

15 PROF. BENGT SUNDELIUS: Dr. Walker is Director of
16 Research with DHS responsible for setting direction,
17 setting priorities for the various division heads, and
18 we will get for the next hour and a half or so a
19 run-through of the DHS scientific divisions. I'll let
20 you moderate this, and I know you will do it well.
21 Starnes Walker.

22 DR. STARNES WALKER: Thank you, Bengt.
23 Well, I'd like to invite our DHS division heads up.
24 We're going to spend the time ahead describing the
25 portfolios that each of the division heads manage, and

112

1 one of the things that you will see as they describe
2 their efforts is that the focus is established to be
3 very strategic and enduring, as viewed from our
4 customers' perspective and from the first responder
5 community. So the areas that I'm going to be asking
6 them to discuss will be kind of along three central
7 themes: One would be what type of challenge or
8 challenges do they view as being something most
9 outstanding in their portfolio. It gives you a sense of
10 where science, technology, interoperability
11 all interplay, because again the focus of these
12 strategic enduring areas are such that we can see where
13 the adaptation of discovery into operation makes sense.
14 The second area is then to take maybe some discussion in
15 terms of the technologies and the advancements of how it
16 looks across the international community, because we
17 have a large forum here today with academia, industry
18 and government from Europe, the Baltic area, so that
19 we're able to kind of describe things that will make
20 sense or what would be natural resonances for you to
21 engage in our partnership.

22 And then, thirdly, the areas where what will be the
23 things that will be a take-away for this audience today.
24 So I think we'll certainly start with Dr. Beth George
25 who runs our chem/bio division. Beth?

1 DR. ELIZABETH GEORGE: Hi. Thank you, Starnes. The

2 biggest challenge we have in chemical and biological
3 defense is detecting the attack before it happens, so we
4 have focused our resources on responding to the attack
5 or being able to detect the attack after it happens and
6 then developing strategies then to counter the attack.
7 We very much would like to move to the before-bang kind
8 of scenario where we can actually keep an attack from
9 occurring. So I believe that's the answer to your first
10 question.

11 Now I'll talk to you a little bit about what we do in
12 the chemical and biological division. We focus our
13 resources on developing countermeasures, and
14 countermeasures can be technology or con ops, guidance
15 documents, that kind of thing. We develop
16 countermeasures against chemical and biological attacks
17 on our people, our infrastructure and our food supply.
18 Primarily our agriculture in the animal area. We work
19 in areas such as threat assessment, surveillance and
20 detection, forensic support for attribution and response
21 and recovery.

22 So now let me tell you just a little bit about what we
23 have done and what we're doing in each of those areas.
24 In terms of threat assessment -- and threat assessment
25 in this case is terrorism threat and risk assessment --

1 we use that to help prioritize our resources. Because,
2 as all of you know, we have a limited amount of
3 resources and we have to maximize our investment. We
4 have delivered a chemical terrorism risk assessment,
5 biological terrorism risk assessments and just last year
6 we delivered our integrated chem/bio radiological and
7 nuclear risk assessment, which essentially incorporated
8 all the information on all of the threats and put them
9 on the same scale so we could do direct comparisons
10 among the four threat agent categories. We also work in
11 surveillance and detection. In chemical surveillance
12 and detection we have deployed the Protect system which
13 is a chemical detection and response capability that is
14 in various transportation hubs around the country.
15 We're now working on our next generation chemical
16 detection systems for facilities, as well as handheld
17 tools for responders. These are very challenging
18 systems, the ones for responders, because they not only
19 detect an array of chemicals; they do it at acute
20 exposure limits as well as permissive exposure limits.
21 So they have a wide range of detection capability.
22 As we move into our next generation of chemical
23 detection devices, they will have lower false positives
24 and see multiple classes of agents very rapidly at these
25 wide detection ranges.

1 In terms of biodetection, we employed the biowatch
2 environmental monitoring system in 2003, and that is
3 considered the gen 1 of the system. That particular
4 system has a 12-to-36-hour time lag before detection,
5 but it's been deployed to a goodly number of urban areas
6 and provides protection or provides detection with a
7 high confidence for a larger attack, where our gen 2
8 system is essentially the same system put into
9 transportation facilities, and we're now finishing up
10 development of our gen 3 system which provides a
11 detection response in four hours and at a higher
12 sensitivity so that we can get a greater network and
13 provide protection across a greater area.

14 Our next generation system will be one hopefully -- and
15 I know people will laugh in the audience -- but one that
16 detects something that makes U.S. sick because now we
17 are targeting our detection capability, and with
18 emerging and advanced and engineered threats, it opens
19 up the space, the detection window, much larger. So we
20 need to be prepared to deal with that. In our forensics
21 area we have both chemical and biological forensics, and
22 the research area primarily looks at signatures or
23 fingerprints of a biological agent or chemical agent or
24 its precursors that one can then draw a correlation
25 between a particular piece of evidence and a crime scene

1 or a crime scene and a perpetrator. And we're not only
2 looking at fingerprints or signatures of the agent, but
3 we're also doing analysis to understand matrix effects
4 as well. So we do physical and chemical analysis of the
5 matrix.

6 Finally, in the response and restoration or restoration
7 and recovery area, we are working to develop
8 preparation, guidance and response documents for our
9 local facility owners and emergency responders in public
10 health that help them preposition and preplan the
11 materials they need to clean up a facility, a
12 transportation facility in this case, as rapidly as
13 possible. We have developed guidance for an airport for
14 biological. We're working on the guidance for the
15 chemical attack on an airport. And at the federal
16 level, at the national level we recently delivered in
17 the federal register an overarching framework for
18 biological cleanup, so we have made some advances there,
19 but we still need to be able to quickly restore an area
20 to get it back in use so that we don't completely shut
21 down our economy.

