THE BROOKINGS INSTITUTION

THE CYBERSECURITY EXECUTIVE ORDER AND PRESIDENTIAL POLICY DIRECTIVE: WHAT DOES SUCCESS LOOK LIKE?

Washington, D.C.

Tuesday, November 19, 2013

Moderator:

IAN WALLACE
Visiting Fellow
The Brookings Institution

Panelists:

SUZANNE SPAULDING
Acting Under Secretary for National Protection and Programs Directorate
Department of Homeland Security

ALLAN FRIEDMAN
Fellow
The Brookings Institution

RICHARD BEJTLICH
Chief Security Officer
Mandiant

* * * * *

P R O C E E D I N G S

MR. WALLACE: Okay, hello, and welcome on behalf of Brookings' Center for 21st Century Security and Intelligence. My name is Ian Wallace, and I'm the visiting fellow for cybersecurity within 21CSI.

Today we're honored to have a distinguished panel to discuss what Acting Homeland Security Secretary Beers and FBI Director Comey told the Senate Homeland Security Committee last week is one of the greatest threats to the nation, a cyber attack on the country's critical infrastructure.

Now, that herring was of course not the first time the administration has warned Congress about the threat to such an attack. It was in fact -- I'll give you the administration's frustration at Congress' unwillingness or indeed inability to pass legislation that prompted the White House to issue two documents on the 12th of February, same day as the President highlighted the significance of the cyber threat in his State of the Union, and those two documents -- Executive Order 13636 and Presidential Policy Directive 21 -- immediately became the centerpiece of the government cyber policy.

Now, I think we can certainly argue that they've been successful in at least one regard, and that is, I think, (inaudible) is to diffuse some of the political rancor that surrounded this issue. However, one of the ways they did that was to promise a long set of deliverables, many of which the timelines for delivering them have passed, and that is what we're here to explore.

Not surprisingly, the centerpiece of the Executive Order was a voluntary framework that's been taken forward by NIST, along with the

representatives of the 16 critical infrastructure sectors. But there was a lot more that the government undertook in that framework from voluntary information sharing scheme, reissuing of national infrastructure protection plan, as well as certain organizational issues within government.

Much of that work fell on the plate of Suzanne Spaulding, the Acting Under Secretary for National Protection and Programs, and so we're very pleased to have her here with us to explore whether that effort is indeed making us any safer or at least taking us further forward on the path to being safer. In other words, what does success in terms of the Executive Order and PPD 21 look like and, as importantly, how will we know when we've got there.

And to help us understand the complexity of the (inaudible) behind that, we're also joined by two cybersecurity exerts, Richard Bejtlich, from the end, who is the chief security officer of Mandiant, and Allan Friedman, my Brookings colleague and a Fellow within our Governance program.

I'm not going to take too much time on bios. You should have them in front of you. Suffice it to say each of the panelists is extremely well qualified to talk on this issue.

Prior to her current position, Suzanne was the deputy under secretary at DHS for infrastructure protection. Before that she had been a lawyer in the private sector, staff of Intelligence Committees in both houses of Congress, and spent six years at the CIA as well as being on numerous radio panels, including at the state level and working closely with business roundtables.

For his part, Richard began his work in this sector as an Air Force

intelligence officer and then pursued a career in the private sector, as well as authoring some very well-regarded cybersecurity books. Most recently, he set up a particularly impressive cybersecurity team at GE before joining Mandiant, one of the world's premier cybersecurity consulting firms, as their chief security officer.

And Allan is one of our cybersecurity experts here at Brookings, most of his current research focusing on the economic aspects of cybersecurity. He is, in fact, the only computer scientist on the panel, having been a Fellow at Harvard's Computer Science Department before coming here. But just to show you that he's a man of multiple talents, he's also the author of a book with the 21CSI Director, Peter Singer, called *Cybersecurity and Cyberwar, What Everyone Needs to Know*, which will be on the bookshelves in January.

So, I'm going to hand it over now to my three panelists, starting with Suzanne, have some short discussion, and then we'll follow that with questions from the floor. We are live tweeting this, hash tag, you can see, cyber2014. Feel free to tweet along, although please keep your devices silent if you wouldn't mind.

So, Suzanne.

Three questions to get her started.

First of all, just to get everyone on the same page, if you could tell us what the EO and the PPD were meant to achieve from the administration's perspective. Second, if you can tell us what you at DHS and what the administration have been doing to put that into practice for the last nine months

and what you have to show for your efforts. And, finally, give us your assessment, if you wouldn't mind, of where that takes us. Are we safer? How would we know if indeed we are getting safer?

MS. SPAULDING: Great. Happy to do that. And thank you. Thank you to Brookings for holding this session. You know, it's really very valuable for us to have these opportunities to get out and let people know what we've been doing and where we're headed and why we think this is really important. So, I'm grateful to you for sponsoring this event, and thanks to the both of you for agreeing to participate.

I am the Acting Under Secretary for, as was mentioned, something called the National Protection and Programs Directorate in the Department of Homeland Security, and we have the responsibility for worrying about strengthening the security and resilience of our nation's critical infrastructure, and we do that by working with a wide range of stakeholders: other departments and agencies across the federal government who are the sector-specific agencies for some of the 16 critical infrastructure sectors that we've identified; folks at the state, local, territorial, and tribal level; and perhaps, most significantly, critical infrastructure owners and operators both public and private. And of course all of you know the statistic that we've been using for at least a couple of decades now that about 85 percent of our critical infrastructure is owned and operated by the private sector. So, that relationship is extremely important.

Basically what we do and what the Executive Order and the PPD

are designed to improve and assist and advance is that we work with those stakeholders that I've just described to help ensure that we are all making wise risk management decisions. The notion of strengthening the security and resilience of our nation's critical infrastructure is really an exercise in risk management, and so much of what we're doing and what I am about to describe is really designed -- we are basically, at the Department of Homeland Security and NPPD, a service organization. We are here to provide services that help critical infrastructure owners and operators make wise decisions as they look across their enterprise at risk management; we help to inform those decisions. So that's, at its base, what we are all about in NPPD.

On February 12th of this year, the President issued, as was said, the Executive Order on Cybersecurity and the Presidential Policy Directive on strengthening the security and resilience of critical infrastructure. It was not a coincidence that these came out on the same day. One of the things that we have been really driving toward is making sure that we are taking a holistic look at that risk management proposition, right? So, when we talk about strengthening the security and resilience of critical infrastructure, what we're focused on is that functionality, right? What we're really talking about is making sure that when people in this country get up in the morning and turn on the light switch, the lights come on; that when they go to brush their teeth, they turn the faucet and water comes out; that when they go to eat their breakfast, the food has made it from the farm to the table; they get in their car or their public transportation and the transportation infrastructure is there to get them to their

office; when they get there, they can turn on a computer and the entire information highway is open and available to them. Those are the kinds of things that we worry about. It's that functionality and sustaining that and making sure that that is there in order to sustain our ways of life and to ensure our economic viability, our national security, public health, and safety, right?

So, if you think about it in those terms, you realize that that functionality can be disrupted in ways that are both physical and cyber. If you're taking that classic risk management approach, which says start by assessing your risks as a function of threat vulnerability and consequence, you have to look at what are the ways, what are the risks to sustaining that functionality across the critical infrastructure sectors. The risks can come at you from all hazards: from natural events, extreme weather, aging/failing infrastructure, sabotage, terrorist attacks, cyber attacks, a wide range -- pandemics, lots of things that can disrupt the sustainability of critical infrastructure functionality. So, it's really important that you look at it in that kind of holistic way.

Similarly, the vulnerabilities that those threats that are coming at you can exploit -- you have to look across physical and cyber vulnerabilities. When you're thinking about how do I prioritize these risks that are coming at me, one of the most important aspects of that is consequences, right? What's the so-what? If a threat comes at me and it is able to exploit a vulnerability, you know, what is the consequence of that?

