts, what I would call operational thrusts for the department. And I very much agree with those thrusts. They're efficiency, partnership, and one DHS. And I think you'll see, when I briefly describe these public-private partnerships, that these are good examples of all three of those operational thrusts. And for those of you in the private sector, I had the opportunity as I said many times to interact with the secretary, the deputy secretary, and I asked a question of them. I said, I have come from a world where it's not only good enough to execute, but the speed of execution is critical. Where would speed of execution be more important than protecting the citizens of our country and the property

of our country? That was what not only let them support these programs; they embraced them. So the Secure program is a certification program as I described. We put out detailed operational requirements, conservative estimate of the market, and we get back in most cases many, many potential solutions from the private sector. This is not a procurement activity. We create a clearing house, and every ORD has many solution providers. This is organized at the discretion of the program manager, and as I said, in the next year there will be probably around 43 products released from the department based on just eight ORDs. And as President Obama recently said in a speech to the Congress, he said, show me a program where there's competition and choice, and I'll show you effectiveness. And this is precisely what we're doing. And why would the private sector be interested? We're trying to make it easy. We're trying to keep it simple. We then certify their product or service. They actually get a seal as you see here, which let's them share in the imprimatur. As I mentioned yesterday, I've been a first responder for over 30 years. A lot of junk has been sold to first responders. They need the assurance that the product works or the service works. This is worth gold, as we would say in the United States, to the companies who are

involved.

Now, of course when you have successful programs the first things that happen are people say, well, what about us? And this happened with the university community, and a lot of people have asked the question, how can we help if we're working on research? We are not interested, we do not have the core competency, to commercialize products. The good news is is we have developed a program which we want to share with you called Future Tech. The idea here, it's analogous, it's the sister program to Secure. Where Secure has as its ultimate objective to deliver products and services to meet the detailed needs of the DHS stakeholders, the Future Tech program is targeted towards the university community, the national labs where we will certify a technology at technology readiness level six. This is what I would call the sweet spot for technology that could be ultimately transferred or transitioned to one of the operating components or to the public sector. And, again, you share in the imprimatur, it makes an entity's technology much more valuable on the open market.

So these are two public-private partnerships. Why are they working? They're working because, as I said, every participant wins. The taxpayer wins, the private sector

wins, and the public sector wins. Now, change is not easy. Just ask President Obama. And I was a change agent before that became popular in the United States. People often ask me, what's the biggest challenge in doing commercialization in the federal government? The biggest challenge is analogous to losing weight. If you've ever tried to lose weight, the hardest part is the middle. And so getting the not only support but embracement of these kinds of programs from the senior executives of government actually was quite easy, because you can't argue with things that are good for the taxpayers, the public sector, the private sector. But there's differences in culture, and many people in government have spent their whole careers in building large groups of people and money, and it's counterintuitive to them to right away embrace something like this. The good news is that you can change things. It takes time, but that's been our experience, that the challenge is not working with the universities, the national labs or the private sector. It's working internally to create a commercialization mind set in government. The cultures are different. One is not better than the other. In the private sector, which is geared to more financial, results oriented, speed of execution processes, versus the government which in many

cases is much more difficult. In many cases it's much easier in the private sector to prioritize programs and projects because it's mainly based on financial factors. In the government there are other factors that are involved. So that has been the challenge. The good news is it's happening. It will not happen overnight, but the reality is, as I said, we now have 50 or so ORDs that we've generated and now are vetting throughout the process. And so there is hope, and as I said we're working to look at how this can be spread.

There are undoubtedly cross-cutting requirements that the Department of Defense, Department of Homeland Security, the Department of Energy can look at together. And in fact we are starting to use technology. Those of you familiar with what people call Web 3.0 or the Semantic Web think about a day when we can actually put the framework of detailed requirements in an open and transparent way to let the private sector, the venture capital, the angel community and potential users build it up to build a solution-agnostic ORD with millions of people interacting on it so that you can get all that positive input. The internet was used quite successfully in the recent elections campaign cycles to generate money, ideas, et cetera. Why not do this for a global community to develop the future detailed

operational requirements? With that I'd like to thank you for your attention and just also mention that all of these materials are available on the DHS website. Thank you.

PROF. BENGT SUNDELIUS: Thank you all for your excellent input.