22 So I think I've answered your second question, Starnes,
23 and one of the things I'd like to leave you with are
24 four take-home messages. First is that we need
25 scientific risk assessments to help U.S. prioritize our

1 work. I just wanted to repeat that. I know I've
2 already said it. Another point is airline detection
3 saves lives. We've spent a lot of our effort looking at
4 detection, environmental detection, but we need to have
5 a national overarching biodefense architecture that not
6 only looks at biodetection but brings in the public
7 health information, the veterinary information, and
8 matrixes it across local, state and federal government
9 and the private sectors. And so this is an area that in
10 our country we need to make investment in, and I can see
11 how it would be an international effort that would be
12 tailorable to a particular country, based on what their
13 structure is.

14 I talked about response and recovery. Rapid recovery is
15 necessary to minimize economic impact. It's probably
16 the hardest part of the problem because we don't have
17 good standards for cleanup, but we have to take a
18 risk-informed optimization approach to quickly restore
19 an area, bring it back up to use. That area needs quite
20 a bit of scientific advancement before I feel like we've
21 finished.

22 Finally, international collaboration is key to achieve
23 this chemical and biosecurity that we need. I brought
24 the ESRIIF, European Security Research and Information
25 Forum, summary up here with me primarily because I see

1 recurring themes in all our work, and it's clear to me
2 that we're all working toward a lot of the same goals:
3 Preparing, responding and recovering, the countering
4 different means of attack. It talks about the
5 nonconventional attacks for emerging and advanced
6 engineered threats -- again, areas that we're very
7 interested. Finally, the securing critical assets, the
8 Director General of enterprise and industry talked about
9 the very large impact shutting down a subway system
10 would have, for example. We're investing there, you're
11 investing there. We need to invest together and we need
12 to not only include the European Union and the United
13 States in our discussions but also our other colleagues
14 such as the ones in Canada and in Australia, who also
15 actively invest in these areas. So thank you very much.

16 DR. STARNES WALKER: Just one quick question, Beth. In
17 terms of we've heard today the importance of policy
18 along with science and technology. And you talked about
19 the sharing of information databases and things like
20 this. Do you also see a role in terms of policy helping
21 U.S. to advise better on the sharing of personal
22 information, when it comes to medical information and
23 things like this, which is always an issue? Because you
24 want to have advanced warning of things evolving, how
25 much can you share? Would you say a few words about the

1 role of policy as well.

2 DR. ELIZABETH GEORGE: Well, obviously policy is a very
3 important factor as one's developing road maps perhaps
4 for an R&D program. But policy also is very government
5 specific. And so we need to get together more as an
6 international community and talk about what makes sense
7 in my case for chemical and biological security and then
8 help inform our policy makers on what those
9 conversations and those consensus decisions were. When
10 it comes to sharing something like medical information,
11 that really is not in the bailiwick of my division.
12 It's more of a health and human services issue. But
13 there are ways that one can strip personal information
14 off of data and share that information or could roll up
15 that information into a more -- a higher level and then
16 share that information. So there are ways to get around
17 that, but one has to be very careful to secure the
18 privacy of individuals' information.

19 DR. STARNES WALKER: Of course we all come down to a
20 risk-informed decision-making as being so important in
21 chemical and biological in how we approach things. It
22 also impacts how we make investments in science and
23 technology, because we have limited amount of resources
24 in each of our countries that go into science and
25 technology. So it behooves U.S. to have sharing and

120

1 collaboration on science and technology, but also to
2 address the things that we are most concerned about and
3 get a consensus as an international forum. Thank you,
4 Beth. Okay.

5 Chris Doyle is head of our infrastructure geophysical
6 division, and we've heard a lot again today about the
7 importance of critical infrastructure, the resiliency of
8 society and how we can have enhanced consequence
9 management recovery, and a lot of this fits squarely
10 onto Chris's portfolio. So I think you'll be very
11 pleased to hear about some of his thoughts following
12 this.

13 MR. CHRIS DOYLE: Okay, thank you, Starnes.

14 First I'd like to thank my friends from the Swedish
15 Fortifications Agency for this wonderful red tie they
16 supplied me with before I came up today. I appreciate
17 that. Actually, many of you have probably seen them
18 already around the conference, but they say CIP at the
19 bottom, which of course can only stand for critical
20 infrastructure protection, to a civil engineer at least.
21 But I'm glad to be here to talk about what keeps me up
22 at night. There are lots of things that keep me up at
23 night, but none probably more important than the subject
24 we're here to talk about today, and I can tell you that
25 in my world where I'm dealing with infrastructure

1 protection and emergency preparedness and response, the
2 thought of an event that could have vast geographical
3 impacts and affect multiple critical infrastructure
4 assets and lots and lots of people in one way or another
5 is really I think what keeps me awake at night and kind
6 of drives my R&D agenda. And it certainly keeps my
7 customers inside the Department of Homeland Security up
8 at night, and I think they do a good job of dealing with
9 it on a day-to-day basis. But our role is to develop
10 technologies to help them get a little bit more sleep.
11 So on the preparedness and response side, I think you
12 have to look at it from a couple of standpoints, and
13 we've heard a little bit of discussion about this this
14 morning. Certainly the Defense Minister was talking
15 about this as well. And that's how you're able to share
16 information, because I think one of the keys to a
17 successful response, and again talking about a large
18 geographical area where you're involving multiple
19 jurisdictions or multiple agencies at various levels of
20 government, one of the critical aspects or features that
21 you're looking for is the ability to share information
22 seamlessly. And we've been spending a great deal of
23 time on that over the past several years, and it's a
24 very tough problem to address, particularly where you're
25 looking at potentially in the United States we're