So, we spend a fair amount of time improving our capabilities to help inform critical infrastructure owners and operators and our stakeholders

across the Homeland Security enterprise about consequences. You know, what are the kinds of things that will happen, most significant consequences? And, again, we know now that cyber attacks can have very significant physical consequences. Increasingly, that critical infrastructure is being managed through industrial control systems, through networked systems. And those systems can be disrupted. They can be corrupted. They can be manipulated in a way that gives you misleading readings, et cetera, so that through these cyber vectors as well physical vectors they can produce physical consequences that can disrupt or destroy the ability of that critical infrastructure to continue to provide that functionality that we rely upon.

So, again, you've got to look at this across physical and cyber, and then as you look at ways to mitigate those consequences, which is a key part, you want to look at how you can address the vulnerabilities; how you can, across the enterprise, prevent those threats or hazards; how you can reduce those vulnerabilities; and how you can mitigate those consequences. You want to look at that across physical and cyber. Sometimes the most cost-effective way to mitigate the consequence from a cyber attack might be through some physical approaches and vice versa. So, you've got to look at this across the board.

So, that is a big part of what the PPD and the EO were designed to do, to make sure that we're looking at this across a physical and cyber divide, that we're looking at it across all hazards.

So, pursuant to that, very quickly, we had a series of deliverables under the PPD, and I will say, proudly, thanks. Prior to the shutdown we met all

of those very ambitious deadlines for our deliverables.

And I want to ask Bob Kolaski and Jeanette Mamford to stand up, because they are the leaders of our integrated task force. We took both documents. We set up a task force to, in an integrated way, implement these, again, very much in a holistic way, and they've done a fabulous job, and they're going to answer all of the hard questions that come up.

So, we looked at the public/private partnerships, made recommendations for improving those -- what are the attributes that we saw in effective public/private partnerships and how can we promulgate that throughout at the national, regional, and local levels.

We looked at information sharing in the PPD and in the Executive Order and what are the ways in which we can institutionalize more effective information sharing both at the classified and unclassified levels. We're big on unclassified -- getting information to an unclassified level, because that's what we're all about, getting that information out so that we can inform those risk management decisions. And then of course the big one was the rewrite of the National Infrastructure Protection Plan, the NIPP, and that has been delivered to the White House. It's going through the -- I think we just completed the inner-agency review process that happens after that. We're now taking in all of those comments, and we'll turn that back around and get the final product into the White House.

And, again, you will see these themes that I opened up with reflected in that document. It is all hazards across physical and cyber, stressing

the importance of public/private partnership, the emphasis on the risk management framework, and cross-walking that to PPD8, which is on national preparedness, which is another way of slicing that same risk management approach, right?

So, under the Executive Order, the big deliverable is the cyber security framework, which is collecting best practices from across the private sector -- you know, NIST, that Commerce had the lead at that. And they had lots of sessions with the private sector, as did our folks in the ITF, a very collaborative process, thousands of participants throughout this process, to collect the private sector's best practices and organize those in a way that could be useful, again, more broadly, across the entire nation, all of our private sector and state and local territorial and travel and federal stakeholders.

DHS then will have the role, so the preliminary draft is out. The final will be due February 12th. Please read it. Provide your input. I know they're anxious to hear from folks about ways to make that final product as useful as it can possibly be. DHS had the responsibility for developing performance goals and the voluntary program. So, the cybersecurity framework sort of breaks down into categories of identifying, detecting, being able to respond and recover. We tracked those categories in the performance goals at the national level and added one more, which is learning, improving at the end of all of that, that virtuous cycle, to go back and do it smarter each and every time. And then the voluntary program, which is -- you know, it's incumbent upon us to find every way we can to promote the use of this framework and help companies -- small,

medium, large -- find the most effective way to use this framework to improve their cybersecurity.

And I will just close with, you know, I think it has made us safer already, because all of the interaction with the critical infrastructure owners and operators throughout the process of developing I think has educated folks out there all across the country. I think it has great potential. I'm quite confident it will improve critical infrastructure, security, and resilience, because I think it will inform decisions, and I think there's a lot of natural incentive for people, given the information, to make wise decisions to protect their businesses and that functionality.

And my final thought is kind of how will we know if we're successful? I'd like to talk about my kind of utopian vision, because I think it's important to have some notion of where you'd like to go even if you'll never quite get there, and that is one in which we have perfect information sharing, which is a key part of this, starting with information about all of the comparative advantages that each of us who has a role play in this brings to bear.

What are the resources and capabilities that you bring? What are the ones that I bring? What are the ones that they bring to the table? Understand how we might bring those to bear. Have sensors out in the world that detect any perturbations that could disrupt critical infrastructure so you're very sensitive to the threats of hazards coming at you -- and then the ability to communicate perfectly as those threats manifest themselves, as those incidents arise and those disruptions that each of us is able to bring our comparative

advantage to bear on mitigating the consequences and addressing that threat and hazard and to shift as this dynamic environment shifts.

Now, you know, I had the comparative advantage here with regard to this aspect of it, but as it's shifted, actually, you're in a better position now to address that. You've got the (inaudible) on that. I'm going to do this. I mean, that sort of agility, that adaptability, that ability to innovate -- that's my utopian vision, that's what we're striving for, and I think that all of these efforts are getting us closer.

Sorry to take so long.

MR. WALLACE: Thank you very much. Lots of questions. I'll hold them until we've heard from Richard and Allan, who I'm sure have their own questions.

Richard first, same question for you, essentially, what does success look like? But you're on the front line of this in many ways, both seeing threats to the infrastructure and company's data, more generally. And you're also in a very good position to hear what the private sector is saying about what the government is doing.

Two specific areas, if you could particularly comment on. Firstly, Suzanne mentioned the importance of info sharing and this has been a common refrain. Acting Secretary Beers mentioned it in his testimony the other day. A lot of that seems to be happening already, particularly in certain ISACs, like the financial sector. Does the government need to do more? Does Congress need to do more? Is this a real problem that we need to address?

And secondly, Mandiant is famous for its work, particularly on APTs. This report that came out, actually in February of this year -- the same time as the Executive Order -- and that focused mainly on commercial espionage and so that raises the question, have we got our focus on the right ball? Is critical infrastructure taking our eye away from what is really damaging us, this death by a thousand cuts, Richard?

MR. BEJTLICH: Well, thank you for inviting me. I appreciate being on this distinguished panel. As far as what does success look like, I could sum it up in just a very few words. That would be a minimum number of incidents and when something bad happens, you notice it quickly and contain it quickly.

Those are the metrics that essentially I learned in the Air Force, as was mentioned before. And they were the metrics that were given to me -- without knowing my background -- but were given to me by the chief information officer when I worked at General Electric. He had us go into his office one day and he said, what are we doing with security? And I was the director of instant response and I said, well, we're doing this and that. And he said, listen, I want two metrics from you guys. I want a minimum number of intrusions or incidents, and that means categorizing everything that occurs, whether it's a computer that is compromised, whether it's a laptop that's lost or stolen, whatever it is, you classify it and I want you to count all of that and report it to me on a regular basis. And then I want a minimum amount of time to elapse from when the bad thing happens and when you fix it, essentially.

And when we started our preliminary set of metrics, the first number was way too high and the second number was way too high. And we reported back and he said, both of those numbers are too high. And I'll tell you the second number, just as an example, was three weeks. It took us three weeks to go from something bad happening in the environment to containing it so that it wasn't hurting us anymore. And he looked at us and he said, I want that to be one hour. Globally, for a half a million computers, hundreds of businesses, I want one hour.

And of course, after we picked ourselves up off the floor and saluted smartly and said, yes, sir, we tried to figure out how to do that.

So, after nine months, we did. We did get it down to a one-hour process. We did it, though, by focusing on the outcome, one hour, and not the mechanism. He didn't go to us and say, you need to deploy this new software, you need to implement a new process, you need to hire more people. He let the businesses decide what approach they were going to take. And it turns out, every approach under the sun was taken.

Some people threw more problems at their help desk, some people did buy new software, some people implemented process reforms, whatever the case was and that's how we were able to get there.

