

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.