1 talking about 38,000 separate jurisdictions and many of
2 them are using their own proprietary software
3 applications that we then are trying to find a common
4 ground, a standard, if you will, that will allow for
5 this seamless exchange of data at the emergency
6 operations center, from the state to the local level,
7 from the state to the federal level. And that is a
8 tough, tough problem to try to address. I'm going to
9 deal with one microcosm of that, which is logistics and
10 trying to allocate resources across very broad areas.
11 There are lots of private vendors that are very anxious
12 to get engaged in the disaster response, and we saw
13 this -- really in every hurricane season we see this
14 with big corporations in the United States like Wal-Mart
15 and Home Depot where -- to name just a few. They're
16 willing to supply U.S. with information about their
17 inventories so that the federal government, the state
18 government have situational awareness, they have
19 transparency and understand where various types of
20 materials are located for distribution. However, right
21 now the level of sophistication for exchanging that
22 information involves printing it out and faxing it back
23 and forth to one another. So one of the areas that
24 we're looking at is using this overall standardization
25 of data exchanges to account for that. And one of the

1 other peculiarities when you're dealing with Wal-Mart or
2 Home Depot or the UPS, Brown, you all may have seen the
3 commercials, I don't know, maybe it's just a U.S. thing.
4 I guess it is, judging from the reaction. It's not.
5 But, you know, all of these private corporations have
6 proprietary packages that they use for allocating their
7 own resources, and the last thing that they want to do
8 is pry them open and allow the federal government to
9 take a look at how their code was put together, because,
10 frankly, there's just not a high level of confidence in
11 the U.S. that the government can take care of and
12 protect that information. That's why personally
13 identifiable information is such a big deal in the
14 United States. But, by seeking a standard through which
15 this data can be exchanged, we think we can get around
16 that issue and still provide a workable solution. And
17 right now we have one that we think is about 35 to
18 40 percent effective right now, and we're continuing to
19 pursue that. So from an incident management standpoint,
20 I think being able to manage people and resources across
21 multiple jurisdictions, but also providing tools that
22 are going to protect responders, because what we're
23 really interested in is protecting people, and that
24 includes the people who are going in to save other
25 people. So we spend a lot of time developing

1 technologies that are going to help responders be safer
2 with what they do and more effective with what they do.
3 And I think one of the flag ship programs that I'm proud
4 to have in my portfolio we call a three-dimensional
5 locator or tracker for firefighters, and I'm sure many
6 of you are aware that GPS is denied inside of a
7 structure. You lose it at the front door of a building.
8 So our hope is to develop a solution that is going to
9 work in three dimensions, provide that altitude, and
10 work in skyscrapers in an urban environment where you
11 have lots of steel reinforcement in concrete or you have
12 lots of iron that's been welded or riveted to build the
13 frame of the building itself, and lots of glass. So all
14 these things can contribute to obstructing transmission
15 of signal. So we're working on developing a solution
16 that's going to get around that. We actually have a
17 prototype that's good to about three meters or so
18 already that we're continuing to refine. I think I can
19 say that the three meters is repeatable approximately
20 50 percent of the time or so. And the program manager
21 is actually here with me this week. Jalal Mapar is
22 somewhere out there. These lights are pretty bright so
23 I can't see where he is, but I brought him with me to
24 talk more to our international friends about that
25 particular product and a few of the other training

1 things that we're working on.

2 One last program that I wanted to raise with respect to

3 incident management is a real-time data transmission

4 from aircraft. Surveillance, obviously one of the

5 biggest issues that the European community is dealing

6 with, same with the United States. You might hear more

7 about that from Anh Duong, but certainly from an

8 incident management standpoint and from an

9 infrastructure protection standpoint, we're very

10 interested in surveillance technologies and,

11 particularly following a disaster event, being able to

12 capture the imagery, do some kind of an analysis of what

13 the changes in that area are and get them back to

14 decision-makers as quickly as possible has been a very

15 difficult task to achieve for lots of different reasons.

16 But we have worked a project that we demonstrated about

17 two months ago where we have real-time transmission of

18 that data, of that process data to a ground station

19 using microwave technology. So we're continuing to work

20 on those things. We've not gotten all the way there in

21 terms of incident management, but I think going back to

22 resilience -- and a lot of people think in terms of

23 people's resilience to bounce back from events or a

24 facility's resilience to deal with an event, but I think

25 you also need to think in terms of resilience of

1 operations and particularly resilience of response. And
2 technology is a key instrument in effecting that kind of
3 resilience and response.

4 I'll talk about critical infrastructure protection very
5 quickly. I've probably run out of time already, but I
6 just want to impart one thing about infrastructure
7 protection that is key to resilience from my standpoint,
8 and that is materials science. I think that -- and I
9 guess I'll kind of combine this with the last question
10 that you had, Starnes, which was take-aways for this
11 crowd, and that is that I think materials science is
12 really the next frontier for infrastructure protection.

13 The big problem that we're dealing with from an
14 engineering standpoint right now is the existing
15 building stock and the historic fabric associated with
16 much of it. Nowhere is that more prevalent than right
17 here in Europe. We think of old as 200 years or so in
18 the United States. I know that's just an infant over
19 here in Europe. But there's tremendous existing
20 inventory of building stock that needs to be protected,
21 and advanced materials are the way to go because we're
22 never going to move these buildings, we're never going
23 to achieve standoff, we're never going to effect
24 building codes, at least not in the United States, to
25 recognize terrorism restrictions and be prescriptive

1 against terrorist attacks. So I think that we need to
2 come up with the materials and provide the information
3 to the building designers, the architects and the
4 engineers, so that they can make the decisions on behalf
5 of their clients, the building owners, to make
6 responsible investments in materials to provide this
7 infrastructure protection.

8 DR. STARNES WALKER: I would make one comment that many
9 in the audience I think would appreciate is that much of
10 the advances we have in society, hundreds of years, has
11 been our understanding of how materials behave in
12 extreme environments -- the physical, the optical, the
13 electronic properties. And I think as Chris has pointed
14 out, as we make advances in materials science and how it
15 ties to resiliency and how to enhance the ability to
16 withstand either a natural disaster or a man-made
17 disaster is really important. So the breakthroughs that
18 are made through Europe, in the Baltic area here and
19 these will have great adaptation to enhancing homeland
20 security, national security interests.