So I present that as a story that may sound like, well, hey, that's pretty easy. Why don't we just do that for all this stuff? Well, as it turns out, security is one of the most interesting subjects because it is so fiendishly complex. And I applaud Suzanne and her group for all the work that they've

done. It's definitely a step in the right direction, but I would offer just a caution and that is, there are sets of assumptions built into the framework, in particular, that aren't necessarily obvious. In other words, you didn't have to have a framework necessarily in order to get the right outcome -- or a more desirable outcome.

For example, other ways you could have approached this: software security -- DHS funds a very robust software security program and yet that doesn't appear in the framework. I know that they're parallel. They're both issues, but the mention of -- software security could have had a more prominent mention.

Threat reduction: in other words we're going to identify the threats who are harming us and we're going to throw even more resources against them so that they are less of a problem. And that would be reducing another element of the risk equation that Suzanne mentioned. The risk equation is vulnerability times threat times consequence. And the framework mostly focuses on the vulnerability, reduce the exposure, that sort of thing.

You could have decided to focus on T. What can you do to make the threat go down? And there's a whole suite of things you could do there. You could have counterintelligence operations, there's support for civil activities, like we're seeing Microsoft do with private botnet takedowns. So I'm not saying that the framework is wrong or anything, but it's important for us to sort of step back and think about -- there are other strategic choices that could have been made that would have potentially changed the way we go about this. And maybe

there's still room for introducing them alongside the framework?

The last thing that I'll say before turning it over to Allan is that after speaking about the framework with private sector companies -- those that we work with and just those that I meet on a regular basis -- two things have become clear. The first one is that although it's a voluntary framework, there's great concern that it will become mandatory. And not necessarily mandatory as in made mandatory by the government, but it becomes the standard against which everyone is judged.

And that may be a good thing. Some people actually want that. Some people don't want it. And one of the reasons they were afraid of it in the don't-want category is because of the privacy provisions. The security provisions are more or less -- they're very fluid. For example, they say things like -- and I've got them all highlighted in here on my tablet. Sorry, I didn't bring a notepad.

There are things like network integrity is preserved or malware is controlled. And that leaves you -- you could drive a truck through that as far as the hole that it opens as to how you would implement it. But the privacy discussion is much more specific and is much easier to know if you're complying with the privacy prescriptions than it is to know if you're stopping bad guys. So there's some concern in the private sector that if the entire framework becomes more or less mandatory, now you have what I've heard being called a privacy tax. And this is not something the private sector had anticipated when this took place.

Now, again, it's not necessarily saying that we don't need privacy

elements to this. Privacy is very important, but it's something that the private sector wasn't necessarily expecting in the document.

MR. WALLACE: Richard, thank you. And I'll give Suzanne the opportunity to respond to some of those after we've heard from Allan. But just picking up on some of the themes we've heard from both, Allan, one aspect of your work that I think is extremely relevant here is the economic aspects of this. So, incentives are integral to this process. The White House has blogged the result of the cross-government work. Some thoughts on that would be very interesting.

Reflecting on what Richard said, this raises the question of, you know, does Congress engage on this? Are we now in a position where we don't need any legislation and, if so, the legislation that is currently on the Hill, whether it gets through or not, is it required?

And finally, just picking up on the issue about privacy, an area I know that you've looked at in the past, the most recent NIST workshop, one of the suggestions was that the privacy annex was made much more general in order to avoid the problem that Richard suggested. I wonder if you could just give us some reflections on this intersection between cybersecurity and privacy?

MR. FRIEDMAN: Sure, so let's start with this question of Congress and politics. And I think there's three ways that we can look at reaction to DHS and the first and sort of most contentious, which is if you're getting hit from both sides, maybe you're doing something well. And so, if you go out into the world and you say, okay, on one hand you have the people who are focusing

on the threats. And they say, listen, DHS is still letting people have unpatch machines. They don't tell everyone we'll staple you to the wall if you have anything bad going on. So we need more teeth.

And on the other side you have people saying, DHS is trying to take over everything. And, of course, I think both of those are exaggerations and the fact you fit in the middle. It's sort of flipped.

But the second part is that, actually, the goal -- and I think we're getting close to this -- is security should be boring, right? We want this to be a level when it is something that, okay, we have to go through and understand the mundane organizational questions and everyone's handling it themselves, so we don't want this to be flashy new ideas. If we're still coming up with flashy new ideas in a couple of years, we've done something wrong. We haven't talked to enough people. We haven't brought the brainpower together.

And that leads me to the final point and perhaps the greatest success that DHS can point to so far, which is that we have more consensus now about what we need to do than I think many of us imagined we ever would have, even two years ago, when you had very senior people running around saying, the problem is the Internet was not built with security in mind. The solution is we should build a new Internet.

You had very senior people talking about it n two years ago. And the fact that a consensus has emerged that said, listen, let's think about it from a risk-based perspective and let's align incentives because ultimately it has to be a private sector problem, government can help, that's, I think, a great success

point.

So, on this incentives question, it's been really interesting to see how the different agencies that were directed to think about incentives responded. So, Department of Commerce did what I think is a classic Department of Commerce response. They went out into the wide world of commerce and said, hey, what's going on? What should we be thinking about? And, of course, they heard that the government should give more money. It should be all carrots, no sticks, which is useful because we actually learned a little bit about the different types of carrots that are available, particularly with pricing.

When you have regulated sectors who want to sort of understand how can we recoup some of this, and that's very useful, DHS went back to school. They talked to everyone who's been thinking about this problem for a while, many of whom I know well, so I applaud their effort on that, and said, okay, what's been out there? What do the theories say? What data is available?

And, unfortunately, the answer is not much, but I think they did a very good job of synthesizing and integrating this, particularly on the question of liability and insurance. I'll get back to that in a second.

And, of course, Department of Treasury said, listen, we're dealing with banks. There's nothing that we're going to have money to do that's going to change their keel one way or the other, so let's find ways that we can take their existing processes and just make them focused on security as well as all the other things they're doing. And you see three very different perspectives that

underscores the challenge just in these three very large cabinet agencies; they're thinking about this problem differently.

So any time we start talking about a comprehensive solution, if we have that level of difference in paradigm at the cabinet level, outside in the wide world it's going to be different. So we need to reflect that.

There's been an infatuation with insurance and I think there's a reason why everyone loves the idea of insurance. The story goes a little like this: I, as an actor, don't have the time and energy to care about my risk, to figure out what I need to minimize it, so I'm just going to push it onto an underwriter. Now, this underwriter has a financial interest in making sure I'm doing the right thing, so they're going to tell me exactly what to do and now I, as a CSO -- or, even better, as a CFO -- can go to my board and say, hey, listen, this isn't what we want to do, this is what the underwriter tells us to do, so we have to do it. So you have this sort of bootstrapping process. And unfortunately, we really haven't seen that in the world, except for a couple of narrow examples, particularly when it comes to data breach.

Now, why is data breach such a powerful example? Why has there been this growth of market solutions? And that's because government has defined a liability point. There's a discrete point where companies feel harm and so once you have a discrete, quantifiable liability model, it's not an actuarial question, it's simply a mathematical question. What are my losses? And once you have losses that you can define, then you can start to insure them and then we can see whether or not the market cares.

Finally, I just wanted to get back to Suzanne's last point on organizations. And I think this is key that I will know that DHS has been truly successful when they successfully participate in an ad hoc process; when they engage in a crisis, they set up an organization and when it's done, they take it apart again. Because that, I think, is the true path forward and I think the ideal model is Conficker. You have a bunch of different companies getting together, working to solve a problem, taking themselves apart when they were done. And if you haven't read it, they -- a brilliant thing -- hired a consultant to tell their story. And so there's actually a report that you can find out what a model of an ad hoc organization can and can't do.

MR. WALLACE: Thank you, and we will return to Conficker. I think one of the arguments that was made was that the success of that was due to the lack of government involvement, which is in itself an interesting reflection.

But, Suzanne, there are few points that you may want to pick up on, but just to frame them. One of the things that DHS was mandated to do was take forward the voluntary program to, I think the Executive Order says, encourage adoption of the framework. And I think NIST is suggesting this is more of a process rather than an adoption thing now, but that leads into this question of incentives, some of which will be market-driven, but some of which actually require government initiative. Can you give us a little bit more detail about how you see this process working beyond February and what DHS plans to do?