21 The other, just a question: What's the role of test
22 beds and exercises in looking at the seams of
23 vulnerabilities relative to consequence management
24 recovery? Could you just say a few words, because I
25 think that's something that we saw in the last video

1 that was very important in terms of how everything
2 worked, but you also want to exercise that to find out
3 where those vulnerabilities are so that you develop
4 programs to address those.

5 MR. CHRIS DOYLE: Yeah, I think testing and exercising
6 your plans and your ability to respond is a critical
7 feature, and we do that incessantly in the department.
8 We have national level exercises that we conduct within
9 the department that are government wide and also go down
10 to state and local level. And there are also
11 requirements at the state and local level to conduct
12 periodic exercises of their plans for response to ensure
13 that they have all of the right parts in place. In
14 fact, those exercises they conduct locally and at the
15 state level are required in order for them to receive
16 grant funding to carry those out. So our technology
17 part of that is that we watch very closely because we
18 are also building technology enablers, if you will, to
19 help with that training and that simulation, and
20 understanding that the more people that you can get
21 involved in these exercises and the more realistic you
22 can make it, all of these things only go to enhancing
23 the virtual experience of the exercise, if you will, and
24 making it seem realistic and being able to capture data
25 about the decisions that were made by the incident

1 commanders, by the mayors, et cetera. One of the things
2 that we're striving for is developing a training
3 simulation that will enable U.S. to turn back the hands
4 of time and change the decision and see what the outcome
5 might have been had a different decision been made. And
6 I think that that kind of thing is going to be very
7 critical particularly to elected officials who are
8 constantly struggling with what decisions to make and
9 all of the possible outcomes and consequences.

10 DR. STARNES WALKER: See, one of the advantages I have
11 in being moderator is I know when to throw a slow pitch.
12 Chris spent years at FEMA before coming to S&T, so I
13 knew that he would be able to answer this very well.
14 Thank you, Chris.

15 Jim Tuttle is head of our explosives division. As we've
16 heard from the Defense Minister about the issues in
17 Afghanistan, we certainly have seen this around the
18 world, that the terrorist's choice weapon, weapon of
19 mass influence, if nothing else, is of course the
20 improvised explosive device, but also just the
21 unauthorized use of explosives. We've also seen around
22 the world the propagation of understanding of how to
23 make homemade explosives, not necessarily conventional
24 explosives, so the threat continues to expand. And how
25 we approach that is specifically right into Jim's camp.

1 So I think we're all going to look forward to seeing how
2 Jim looks at this in his portfolio. Thanks, Jim.

3 MR. JAMES TUTTLE: Thank you, Starnes. Appreciate it.
4 Thank you also to the Swedish Civil Contingency Agency
5 for having U.S. here. I'll start off with what keeps me
6 up at night. As far as on a nonprofessional level, it
7 would be taking a red eye over here, in the middle
8 aisle, the middle seat, with two hockey players on each
9 side of me. That keeps me up at night. But in a
10 professional side, as far as being explosive division,
11 is having IEDs go off in our country. We talk about
12 mass disruption. We years ago had a sniper in
13 Washington, D.C., and he was shooting somebody about
14 once a week. And after about four or five weeks the
15 whole city was just totally changed, the thought process
16 of people of how they went about their day, daily life,
17 and it really disrupted the city. They eventually
18 captured him, thank God, but imagine if IEDs started
19 going off, explosives started going off. There are some
20 people that view IEDs as more of a war-like type weapon,
21 and we all know that that's not the case. Israel went
22 through years of this. And it doesn't have to be a
23 suicide bomber either. It could be a placed package.
24 Someone walks in the metro, places a backpack and just
25 walks off. So it's definitely a real and present

1 danger, and it's very easy to make a homemade explosive
2 device now. Get right on the internet and Google it,
3 and it will tell you how to do it. I mean, they've got
4 videos. So it's a very dangerous thing we're dealing
5 with here. So the challenge, after saying that, the
6 first challenge that comes to mind is the homemade
7 explosive, detecting it. Around the world we're trying
8 to do this right now in our airports. I mean, that's
9 the main focus I would say in the airports of the
10 screening versus mass transit. In the airports they're
11 looking at how do we allow people to start bringing
12 liquids and gels back on the airplane, and I'm here to
13 tell you it's a real threat and it's really hard for
14 these machines to be able to tell the difference between
15 a benign substance and the real threat.

16 Now, there is technology out there that can do those
17 things, but the problem there is not only detection but
18 the other part is the false alarms. And that's what's
19 really going to get you right now. There are going to
20 be so many false alarms with some of the technology out
21 there that, for example, if you're going through a
22 checkpoint and you yourself or the bottle you had
23 alarmed, what do you do if it alarmed? Do you open it?
24 There's all sorts of issues with false alarms. So until
25 we drive the false alarms down and the detection, that's

1 going to be a big challenge. So that's on homemade
2 explosives.

3 As far as another challenge would be mass transit. When
4 you think about detecting a threat before it gets on a
5 train, subway, before it gets on a ferry, whether it's a
6 vehicle or a person, it's a great challenge to be able
7 to see that. We can't have checkpoints like we have at
8 the airport at a metro system, a subway system. That
9 would just impede the flow of travel. So how do we do
10 it in a way that it doesn't slow people down, but we
11 still can detect weapons and explosives? That's a big
12 challenge there.

13 The last question you had was based on what are the
14 three take-aways. I'd say the first one is I mentioned
15 the homemade explosives in mass transit is going to have
16 to be an international effort to work this. It's much
17 more than just the technology itself. It's how you
18 place it and how the users would actually use it. In
19 our country we have TSA that does the screening in
20 airports. Well, they don't do the screening in subways
21 and metro stations and ferries, so that means that the
22 law enforcement people are going to have to operate this
23 equipment. So that would be the second take-away: It's
24 very important to bring the users involved with the
25 technology as early as possible, because what we don't

1 want to do is develop some technology in the back room
2 and think it's perfect and say, okay, go ahead and
3 productize it now, and people start buying things. Now,
4 if you put quality equipment on a quality products list,
5 then the first responders are going to feel like okay
6 it's thoroughly tested; let's buy it. But you have to
7 have them test it, develop it with you, get the inputs
8 back from the users. So it's very important.