MS. SPAULDING: Yes. So the voluntary program is being stood

up, as we speak, and we're putting that together and will be stood up as the framework is released early next year.

And it begins with just making sure folks are aware of all of the things that we already have to offer that can assist companies that are looking at this framework and trying to use it to improve their cybersecurity. You know, you used the word "adoption." A lot of people are talking about adopting the voluntary program. Jeanette, you know, has this wonderful image that you will wrap it up in a little blanket and take it home, you know, and take good care of it. And there's been a lot of discussion about what does it mean to adopt the framework. And that's part of what this discussion between now and the final framework in February, frankly, will inform is, you know, what does that mean to either implement or adopt?

I will say that at the moment, the way I'm thinking about this is I would substitute the word "use." So use this framework to inform your risk management decisions and the actions that you're going to take to improve your cybersecurity. And so, as we think about our voluntary program, what does that look like? It is, how can we help? Again, we have a particular focus on small- and medium-sized companies, but not an exclusive focus. There are a lot of large companies that need this as well and a lot of small companies that are doing it just great in a very sophisticated way.

But how can we help companies that look at this framework and translate this list of best practices into effective action that increases their cybersecurity in an effective risk management way? So we have a number of

things underway that are related to the work we do on threat.

The framework and the work under the Executive Order and the NIPP are really about what can the Homeland Security enterprise do? Which is why I think the focus was less on how to address the threat, but that doesn't mean -- and I know you know this -- that there isn't an awful lot of work being done at the federal government level to address the threat in a very direct way.

But a big part of it is informing people about the threat, making sure that there is situational awareness about threats, vulnerabilities, and mitigations. And so, Bobby Stemply, who's here, who's our acting assistant secretary for cybersecurity and communications, and her shop within NPPD have a number of things underway that will be an important part of the voluntary program. So, they have an information chairing program, Cybersecurity, Information, and Collaboration Program -- did I get that right? Wow. CICP, which is a very effective and collaborative way in which private sector entities can enter into arrangements with DHS to make sure that they are getting threat information and vulnerability and mitigation information.

Cybersecurity resilience reviews which help critical infrastructure owners and operators to assess their vulnerabilities and assess their resilience posture, how resilient are they, again, as a way of informing that risk management decision-making.

If I don't look at this I'm going to forget all of the things. One of the challenges, I talked about trying to get unclassified information out as much as possible and we work hard at that every day. At the end of the day there may be

some classified information that we aren't able to declassify that would be valuable. And how do we get that out broadly?

So, we are putting out something called Enhanced Cybersecurity Services where we work with commercial cybersecurity providers or consolidated cybersecurity providers who develop their own ways of handling classified information that we would give them -- government furnished information -- and using that information to provide enhanced cybersecurity services to people who sign up. So it's a way of getting that information to be valuable and to be able to be used by wide range of users who don't all have to get clearances and have classified facilities.

All right? So you give it to a provider who then can use that information to give you enhanced cybersecurity services. That's an important effort we have underway.

Continuous diagnostics and monitoring, which we're doing at the federal level across the dot-gov, for which we have the lead, the civilian government departments' and agencies' cybersecurity. This is an automated way of assessing their networks and systems and helping the government folks make risk-based decisions about allocation of resources to protect their systems.

What we learned from that, because that's obviously a lot of experience and data that we're gathering at the dot-gov level where privacy concerns are mitigated by the banner and the fact that federal employees sort of waive a lot of those rights when they log onto their computer. We get a lot of that information. We can then use that and get that back out to our critical

infrastructure owners and operators.

And then, finally, we have private sector folks who sit on our operations floor, our National Cybersecurity Integration Center, the NCIC. The NCIC is our 24/7 ops floor and we have private sector folks with clearances sitting on that floor who help us assess threat information that we get and help us determine what we need to get out more broadly and how to get that out more broadly. And we do that on the physical infrastructure side as well.

So that will be those things that we're doing and similar activities underway in department and agencies today, those will all be a critical part of the voluntary program going forward.

On the incentives, what we provided to the White House and the other departments was suggestions for further analysis and we are now doing that further analysis. And some of these will be near term, so right away we're talking to the folks across the government who do have grants programs to say how can current grant programs be oriented in a way that could help promote adoption of the cybersecurity framework, right? So, are there grant programs out there now where this could be a factor?

Expedited security clearances or other provisions, access to technical assistance that we provide, can we prioritize that for people who are trying to implement the cybersecurity framework, at least during steady state? Obviously, during a crisis you go where the crisis is, but during steady state, could we give some priority to them?

So those are the kinds of things that we're looking at now that

could be sort of near term; the insurance, ways in which the government might be able to promote a more robust cybersecurity insurance market is going to be a longer term effort, but it's something we've had a number of workshops on already and will continue to have workshops on.

What other key points am I leaving out here, Jeanette and Bob? So there's a near-term and a long-term. The goal of it really is to assist in the voluntary use of this framework to improve cybersecurity across the board.

MR. WALLACE: And we will come back to this issue of the voluntary nature of the program, which is clearly very important to the government. But just before we do that, Richard, Suzanne's outlined an enormous amount of work, which I know is being taken forward by the team at DHS, which is working extremely hard. But I think it's fair to say that traditionally DHS's involvement in this space hasn't always been welcome by the private sector. Correct me if I'm wrong.

But I also think it is true to say that some of these things will prove more important than others. And so, given all of that work going on, what do you think the private sector really wants? What's most important to deliver from that menu of activity?

MR. BEJTLICH: Well, that's a good question. Let me just give the government two forms of praise. The first one is, DHS, specifically the ICS-CERT sending -- ICS stands for Industrial Control Systems, CERT is Computer Emergency Response Team -- the fact that there is a group funded by DHS that can go to a critical infrastructure provider, such as a power plant or water plant or

something like that, and show up and deal with serious intrusions is wonderful, honestly. It's the only model that tends to work, I think, for large organizations because no single company, unless it's sufficiently large -- and we're talking on the scale of maybe 100,000 people or more -- can fund a team with the right capabilities and all of that to deal with advanced intruders.

So the fact is that the way that you deal with that in other places is you have a central team that goes out when needed. So the fact that ICS-CERT is doing that for their critical infrastructure providers now, and they write about what they find and it's public. You can see the number of times they've gone out, the number of incidents they've dealt with, I think that's wonderful.

The second thing, and it's not a DHS initiative, but it's the FBI, the FBI has a program of third-party notification. In other words, they send agents to, in many cases, literally your door. They knock on your door -- you, as a large company or even a small company -- and say, excuse me, is this your data? And you look at it and you say, yes, that is my data. Where did it come from? And they say, well, we found this on a server in Romania and it means you have a serious problem. And that can kick off an entire universe of response action, and it's been going on now for the last six or seven years and it's just been a wonderful, wonderful program.

As far as what the private sector wants, I think the private sector, in many ways, wants to be left alone, as you might imagine. But, more or less, they want certainty. They want to know, okay, what is it we're supposed to do and then let's figure out how to do it.

I think the private sector also would like to know when there are very large classes of threats which could be told to them. They would change their risk equation. For example, let's say two years ago the government learns that an entire class of enterprise product -- like a VPN token that used to access a remote site securely -- the government learns that that infrastructure can no longer be trusted because it's been compromised by agents from China. A solution like that that is used in thousands of companies, not just in the U.S., but we'll talk -- probably hundreds of thousands of companies across the world, to know that you can no longer trust that infrastructure, that's a big deal.

Now, to reveal that doesn't necessarily tell a private company or it doesn't reveal the identity of the private company that suffered that intrusion because that's the other biggest fear that the private sector has. They don't want to be called out and said, hey, Company X, you've been compromised. I'm going to tell the world about it. But the fact that you could share this very, very, very important information that says, private sector, you can't trust that anymore, come up with a way to mitigate that risk until there's a patch, there's a fix, whatever, I think that's a whole class of activity that the private sector would like to know as well.