9 And the last thing is basically the international
10 community, the researchers, as we're doing with Sweden
11 and some other countries, it's very important to work
12 this issue together because there are bright minds over
13 the world that think about how we're going to be able to
14 solve this problem. Because right now we don't have the
15 problem even nearly figured out at the checkpoint and
16 now we're thinking about doing it at a standoff
17 distance, whether there's a vehicle or suicide bomber or
18 package itself. Every day in our country there's a
19 suspicious package found in the country, and if it's
20 found near a -- well, you just had it happen not too
21 long ago. It was a criminal activity. If it's found
22 next to a police barracks or a helicopter or whatever it
23 is, you have to figure out what it is, what you're
24 dealing with, call in the robots -- it takes hours. If
25 it happens in the metro, it shuts the metro down. If it

1 happens in the airport terminal, it shuts the terminal
2 down for hours. So how do you have technology to be
3 able to tell quickly and effectively is it a threat,
4 what kind of threat it is, if it is a threat, and then I
5 haven't even spoken about the last thing: How do you
6 defeat it at a standoff distance. So those are some of
7 the challenges. Thank you, Starnes.

8 DR. STARNES WALKER: Jim, you talked about the
9 difficulty of detecting the devices and the explosives.
10 Could you say a few words about the importance of
11 lessons learned from operations on an international
12 standpoint and the importance of intelligence sharing.
13 The more you know about your adversary or potential
14 adversary, what role does that play in enhancing
15 homeland security?

16 MR. JAMES TUTTLE: Intelligence plays a very, very vital
17 role not only in U.S. defeating the threat but also from
18 a research standpoint. When you look at homemade
19 explosives, I'll just give you an example. There's all
20 sorts of different types of homemade explosives you can
21 develop, and a lot of the technologies, for example,
22 X-rays, it looks for the density of this material. And
23 the material, you could have different materials. You
24 could add pepper, you could have cumin, all sorts of
25 different things. So what intelligence will do is help

1 U.S. determine what do we need to put as the highest
2 priority for the technology, because we're not going to
3 be able to do everything. Focus that technology on the
4 more likely threats, and in the meantime develop the
5 other capability to see the wider gaps and threats. So
6 it's very important.

7 DR. STARNES WALKER: Thanks, Jim.

8 Anh Duong is head of our borders and maritime security

9 division. She has years of experience with the U.S.
10 Navy. And I think we saw again from the Defense
11 Minister's movie the importance of maritime security,
12 maritime surveillance in the regions here, and certainly
13 that's shared globally, so I think she'll have a lot of
14 exciting things to talk about in what we have underway
15 that will have very common grounds with what we have
16 been hearing today.

17 MS. ANH DUONG: Good afternoon. Just like the name of
18 my division suggests, we basically have three
19 portfolios: Border security, maritime security and
20 actually cargo security as well. So in general just
21 like our green book talks about, in general we are
22 looking for technology or capabilities to detect,
23 attract, whether it's bad things or bad people trying to
24 cross the border getting into United States, as well as
25 incoming cargo, whether it's maritime cargo or air cargo

1 going to airplanes. More specifically, what keeps me up
2 at night, you know, the most challenging S&T questions.
3 When it comes to border security it's actually the
4 ability to tell the difference between an animal and a
5 human, because we could theoretically sprinkle our
6 borders with sensors, but as you know sensors without
7 the smart algorithm to tell our agent whether it's a
8 bear, a tiger, a rabbit or it's actually a person, would
9 not do much good. Because of that, because of the lack
10 of very smart algorithms right now, any system that we
11 even think about deploying on the borders we would have
12 to have cameras so that the agent could look at the
13 camera and determine whether it's a human or just a bear
14 or a tiger or a rabbit. But, as you know, cameras are
15 expensive, and you can't see everything with cameras,
16 can't place cameras everywhere, can't see through thick
17 forest from top down, can't see very well under water.
18 The same technology that works for land doesn't work
19 under water. A lot of technologies don't work well in
20 thick fog, salty water, high humidity or our border with
21 Canada in the winter, sensors that would have to be
22 buried under feet of snow, frozen ice, et cetera. So on
23 top of just having sensors is the ability to tell
24 whether it is a true border crossing event so that our
25 agent wouldn't have to have so many false alarms, so to

1 speak.

2 As far as maritime security, the Minister of Defense
3 talked about the high level, how do we tie the various
4 capabilities from regions or even from one country to
5 another to create the common big picture. Also I would
6 like to add to that the tactical level. Even from one
7 region to another or even just at one region, one
8 sector, one harbor, one port, right now we do not have a
9 very good capability to detect and track small vessels.

10 As you know, the AIS transponder is only for big ships.
11 We do not have a way to track small vessels out there --
12 fast boats, yachts, fishing boats. And one specific
13 class of small vessel that we are very worried about is
14 the semi-submersible, semi-propelled vessel. These are
15 little dinky boats that could go from Colombia to the
16 U.S., to San Diego and could carry up to 20 tons of
17 cocaine or whatever else that they choose to carry,
18 whether it's WMD or chem/bio or whatever. Just one
19 scoop, no need to refuel, just need one or two guys to
20 drive the boat. And it's not a sub. If it's a sub,
21 it's easy to detect with our submarine detection
22 capability and technologies. It's not a boat, it's not
23 a ship. It's semi-submersible, meaning it's right in
24 that area where there are a lot of noises. It's very
25 hard to listen or to detect these things. And of course

1 these boats usually are built with fishing boat engines,
2 so from any signal perspective they give the same signal
3 as you would get from a fishing boat. So that gets to
4 the next point I'd like to make is, even if we're able
5 to see everything, how do we know among the thousands of
6 boats, vessels out there in our harbor, does this one or
7 that particular one have bad intentions that we have to
8 pay more attention to. So being able to detect is one
9 thing, but the next thing is how do we determine the
10 intent of that vessel.

11 And that brings up the next point, which is data fusion
12 and how are we able to block into many different what we
13 call many different nontraditional databases to get the
14 information to put together information so that we can
15 be more effective at flagging what we consider high
16 threat, whether it's high threat cargo or high threat
17 vessel or just things that we need to take a second look
18 or further inspection. That is not just about
19 interoperability. It's actually about data mining,
20 different algorithms, different smart ways to look at
21 nontraditional data, to pull out just one key word or
22 context to help our agents do a better job at flagging
23 high threat things.

24 In the area of cargo, especially maritime cargo, as you
25 know there are what we call layers of defense that our

1 customer, the Custom and Border Protection agency, is
2 doing or considering doing right now. We screen
3 100 percent of our cargo, and screening means our agents
4 use a technology database to read the manifests and
5 getting other data or intel data to help them determine
6 which cargo will need further inspection. So those
7 would be flagged as high threat cargo, and then the high
8 threat cargo would then be scanned using X-ray, other
9 imaging technology and then as well as manually
10 inspected, open up the box as necessary. So we are
11 looking at technologies that help our customers, in this
12 case the Custom and Border Protection agency, to do a
13 better job, cheaper, faster, more efficiently for all of
14 the above, whether it's screenings, whether it's
15 scanning, whether it's enhancing the image. Maybe in
16 the future we'd like to have a 3-D image so that they
17 can tell better when staring at something whether it's
18 anomalous or not, as well as another layer which is what
19 we call supply chain security. These are devices that
20 would alert authority when a cargo has been tampered
21 with or somebody has attempted to poke a hole or put
22 things in the cargo or take things out of the cargo or
23 remove the door, for example. So when it comes to cargo
24 security, it's not just the technology, whether
25 technology can help U.S. do that. Because there are

1 plenty of technologies on the market which could help
2 U.S. alert when there's a tampering event, but the key
3 here is how do we make sure that those technologies are
4 internationally acceptable, internationally approved,
5 because when we talk about cargo it truly is a global
6 chain. So we in the United States understand very well
7 that when it comes to cargo security, especially supply
8 chain security, we need your help. We need to talk to
9 all of our international partners, because a lot of
10 these technologies will not be used by just the U.S.,
11 and so when it comes to cargo security, especially
12 supply chain, we in DHS do not aim to develop new
13 technologies or gadgets and deliver them to our
14 customer, because in this case the United States Custom
15 and Border Protection agency is not going to buy these
16 devices and issue them to the shipping industry.
17 Actually, in this case the users will be the shipping
18 industry. So that means that we have to build a
19 business case. It has to make business sense to these
20 industries from their standpoint. They certainly have
21 gone into business to make money, to make profits just
22 like anybody else. They didn't go into their business
23 to make the United States more secure; we understand
24 that. So from our standpoint it's security, but we have
25 to look for ways to enhance what's in it for them, to

1 help build a business case for them to entice them to
2 use technologies. So one thing -- and it's a key
3 take-away when it comes to cargo security -- is that I'd
4 like to make sure that this audience and anybody else
5 who talks to U.S. understand that we are not proposing
6 or mandating or encouraging or promoting a particular
7 device, a particular vendor. Instead what we're doing
8 is we are trying to develop open standards that
9 eventually, hopefully, will be approved and acceptable
10 internationally so that any vendor out there could build
11 these devices and then sell the shipping industry. That
12 is one way to keep the costs down. It also then doesn't
13 run into proprietary issues so that for example EU
14 doesn't have to worry about using U.S. proprietary
15 technology. Again, we're not going to promote any
16 specific vendor. What we're doing is we're developing
17 technology to prove to our customers that if we set the
18 standards this way and these are the requirements, at
19 least we know that there's one device out there, one
20 company out there, that will meet the requirements. So
21 it's doable from that standpoint, but we have no
22 intention of pushing any specific vendor or technology.
23 Once the standards are approved and accepted, it's an
24 open market. Anybody who can build the device that
25 meets those requirements will be in a good competitive

1 position.

2 Another take-away is the fact that I have a lot of
3 vendors approaching me and then somebody asks me a very
4 good question like another forum like this is, what are
5 some of the things which as a vendor you shouldn't do?
6 Because it really is a waste of your time as well as my
7 time, so I thought I would repeat that here because it's
8 a really very good point. One thing I would point out
9 is a lot of vendors that I've come across had the
10 assumption, made the assumption, that all they have to
11 tell me is, oh, my gadget or my technology has worked in
12 Afghanistan or it's being used by U.S. Special Forces in
13 Iraq, for example. And they think that that would be
14 the key word that would get DHS's interest. No, because
15 there's a big difference. When a technology could be
16 used for defense it doesn't mean that it will be viable
17 for Homeland Security. Many different reasons why
18 that's not the case, but I'll just give you a simple
19 reason or simple example because it just happened to
20 U.S. very recently. Something simple, very simple. We
21 tried to set up a test bed in New York, and as you know
22 a lot of times when we try to put up a sensor or camera
23 or whatever it happens to be, the ideal location happens
24 to be on private property, which means we can't just put
25 it there. We have to ask permission. So we talked to

1 the owner, and the property owner, a U.S. citizen, of
2 course is very worried about homeland security. At
3 first he's very cooperative. He's more than willing.
4 Then when we talk in more details, then he looked at the
5 picture of what we're proposing to put in his backyard
6 so to speak, and he says, oh, no, you're not going to
7 put that big ugly gray thing in my backyard, are you? I
8 have a \$5 million property. You're not going to put
9 that ugly sensor up. Can you just give me a little
10 small box and paint it green so that it melts into my
11 garden, things like that. And, well, you know, it's not
12 a trivial thing to downsize a big radar system into a
13 little box. So there are considerations that one would
14 not have to worry about when one develops something
15 that's going to go on a Navy ship. Yeah, it could be
16 ugly. It could be gray. Who cares? But Homeland
17 Security, we deal with other folks, other stakeholders
18 like private property owners. On our border with Canada
19 we have many Indian tribes there, so it's not even U.S.
20 territory in that sense. So there are a lot more
21 considerations. And cost is another big reason why many
22 DOD or defense systems cannot be used by Homeland
23 Security, just because of the pure, simple reason it's
24 too expensive. At the same time there are many cases
25 that we might be able to trade the cost -- trade that