The type of intel sharing you often hear from -- and I kind of dodged that question when you first asked it -- the private sector isn't necessarily that interested in sort of IP addresses and domain names and things like that. I mean, Mandiant provides that, Symantec provides that, Trend Micro provides that -- you can get all that stuff from other private sector entities. I think it's these

sorts of grand problems that if the world knew, it would really rock your foundation. I think that the private sector would like to know about that.

MS. SPAULDING: So I will say, for those who are interested in that kind of information, that going to -- so you mentioned ICS-CERT, and thank you for that plug. I appreciate that. They do outstanding work; award-winning work, I will say. But there's also US-CERT, which is their sort of companion computer. The CERT actually stands for something slightly different, doesn't it? Just to confuse me. And they post on their website vulnerabilities that they learn about and things, you know, maybe not quite as grand as you've described, but pretty close, and oftentimes, usually, ways in which to mitigate that.

So that is posted and when I travel around the country and I talk to CSSOs in companies, particularly, again, that sort of medium-sized company, smaller- to medium-sized companies, they talk about going onto that website on a regular basis and how helpful that is, so I think you're exactly right. It's the kind of information that no company wants to put out there with their name and it's one of the ways in which we can actually add value is to be a central clearinghouse where that information can come in, be sanitized, and be distributed much more widely and broadly, and so that is an important role we can play.

MR. WALLACE: And I think I'm right in saying that you're acting secretary said last week -- was encouraging Congress for legislation that provided liability protection. Can you just talk a little bit more about what the government is now asking Congress to do?

MS. SPAULDING: So, what the government is really asking Congress to do is to pass legislation. We had sought and would love to have comprehensive legislation. We recognize now that we may have to settle for some pieces of that legislation. And I think what he was talking about is a particularly important piece, which is information sharing.

You know, I've talked a lot -- we've talked a lot about the ways in which we need that bidirectional information sharing. We have information valuable to the private sector. The private sector is seeing threat information and threats that we're not seeing or in a different way than we're seeing it. We need that information from the private sector so that, again, we can get it out more broadly. We need that bidirectional information sharing.

There's uncertainty in the private sector today about the legal authority for them to provide us that information under certain circumstances. And so what we really need, the greatest protection against liability is clarity in the law. If you have very clear delineation of who can provide what information to whom, under what circumstances? You know, you're going to be able to make sure that you're abiding by the law and avoiding liability.

In addition, in order to really reassure the private sector and get that information flowing the way we need it, we may need to have some very targeted, very narrow liability protections. I say very narrow and very sort of limited because liability is generally imposed for very good public policy reasons. It is designed to encourage appropriate behavior, about protection of privacy, for example, in customer information, et cetera. And so you want to make sure that

as you're eating away at that liability, that you're doing so in a way that is narrowly crafted and doesn't have unintended consequences.

MR. WALLACE: Allan, you've done some think on this, your thoughts?

MR. FRIEDMAN: So information sharing is a lot like cybersecurity in that if you try to treat it as a broad issue, particularly at a legal level, you're just going to miss the problem. There's a huge difference between plugging my IDS into your IDS and having our systems share from each other. And to CSSOs having drinks together and saying, hey, people are going after this new source of value, you should check your business unit because you're in a separate thing.

And there are a number of different issues and inbetween you have different types of data, you have different organizational roles, and you have different policy goals as well. One framing of information sharing says, really, it's just crowd sourcing, right? Because there are different types of attacks that hit different people, so if everyone just shared the types of attacks that are coming at them, that's essentially just a global censor network.

That's one perspective and there's certainly social value there. Another approach is to say, listen, we need information sharing to make markets work because markets thrive on information. If you asymmetric information you're going to have a market failure. So that's more of a transparency story. And there's, as I was saying, a huge challenge between reconciling transparency and accountability. And that's one of the dangers of a blanket liability protection, is it is one of the few carrots the government can offer, right? Liability protection

makes private actors better off, it helps incentivize certain types of risky behavior.

What liability are we trying to protect? A lot of people say, well, I'm worried about sharing information because of anti-trust issues. Now, I'm not an anti-trust lawyer, however, if the anti-virus community can share virus signatures for 15 years and not raise any flags with DOJ, then surely we're allowed to talk to each other about IP addresses and not have that challenged.

So we need to think about what the goals are and what type of information sharing before we end up with a blanket thing. So I think the approach is exactly right. We may say there needs to be targeted style of information sharing. There also may need to be certain other types of liability protections. So, for example, Richard says, listen, we're doing a lot of information sharing in the market already. Companies will bring in security service firms and because they may work with a host of different companies, they see a lot of different threats. The challenge is, what are they allowed to share with their competitors, just from a contract prospective. Or if they're really working closely with their customers, what have they signed that prevents them from doing internal knowledge management? And what can we do to make sure that we have maximum learning inside the private sector before we start throwing public sector solutions around?

MR. WALLACE: Learning is a key theme. Allan, you raise it yourself. It is also a key theme in the Executive Order. You're mandated to do a lot of studies and presumably learn from them. Just before we move on to questions from the floor, I wonder if you could just give us a sense of what you

have learned, both in terms of who does what within government -- which is one of the key things in PPT, but also in terms of the requirements of different sectors.

One of our Brookings colleagues, Ralph Langner, who is an expert on industrial control systems, is very vociferous about the fact that the challenges he faces in his work are very different from those, for example, faced by financial institutions and NDGE or (inaudible).

What has the government, and specifically DHS, learned as a result of this process and how is that changing the way you're doing business?

MS. SPAULDING: So I probably learned a lot more than my very expert staff, who probably knew all of this before, but there have been some interesting things that have been both sort of driven home and reinforced. And insights that we've gained by virtue of this incredibly collaborative and consultative process that we've gone through. And one of those is -- and this is sort of a di-guess -- but, you know, obviously we talk a lot about, and then there are critical infrastructure owners and operators, or the private sector. And what you really appreciate when you go through this process and you're trying to achieve some kind of, you know, not quite consensus, but a good strong support for the direction in which you're moving is that there is a wide range of views, as we talked about up here.

There are among critical infrastructure owners and operators and among the private sector, they do not speak with one voice. So that's an important -- it may seem obvious, but it really is an important thing to understand

and it helps to inform you approach then. It reminds you that there's no one-size-fits-all. For example, everybody comes at this from a slightly different place, that some are more sensitive to the value of having good cyber hygiene among their vendors, suppliers, companies they may want to take over or otherwise establish relationships with, who are going to be connected into their networks and systems. And other companies that really aren't that interested. They assume that everybody around them is a mess from cybersecurity and they're going to take of their little castle, you know, just as one example.

Those who insisted that we acknowledge that the private sector should only be expected to only appropriately go so far and that there's a delta and government needs to fill that gap. And those in the private sector who were insulted at such a notion, that somehow they were unwilling to rise to the occasion on cybersecurity. So that was a very interesting and important insight.

Again, as you noted, that not all sectors are the same. As we get into the water sector, you know, the old adage of, if you've seen one water treatment plant, you've seen one water treatment plant. They really are incredibly different and they're very different in the cyber dependence.

The fact that in the electric sector it is surprisingly resilient. We think of it as being very cyber dependent and, in fact, they rely heavily on network systems for load shifting and all the rest of that. But what's interesting is that those things were tacked on because most of the electric grid infrastructure was actually built in the '70s and those sort of mechanical, physical redundant things are still there to fall back on, in the event of a cyber incident. And so, in

many parts of the electric supply chain -- generation and transmission, et cetera -- there's great resiliency, more than you would have thought.

The important lesson there is, it's nearing the end of its useful life. It is going to be upgraded, replaced with much more efficient, smart grid kinds of things, and will be much more cyber dependent. And we have to know that today's resilience that we rely upon is because of things that will not be there tomorrow. So those are just a handful of some of the many things, insights that came out of this process.

MR. WALLACE: Rich and Allan, I'd like to pick up on what the private sector and others have learned in the course of the last year and how that's changing the environment, but I'm also quite keen to get some questions from the floor, so perhaps we could pick that up as we go along.

There should be some microphones floating around. As ever, please keep your questions short, please end them with a question mark, and I assume there will be a number of questions, so let's take two or three together and then we'll answer them as a panel. Right here in the aisle.

MR. PERDY: Hi, Andy Perdy from Wallway. I'll forego my four comments and ask a question to Ms. Spaulding. The intersection between the revisions of the NIPP on the one hand, and then this cybersecurity framework which is focusing on what individual organizations need to do, on the other. Where do you see and how do you see the sector-specific plans, the sector risk assessments, being improved to help address the priorities of the Executive Order?

MR. PEARL: Mark Pearl, Homeland Security and Defense Business Council. Allan didn't address the issue of legislation, so I'll throw it then to Suzanne and Richard. And it comes in the form of, do you think legislation is necessary, whether or not it's going to get passed in the nature of this Congress?

And, Suzanne, this simple question. Knowing what the reports are going to be coming out and deadlines and February 12th of 2014, what is keeping you up at night in terms of what you've now learned?

MR. WALLACE: And one last question in the back.

SPEAKER: Picking up on the legislative question, part of the government is under attack for collecting too much information and another part of the government isn't getting enough. How is that debate impacting your ability to articulate policy on the Hill?

MR. WALLACE: So plenty there, chomp on that. The National Infrastructure Protection Plan intersection with CSF, both aspects of this work and how do those things come together at the sector level?

Legislation, is it necessary? One of the things that the Executive Order asked DHS to do was identify with sectors where later on regulation may be required. And it would be interesting to hear how that -- at what point will you know whether that is required. And the S-word, Snowden, it hasn't been mentioned so far. One of the things that has changed the environment and the reason why we don't talk so much about China is because this has completely changed the environment. How, if anything, has that effecting consideration of critical infrastructure? Suzanne?

MS. SPAULDING: Great. Easy questions. So, on the sector specific plans, I met recently with our new Cyber Deputy Under Secretary Phyllis Schneck, who's fabulous. We're incredibly fortunate to have her on board. She comes to us from years in the private sector, but also with very strong technical credentials, and she's going to be a terrific addition. And she and our assistant secretary for infrastructure protection, Caitlin Durkovich, and I met with the Cross-Sector Coordinating Council, and I talked with them specifically about this issue and that I need them to very quickly pull together. The Cross-Sector Coordinating Council, for those of you who don't live and breathe this every day, is made up of the leadership of the 16 sector coordinating councils, which are self-forming, private sector groups that come together to help advise the government and collaborate with each other to enhance the security resilience of critical infrastructure.

I talked with them about the need to move quickly on the sectors specific plans. And again, I think where we're likely to go in -- and it will vary from sector to sector for all the reasons that we've already talked about up here. But where we're I think we're likely to see the sectors start is, again, coming up with ways in which they can get the word out broadly, within their sector, about what the framework is and the resources available through the voluntary program to help folks use that framework to improve their cybersecurity. And, to come back to us, with suggestions on ways that we and they can help more companies get to a point where they can actually use that framework to improve their cybersecurity. So that's what I see initially. I think there's a

potentially valuable role that the sector coordinating councils can also play in getting us feedback. Both in terms of how's it going, where are the challenges with implementing this, with using this, so that -- again, this is every year, it's going to be updated and improved and how can we do this better next time around? And, also, what impact is it having?

So, who is actually implementing what kinds of fixes and what are you seeing? And they can, again, fill that role of kind of anonymizing that information and getting that back to us. So those are some of the ways I'd like to use the sector coordinating councils.

On the legislation, again, I focused on the information sharing in response to the earlier question, but we need those privacy and civil liberties protections and I'm going to circle back to that on the last question because I think it's an important part of the way it's informing the debate.

At DHS, we really need some greater statutory clarity around our authority, so that we can do the things that the Congress and the American public expect us to be doing, both in the dot-gov and in assisting in the dot-com world. And to make that more efficient and effective, particularly under FISMA, the Federal Interagency Security Management Act. And to streamline our hiring authority so that we can bring in the best and the brightest to build the kind cyber skills workforce that we need. So those are some of the key areas at building in that privacy and civil liberties.

On the regulatory front, I want to emphasize that one of the things that the Executive Order calls upon departments and agencies to do is to

streamline their regulatory authority. So, when it says look at your current regulatory authority, see how that regulatory authority can be used to promote the cybersecurity framework, but look at way in which we can harmonize across -- right?

So, particularly for sector who have multiple regulatory regimes that may apply, you know, how can we streamline this so that you're not responding in different ways on the cybersecurity front -- differently to different agencies or in the same agency under different regulatory regimes? So streamlining is a really important part of that.

The administration has made it very clear, they are not looking for new regulation. They're not interested in moving on the regulatory front. All of our energy and effort is being put on voluntary adoption of this framework.

In terms of what keeps me up at night, it is knowing that this afternoon, tonight, tomorrow there could be a cyber incident with some very significant consequences. And there is that sense of urgency that's really hard to -- when what you have to deal with is stakeholders all across the country, thousands and thousands and thousands of critical infrastructure owners and operators, the federal bureaucracy, state and local governments, getting all of that machinery to mesh, you know, it's a fairly cumbersome process. It is not that agile, innovative, wonderful utopia that I describe and so that sense of urgency is very hard to translate into fast action. But we're doing our very best. Those were aggressive timelines. As I say, we met them and we're moving forward with lots of help from folks.

The debate as a result of Snowden has, in fact, become more complicated and it's made it all the more important that we help members of Congress understand all of the things that we do to protect privacy. DHS has perhaps the only, but certainly one of the first, if not the only statutory privacy security officer. And that means that statutory is important because it gives that person a degree of independence. And we have, within NPPD, where we lead the cybersecurity work for the department, our own privacy security officer who reports to the department's privacy security officer, but is there with us on a daily basis, who has helped us to write privacy impact assessments for all of our programs. Those privacy impact assessments are all publicly available.

And so we have this privacy and civil liberties baked into the work that we do. And this debate has actually given us an opportunity to really help folks understand why we do that, how we do that, and why it's so important.

MR. WALLACE: Under secretary says Snowden gave us sort of an opportunity. It's an interesting headline.

Allan, legislation is clearly something that the administration is keen to avoid for fairly obvious reasons. Is that realistic? I mean, can we get to the end of this process, not that the process will ever come to an end, arguably, but can we achieve what we need to achieve without looking at some kind of regulation?

MR. FRIEDMAN: So, you know, the last major cybersecurity bill to pass Congress was in 2002, and it only described issues relating to the federal government, it was FISMA, which woefully outdated and needs to be updated.

And the challenges when we start talking about regulation, there are some low hanging fruits out there, which I think aren't politically controversial, fairly straight forward from a policy prospective. You know, there's money on education, better research, probably a little bit of legal reinforcement on things that are unclear statutorily, in terms of authorities. And there's some related forks, Washington has been reminded publicly that federal IT acquisition is a mess. Conveniently, it's in the papers, so it might be a good time to revisit that question, particularly in the light of security, as well as some of the ongoing classification system and over-classification, under-classification. Those are all sort of peripheral areas.

The question about regulation, I think, it really does come down to we're at a preliminary stage at the moment and, in some ways, this approach of let's see what the private sector is willing to do? We've made it clear in the Senate particularly that more aggressive regulation could pass and that probably, in an ideal world, will help certain actors and industry associations that are strongly outspoken against legislation and regulation work very hard to demonstrate that they don't need it.

So, in some ways it's nice to have a club behind one's back while you're offering a present.

MR. WALLACE: Richard's sudden impact -- Mandiant was leading the charge on exposing Chinese commercial espionage. And then the story shifted to Iranian DDoS attacks. Over the summer those news stories had gone away, the journalists were focusing on something else. Do you think that

this is going to impede efforts to improve cybersecurity, or do you think that effort is happening behind the scenes and that in itself may be helpful?

MR. BEJTLICH: So Snowden definitely will have an impact on this problem. There was a great piece in *Newsweek* a couple of weeks ago -- *Newsweek* isn't in print anymore, it's online, but the cover of the online edition was Snowden's impact dealing with China. And as far as dealing with security in general, there's a general principle that the more you try to defend, the more information you need about what's happening. So, if you need more information about what's happening, it has to come from somewhere and that usually comes from greater visibility into ones' networks, one's systems, what activity is happening on those systems.