1 off with accuracy because we don't need -- it's not like
2 DOD where we have to get it right to that location
3 within one meter or one centimeter, because we're not
4 trying to drive a missile there. We're not worrying
5 about collateral damage. So our agents, all they need
6 to know is that general area, because they might know
7 that there are only four ways to get out of that
8 mountainous area, so they just go to the four points and
9 wait for the bad guys to come out. They don't need to
10 pinpoint to the last meter or last foot where the person
11 just crossed the border. So there might be ways that we
12 could so-called dumb down the technology to lower the
13 cost. So that would be another key take-away is it
14 would be a waste of our time if you approach U.S.,
15 Homeland Security, with the assumption that if you have
16 a technology that is of high interest or is being used
17 by the defense side that it will be an automatic sell to
18 Homeland Security. Thank you.
19 DR. STARNES WALKER: Thank you, Anh.

20 Sharla Rausch is our division head for human factors,

21 and I think we have seen threaded throughout today the
22 importance of how we operate and how we have to bring
23 the human element into technology. And as we've said
24 earlier that the integration on the seam of human
25 behavioral social sciences, physical science, we have to

1 look at all of that together, and if we look at the
2 importance of biometrical information and other things,
3 these are some of the things that Dr. Rausch has looked
4 at, is looking at with her portfolio. So I think she'll
5 have a lot of very interesting things to share in terms
6 of the importance of our investments in the science of
7 human factors.

8 DR. SHARLA RAUSCH: Good afternoon. Good afternoon and
9 thanks again to the Swedish Civil Contingencies Agency
10 for hosting this conference. And welcome to all our
11 various international friends out there. It's an awful
12 lot of fun to see all of you. Hey. What keeps me awake
13 at night? People. I'm not talking about my boss. He
14 doesn't keep me awake at night. I'm talking about the
15 extremists plotting a violent action. I'm talking about
16 facilitating the travel of law-abiding citizens and
17 visitors to this country. I'm talking about the people
18 who are impacted by either a man-made or a natural
19 disaster. Chris Doyle focuses on the critical
20 infrastructure of buildings, and we focus on the social
21 infrastructure, the social and psychological impacts to
22 people of an event. I like to say that our division is
23 responsible for the harder science: People. And as
24 part of our mission we ensure that practitioners and
25 intelligence analysts and policy makers have

1 science-based, effective, usable and where it touches
2 the public, and almost everything does, acceptable
3 capabilities that will help them to identify violent
4 extremism well before there's an act that jeopardizes
5 lives or critical infrastructure. And as part of that
6 is our violent extremism program where we're looking for
7 those indicators and signatures that will help U.S.
8 identify those threats in months, if not years, ahead of
9 an act occurring. And if you want to know any more
10 about that you have to come to the breakout session
11 tomorrow because it's going to be good.

12 We also are responsible for identifying known and
13 unknown threats at over 400 U.S. ports of entry. I
14 don't know if you're aware, but we have over 400,000,000
15 people cross our borders in a given year, and we have
16 about 1.2 million pass through our airports on a given
17 day. Now, as you all know, when you're having to go
18 through those ports of entry, you want to move as
19 quickly as possible. So the challenge for U.S. with our
20 biometrics program is to be able to identify in near
21 real-time an individual's identity to determine whether
22 that is a legitimate traveler or whether it is a threat
23 to our country. And the challenge for U.S. is that it's
24 not always optimal conditions. We're on the ocean,
25 we're on the southern border, which is desert, we're on

147

1 the northern border, which is cold. We're mobile and we
2 have to do it quickly and we have to do it accurately,
3 because if we have a false positive, somebody goes into
4 secondary screening. If we have a false negative,
5 somebody gets into the country who shouldn't have. So
6 we have to be as good as we can on that. And then there
7 are the unknown threats, and that's where our suspicious
8 behavior detection capabilities come into play, and
9 that's where we look at various physiological cues,
10 whether it's changes in skin behavior, whether it's
11 pulse or heart rate or the behavioral cues, looking at
12 things such as microfacial linkages or emblems. Again,
13 fast, accurate, noncontact, a tool that the screener is
14 able to use to enhance his or her own capabilities. And
15 we're concerned with identifying capabilities to enhance
16 community resilience. And we look across the whole
17 spectrum in terms of preparedness, response and
18 recovery. Ideally we would like to see communities have
19 those capabilities well before an event occurs so that
20 if something happens they're able to bounce back, not
21 even at the level they were but even at a higher level
22 and a stronger level. So our concern is strengthening
23 that social fabric and avoiding tears in that fabric.
24 The messages I think I would like to leave you with is
25 that it does all boil down to people. I don't care what

1 you're talking about. It's going to boil down to the
2 human being and everything we do. Part of what I do
3 with my colleagues, for instance, is a community
4 perceptions of technology panel, where they bring their
5 technologies in and we have a panel of a variety of
6 people: Different types of lawyers, different types of
7 public interest groups. For Anh's group we looked at
8 border technologies, and those were along the border
9 with Canada. So we brought Canadian groups in to look
10 at those technologies, and to a one, the program
11 managers have said I didn't think of that. It gave them
12 a new perspective on how they approach that technology,
13 and that's important. The other thing I'd like to leave
14 you with is that every single challenge we've talked
15 about is a global challenge, and that means it's going
16 to take a global solution to this. What we need are
17 partnerships, good strong partnerships, and I know my
18 division has benefited greatly from partnerships with
19 just about every country represented out there. Thank
20 you.