That runs completely contrary to privacy interests. So, as an incident responder and someone who has done forensics, someone who has written books on forensics, that sort of thing -- when I read what was required in the security part of the NIST framework, I said, oh, okay. All right, I understand what all of this is. And then when I went to the privacy side and I read, oh, this data that I'm collecting to try to figure out what the bad guys are doing, I have to be careful not to touch PII and if I do, I have to destroy it. And all of these things, suddenly, I said, wow, this is going to be very difficult.

My firm wrestles with this problem right now. There is lots of data that we would love to keep for further analysis, for future investigation, that we have to destroy simply because we're not allowed to -- in order to protect people's privacy, which I think is probably good, but there's no question that it

does make it more difficult in some ways to defend yourself.

It's honestly still an open question whether you can monitor your own network because there's something called the Wire Tap Act. And you get different opinions about whether or not that's true. If you were all lawyers, which -- well, I couldn't imagine a room this size with all lawyers, but.

MS. SPAULDING: A great big secret?

MR. BEJTLICH: Maybe you could. I don't know.

MS. SPAULDING: Wouldn't it, Harvey?

MR. BEJTLICH: A good number --

MS. SPAULDING: Yeah, it would be great.

MR. BEJTLICH: Actually, we had this discussion when we met. A good number of the lawyers would say, you actually can't monitor your own network to look for intruders. It is up for debate. So I would like, in terms of legislation, it would be nice to have legislation that says, no, you can monitor your own network in order to defend yourself. I mean, right now we have to use various exceptions to the Wire Tap Act to do that.

The other area, by the way, I think we need legislation -- just to be very clear about that -- is the liability aspect. The President's Executive Order can't grant liability. There's no real way he could do that without legislation.

MS. SPAULDING: Can't grant immunity.

MR. WALLACE: I would love to turn this into a legal discussion, but I'm going to go to open some wider questions. More questions from the floor, please? Harvey? SPEAKER: First of all, thank you to Brookings for

putting together a really outstanding afternoon with this level of expertise. It's so nice to see someone with such a strong Brooklyn accent go as far as a moderator. You've really done a wonderful job.

MR. WALLACE: I've been practicing.

SPEAKER: I guess I wanted two questions. I drilled down a little bit more. I recently was on a panel with the issue of sharing information and I had some bankers and some accountants. And we had always put forward the anti-trust shibboleth was not a barrier to sharing information, that was our official sort of ABA position when we were looking at it, so I'm kind of curious. Their position was that if they started sharing information, let's say about a vulnerability concerning some software and it was shared that everyone who stopped using that software have asked for the appropriate patch, but the software user might have a cause of action that they were fearful of.

The second issue was that we always thought that the Department of Justice had mechanisms by which you could ask to share the information and therefore not be worried about anti-trust violations because it's going to be DOJ that does it, not Homeland Security. It's going to raise the anti-trust sort of prosecutorial arm. So I'm sort of curious from the private sector, what has been your experience? Do you see that when you share information? Are these concrete things that you -- you said you want some immunity, but is there something else going on that the government should know so they that they could be able to target what that problem is?

And then the second question is, which is Brookings, so it's

always a policy question, is that, yes, there is the enforcement, but one of the big issues that we're thinking about inside the structure of government is, is it appropriate for Cyber Command and NSA to be dual-hatted? Or should we be separating those two functions?

I think Suzanne might be slightly constrained in her ability to address that issue, but the other three people on the panel, it would be interesting to hear your sort of assessments. And, again, thank you all and Suzanne thank you for what you've done and all the sacrifice that you do in this public service. It really is quite wonderful.

And, Mandiant, the only footnote I'll take is that I think the first entity that actually named and shamed China and Russia and Iran was the Economic Espionage Report put out by NCIX, so that the government was the first namer-and-shamer in that particular context, which is quite fascinating.

MS. SPAULDING: Which Harvey was involved with.

MR. WALLACE: What is also fascinating is Mandiant seemed to have taken the credit for the exposure.

MS. SPAULDING: Was that before the Monk Institute in Canada, they were early namers in this?

SPEAKER: Well, the Monk Institute, that was GhostNet.

MR. BEJTLICH: That was Ghostnet.

SPEAKER: But it wasn't an official ID.

MR. BEJTLICH: They didn't show the building, that was the difference.

MR. FRIEDMAN: And their Cambridge co-authors were livid.

MR. WALLACE: Richard, first, to pick first question.

MR. BEJTLICH: To (inaudible), yeah.

MR. WALLACE: And I know Allan has some thoughts on the second question, you may also have your own thoughts.

MR. BEJTLICH: Sure, so Allan mentioned that -- and I think Suzanne may have mentioned as well -- that information sharing has many different dimensions. Currently information sharing is done in a few ways. It's done through people who trust each other, who may have worked together, through mailing list, through sort of informal ad hoc networks that function very, very, very well.

Then there are some networks that were set up via contract or NDA or other sorts of constructs that DIB, the Defense Industrial Based group that set this up has that sort of structure. You have the ISACs, the Information Sharing Analysis Centers, there's information shared at that level. But you don't necessarily have, say, a consortium of auto makers that would share information or a consortium of very, very closely aligned businesses.

Now, you could say the ISACs do that.

SPEAKER: Or ISPs.

MR. BEJTLICH: Or ISPs or that sort of thing. But even then I don't think that's necessarily the concern. The main concern, I think, is if you're a private sector company, you tell the government, hey, we just got our clock cleaned and this is all the data we lost and here's how it happened and, you

know, go ahead and sanitize it and take it out to the world and protect people.

Well, that information is going to be subject to a FOIA request and when someone does that request and finds out, wait a minute, my company that I have shares in suddenly had this happen? Boom. That's the concern. So there's an extreme reluctance of private sector companies to go forward to the government and say, all this stuff happened.

What you'll get instead is, there was an attack because attack doesn't imply anything actually happened and there may have been some issues that involve these foreign IP addresses, do what you will with it, but if you ever want to get to the real nitty-gritty of, no, we lost a lot of data. The only people that are reporting that sort of stuff are typically in the defense industrial base. They have to do it by contract; they have to have hard drives with actual forensic evidence of what happened. You take that model elsewhere and it's going to be a much different problem, I think.

MR. FRIEDMAN: I would say in response to that, if an investor has to use a FOIA to find out that their company, which they own, suffered a material loss because of a cyber attack, there are a lot of other things that are broken and that, I think, gets back to sort of SCC rules and the voluntary guidelines, which probably takes us further afield of DHS's turf.

We've covered a decent amount on the information front, so --

MR. WALLACE: Just one way of achieving some of these information sharing goals is clearly CISPA which is being led by the House Intelligence Committee. And one of their highlights is there are different ways of

achieving the same thing, some of which not as popular as others. You've done some thinking on this, Allan. That, presumably, isn't your idea of what you would want to have in place.

MR. FRIEDMAN: Right. I think the challenge -- and this gets back to what we were saying earlier is that CISPA looks at information sharing as a single problem. And I think that we've tried to establish that they really are a lot of very contact specific questions, so one challenge is -- again, as a non-lawyer, it's always easier to say the lawyers are the problem.

You have very overly aggressive interpretations that, because they become -- they happen early and they spread and that becomes law. And I think the best example there is HIPAA where, if you read the rules, they're not nearly as strong as they were interpreted by the first wave of lawyers and consultants. That sort of constrained what was possible. So that's my worriness -- that having a resource inside the government that we can turn to in specific context can be very useful, as well as perhaps companies building in the importance of information sharing when they're writing their contracts with their security service providers, with their partners, and as the other organization model that I'd point to is the ad hoc organizations or sort of dynamic organizations like ACSC in New England, where you have a group of companies that said, we want to share information, let's write some NDAs between ourselves.

And you have universities, you have research companies, you have defense firms all getting together, figuring out what they want to share and

need to share on a dynamic, real time basis. And I think that's a successful model that gets us away from needing this one size fits all legal approach that potentially offers too much liability protection too quickly.