21 DR. STARNES WALKER: Thank you, Sharla.

22 Trent DePersia is our deputy division head for our

23 command control interoperability division, and again
24 across the theme of what we've heard today, what we
25 heard in terms of the ESRIF report, the idea of the

1 importance of interoperability and how we communicate
2 across is so important in the adaptation of technology
3 to meet and enhance security issues. So I think that
4 all of the technologies that we develop, ultimately how
5 it fits into a structure, an operational structure, and
6 how we're able to communicate across many different
7 domains is very, very important. And it's a central
8 focus for the C2I division, so I think Trent will also
9 have a lot of things that will resonate well with our
10 discussions today.

11 MR. TRENT DePERSIA: Thank you, Starnes, and thank you
12 for the opportunity to be here and intermingle and talk
13 with folks. It's a pleasure. The division, the Command
14 Control and Interoperability division, is one that
15 crosses many domains. There are aspects of what we're
16 doing that touches on all of these other divisions as
17 well as addressing a lot of things that have been
18 discussed already today by various speakers. The kinds
19 of things that worry or concern me, I'll summarize it as
20 addressing the continuum of information issues. How do
21 we acquire, how do we manage, how do we analyze, how do
22 we share, and how do we secure that information? We're
23 not necessarily developing all of the acquisition
24 devices or management devices. In fact, we're relying
25 on others to do some of those things. But in the

1 analysis side there are certainly a number of different
2 things that need to be done better to help provide the
3 information that's actionable, that can get to the end
4 user and make it usable to them. Sharing has to do with
5 moving information from one person to another, from one
6 system to another, as well as communications
7 interoperability, voice communications. And, in fact,
8 we have one of the radios that we are developing
9 inoperable, but it's downstairs and we're in the process
10 of testing and evaluating that multiband radio. And
11 securing the information either through encryption of
12 the voice communications or cyber security, a whole
13 'nother area that we're focusing on. And all of these
14 issues really are necessary, I believe, to provide the
15 security and safety for the communities, for the
16 regions, for the nation, for international use. But
17 there's many more than technology pieces. There are
18 standards, there are policies, there are governance
19 issues. Again, things that have been talked about and
20 discussed already today. And we look at these through
21 our interoperability continuum to make sure that we're
22 not ignoring some aspect of the technologies that we're
23 either developing or trying to use in a different way so
24 that it's impossible to use or the training is too
25 difficult to use or there are governance or policy

1 issues that we now have to make some adjustments to to
2 make sure they're usable. The promising technologies?
3 Well, I mentioned one of them: The multiband radio.
4 It's a radio that is in a small handset that's a typical
5 radio that's available today, but it has the ability to
6 go over all of the frequency bands that are available,
7 at least that we're using in the United States. From
8 approximately 140 megahertz up to 870 megahertz, it has
9 the ability now to be interoperable with all of the
10 various components, be it the federal level, the state
11 level or the local level, and including some of the
12 defense-oriented communications.

13 Another promising area is visual analytics, primarily
14 work that we're doing through our National Visualization
15 and Analytics Center, or NVAC, that is established
16 within the university-based and some industry-based or
17 lab-based entities in the United States, as well as
18 working with some of the international universities to
19 establish a more robust, longer term research capability
20 that will enable U.S. to provide information again that
21 is actionable. An end user has only so many senses and
22 the ability to assimilate and use all of that
23 information, so we're trying to develop the tools
24 necessary for them to understand what is really
25 happening at any given point of time.

1 All of the efforts that we have or we're pursuing are
2 practitioner based. That is, we're working with the end
3 users, as was mentioned a little bit already, to make
4 sure that we're not developing a technology because a
5 scientist likes it or an engineer likes it. And as also
6 part of this we're trying to make sure that each one of
7 these technologies are tested or evaluated in a pilot to
8 make sure that, again, the technology is usable. The
9 button on a radio may not be in the right place because
10 the fireman can't use it. His gloves are too big. We
11 may not have thought about that during our planning
12 stages, but bringing it into the pilots and
13 demonstrations, we'll know early enough in the process
14 so we can make those adjustments. And if we don't make
15 those adjustments, if the button, for example, is in the
16 wrong place, it won't be used by the end user, which
17 means that our technology will not have a successful
18 transition into practical use. Something further down
19 the road that was kind of touched upon already is
20 anomaly detection. What information is there that just
21 kind of sticks out like a sore thumb but we don't see it
22 as a sore thumb? How do we make it, again, actionable
23 information? It's a long-term technology area that
24 we're just trying to get more involved in. So that's
25 what I would call a promising technology of the future.

1 Take-aways: I think I'd like to leave you with the
2 thought that we're looking at it from a holistic
3 perspective, that we're looking at using systems that
4 are available today, not necessarily just improving or
5 developing new technologies. Again, points that were
6 made earlier today. We're building on successes of
7 things that have worked. We're building on the
8 unsuccessful things so that we don't keep making the
9 same mistakes and making sure that the technology is
10 usable and viable. We're trying to evolve all of these
11 and to make them into an interoperable environment so
12 that all of the pieces of information can be used and is
13 practical.

14 We're also looking at more collaboration, not only
15 within the folks within our own division, within our
16 country, but internationally. The NVAC, the National
17 Visualization Analysis Center, for example, is an entity
18 that I had mentioned we're working with a number of
19 universities internationally based. The multiband
20 radio, while it may not have the significant impact in
21 the European community, because of how the spectrum is
22 used here, it does have an impact on our borders on the
23 Canadian border and the Mexican border. Cyber security
24 certainly is another issue, and there have been a number
25 of things that we've worked on with the oil and gas

1 industry, for example, or the domain name system
2 security. So there's issues and challenges that we're
3 working there in collaboration. And just in general to
4 look at the practitioner driven approach for the
5 collaboration across the international boundaries, to
6 make sure that we address all of the technical issues as
7 well as the cultural issues, to make sure that
8 technology finds its home in everyday life for all of
9 the folks in public safety helping U.S. to protect our
10 homelands. Thank you.

11 DR. STARNES WALKER: Thank you, Trent.