MR. WALLACE: NSA Cybercom?

MR. FRIEDMAN: Again, huge kettle of fish. I think the challenge is, from a broad prospective, how do you restore trust? And this gets back to this privacy debate, probably one of the biggest challenges for the American cybersecurity world is -- the NSA was at an all-time high of good relationships with the hacker community. They had great relationships, they were regular speakers, they were sharing information, they were bring people with long hair and t-shirts -- they weren't giving them clearances, but they were actually saying, let's work with each other.

And that's been broken. And so I think from a pure cybersecurity standpoint the question is how do we work towards repairing that? And part of that means if a defense establishment has been unwilling to demonstrate it will prioritize anything other than intelligence collection, then their leadership has to find ways of bringing in other interests -- American diplomatic interests, commercial interests, trade interests -- and so you need civilian leadership.

MR. WALLACE: Richard, anything?

MR. BEJTLICH: Without assigning a value judgment, I think it will happen. You'll get a split. The question will be, will the new NSA director be a civilian, and I will say they're probably going to lean towards a civilian. Which will be appropriate.

MR. WALLACE: Will it make a difference?

MR. BEJTLICH: In terms of perceptions it may help a little bit. In terms of the way the agency actually works, I don't know.

MR. WALLACE: Suzanne, do you want to comment?

MS. SPAULDING: Nope.

MR. WALLACE: We've got time for one last question. Down here in the aisle.

MR. GARDNER: Alva Gardner, I work at the Pentagon. My question may be a little bit off the beaten path here, so perhaps it's appropriate that I'm the last question. My question is, as we begin to normalize how we look at our cybersecurity here domestically, what do you see as the feasibility and or challenges towards taking what we've learned and what we've done and instituting international norms?

MR. FRIEDMAN: A small question.

MR. WALLACE: I think, actually, this is a good opportunity for us to wrap up and I'll come down to give Suzanne the last word.

In some ways, the question behind the question is, how do we improve cybersecurity globally? Which is essentially a different way of saying, you know, how do we prevent threats from abroad affecting us at home? And I'd like to add in there a further question which goes to Suzanne's point about the threat of a serious attack could happen any time and that's what keeps her awake at night.

To take Allan's point, what we want to get to is a situation where

that is no longer the case, that this becomes routine. And so my question is, how long is it going to take us to get to that point? And what are the things that -- how confident are we that we're on the right track, Richard?

MR. BEJTLICH: I think you're not going to see a devastating "cyber" attack -- we'll put the quotes around cyber -- until it is aligned with some type of physical conflict. In other words, you can sort of think about a Timothy McVeigh scenario in cyber, an al Qaeda scenario, or some type of traditional military scenario.

So, the Timothy McVeigh is completely out of the blue. Nobody knew this guy was a nut. Lone wolf. He does something horrible. That's going to be fairly rare, I think, because plenty of people are like that out there now, but they just don't have the capabilities.

The al Qaeda example is, a group that tells the world that they hate the United States; whether we listen or not is another issue. And over the course of many years they ratchet up activity, you know, embassy bombings, ship attacks, until finally they put planes into buildings. So those types of groups are going to be active already in the physical world or maybe in the cyber world, so we'll see that coming, I think.

The final category would be, you have some type of military confrontation and there will be a cyber component to that. We've already seen that in other parts of the world where a physical problem bled over or people with cyber capabilities were motivated to participate. I don't think you're going to see a bolt out of the blue devastating cyber attack from someone we've never even

heard of before or some country that decides that they're going to do that sort of thing.

All of this stuff sort of -- anytime you hear talking about attacks at speed of light or it's going to be the blink of an eye, moving like electrons, no, these things tend to take the same sorts of progressive steps that you see in traditional conflict.

MR. FRIEDMAN: So, unfortunately, it is my belief that Suzanne's job is to stay awake at night worrying about things and all of her successors, right. We want the person in the job, just as all of her colleagues in DHS, who are responsible for other issues are staying awake at night because their job is to focus on it.

We will have succeeded when we're not talking about them at Brookings main stage and when people like Richard's company are making a lot less money because it's a competitive market and it's no longer something that we're willing to spend a lot of money on. So I think that's really where we need to get to. Sorry for both of you there.

The challenge on the international norms -- I think on the international relations side is a separate question, which I'd love to talk about, but one of the real threats -- and this is some work I've done recently -- is, as countries see this as a problem, it's important that they not see it exclusively as a national security problem that they themselves have to face independently. Because that's going to lead them to develop nation specific solutions and the United States is as guilty as many other countries on some fronts are saying,

we're going to throw up national walls and national security protections in a problem that requires a market solution and a market solution that is built on the international trade of information, technology, goods, and services.

And if we break the fact that that market has been built on international standards, we're going to have a cure that's far worse than the disease.

MR. WALLACE: Suzanne, final word?

MS. SPAULDING: Thank you and thank you for the question with regard to internationalization of this issue. It is obviously one that does not recognize borders very well, very often, and therefore requires that kind of international effort. Unfortunately, it is also an area where bringing an international consensus is really hugely challenging for all kinds of reasons, not the least of which is that the efforts at defense get mixed up with the efforts at offense, and the general kind of mistrust.

Cultural differences and areas of emphasis and the varying kinds of nationalist tendencies and what's important to control and what different countries think ought to be set free, et cetera. But it reminds me a lot of the challenges that we had in the early days of trying to come up with an international convention against terrorism, right? And when we realized that that was not going to happen, largely because we couldn't agree on a definition of terrorism, for many of the same sorts of reasons about nationalist interests.

We began to break it down into component parts where we could find agreement, right? And so we had an international anti-aircraft hijacking

convention, bombing conventions, and I think in many ways when we think about cybersecurity, we have to get much more granular in our discussion of it and we've touched on some of those ways today up on this panel.

But I think one of the interesting challenges for those of us who deal in cybersecurity is that we've got to both be comfortable taking that macrocosmic viewpoint that I started out talking about -- holistic, all hazards across physical, cyber -- and at the same time getting very granular; to remember that intellectual property theft is not the same thing as an attack on an industrial control system, that these are all different. That the nation state actor is not the same really as the activist and not even -- though closely allied sometimes with organized crime. That these are different things and we need to really have a granular -- and again, that reminds me of the proliferation days when we used to talk about weapons of mass destruction as if it was one thing. And it wasn't until we broke it down to nuclear, chemical, biological, radiological that we really began to be able to develop some policies and activities and programs around mitigating those risks.

And I think we have to do the same thing with cyber and I think it will help us in the international realm. Start small, start with things that we can build consensus around. Don't try to get the whole governance and norms around cybersecurity as if it is all one thing.

Are we going to get to success and when? I don't know when, but we're not all going to get there at the same time. You know, again, no one size fits all. There are sectors that are really leading the way. We have tremendous

relationships, for example, with the electric sector, all the way from the CSSOs, CSOs, CIOs, up to the CEOs who now take a very active role at that senior leadership level in the Sector Coordinating Council there and are very actively involved in working with us to develop and to strengthen their security and resilience, where the financial for reasons of experience, the oil and natural gas sector for reasons of events around the world that have opened their eyes, the chemical sector, in large part because of regulatory regimes there. These are some of the sectors that I think are really moving out quickly and where I think we will achieve some measure of success sooner than others.

Ultimately, how we will know when we've gotten there, I think, is that sense of unity of effort, which is what we're really looking for when we sit down with our stakeholders across the Homeland Security enterprise and we all have a clear sense of what our goals and objectives are and what we all bring to the table to help advance that.

We're not quite there yet, but we're getting better all the time. And panels like this are very helpful at advancing that objective, so Ian and Brookings, thank you very much. Thank you, guys.

MR. WALLACE: Thank you. I think that the take away to a certain extent is, success is boring, and that may be a good thing. But, you know, granularity will be part of that and this will be a process, rather than a big band event.

I'd like to end by thanking the panel very much. It's been a very interesting and very informative session. So, Richard Bejtlich, Allan Friedman,

and Acting Under Secretary Suzanne Spaulding, thank you very much.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016