THE BROOKINGS INSTITUTION

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY:

THE CYBERSECURITY FRAMEWORK AND BEYOND

Washington, D.C.

Wednesday, February 19, 2014

Moderator:

IAN WALLACE
Visiting Fellow, Center for 21st Century Security and Intelligence
The Brookings Institution

Panelists:

PATRICK D. GALLAGHER
Under Secretary of Commerce for Standards and Technology
Director of NIST
U.S. Department of Commerce

CAMERON KERRY
Distinguished Visiting Fellow, Governance Studies
The Brookings Institution

DEAN GARFIELD
President and Chief Executive Officer
Information Technology Industry Council

* * * * *

P R O C E E D I N G S

MR. WALLACE: Okay. Hello and welcome on behalf of the Brookings Center for 21st Century Security Intelligence. My name is Ian Wallace. I'm the visiting fellow for cybersecurity here at the Center. And today we are honored to have a distinguished panel here to discuss the new Cybersecurity Framework.

Essentially, this document represents the best efforts of the administration and, I think as we'll hear, industry representatives from the 16 critical infrastructure sectors to work together to address a threat which President Obama has called one of the gravest national security dangers the United States faces.

I actually look forward to hear more about how the framework was developed because I think that's going to be pretty central it its future. But it's worth taking a moment to remind ourselves that the voluntary framework owes its existence in large part to the failure of Congress to achieve consensus on cybersecurity legislation in the years up to 2012. And that in turn led to the President issuing an Executive Order 13535 on improving critical infrastructure, at the same time as his State of the Union address on the 12th of February, 2013.

And that, as the President has described it, set out to do three things: improve information sharing within the private sector, raise the level of cybersecurity across our critical infrastructure, and enhance privacy and civil liberties. And while the Executive Order contained a whole lot more than just the voluntary framework, it is clear that the framework has evolved as the centerpiece for the Executive Order and, by extension, the administration's cybersecurity policy, particularly as the vehicle for delivering the second and third of those aims, the raising the security while protecting privacy.

And according to the Executive Order, the framework set out to provide a prioritized, flexible, repeatable, performance-based, cost-effective approach to managing

cybersecurity risk. And, by the way, it had to be completed within a year.

Now, it can certainly be argued to achieve one important objective, even if not the formal one and that is to remove some of the political rancor from the debate. And that is in itself no mean feat. But the real question we're here to discuss today is whether the framework is going to make us any safer. And wrapped in that are some pretty fundamental questions. You know, what is the framework? How is it meant to work? Will it be adopted? Even if it does, will it be sufficient to deal with the greatness of the threat that the President described?

To get to grips with this, we are very pleased to be joined by the very man who was charged just over a year ago with delivering that framework, Dr. Patrick Gallagher, 14th director of the Department of Commerce, National Institute of Standards and Technology, NIST. And alongside him, Cameron Kerry, now the Ann and Andrew Tisch distinguished fellow in the Governance Program here at Brookings, but previously the general counsel and Acting Secretary of the Department of Commerce. And Dr. Dean Garfield, the present CEO of the Information Technology Industry Council. I'm not going to take too long over bios. I think you've got those, but just to recap.

Pat became a NIST director in November 2009, also serves as the Undersecretary for Commerce, for Standards and Technology. He joined NIST in 1993 as a research physicist, having obtained his PhD from the University of Pittsburgh, to where he is due to return later this year, having just been elected as their new chancellor.

Cam joined us at Brookings in December, affiliated with the Center for Technology and Innovation. He's also a visiting scholar at the MIT Media Lab. He became the general counsel at Commerce in May 2009, working across Commerce's bewildering range of legal issues. And before that he was a lawyer specializing in, amongst other things, telecommunications law.

And Dean became the president and CEO of ITI in 2008, a position representing the tech sector in Washington and around the world, in fact. And previous

to that he has held positions at the Motion Picture Association of America and the Recording Industry Association of America. A fantastic CV of fun jobs to be doing, I'm sure.

So, I will begin handing over to the three panelists just to give some short remarks. Then I will lead a bit of a discussion and then pretty quickly we'll open it up to the floor and give you the opportunity to ask some questions. I would ask you to keep your phones switched to silent. Feel free, however, to Tweet or e-mail. The hashtag we're recommending is #NISTCSF.

So, Pat, thank you very much for joining us. Congratulations on the framework. Even among those people who've been critical in the past, have been I think universally complimentary about how the process is run, and that's a testament the way in which NIST has gone about it. So well done on that.

Just to kick off, perhaps you could start by telling us what the framework is, how it's meant to be used, and then touch on the process for how you and the industry developed the framework. And then explain to us why this is going to do what the President wants and make us all safer.

MR. GALLAGHER: Okay. In just a few minutes, right?

So, first of all, it's great to be here. Let me start with the what is the framework question, but answer it in a non-typical way because you're probably expecting me to lay out how it's structured, what the key parts of the framework are. And a lot of you have probably taken a look at the framework, but let me actually do it from a different perspective which is some of the key attributes.

First of all, the framework is a living document. One thing to really keep in mind is it is not static. So when we ask the question is this framework going to solve the problem, you're really going to get to a very different answer, which is, does just this ongoing framework process continue to adapt and work for this? This is a very fast, dynamic area and it's important that you understand that this is an ongoing process.

The other part about the framework that was critically important is this is a market response. What do I mean by that? You characterize this as being a failure of Congress. I actually don't view it that way, but a discussion in Congress was rather naturally focused on questions of authority, and, therefore -- so it already had a lens already on the problem in terms of what the solution set was.

What we're saying here is that one of the best ways to address cyber risk is to have the private sector organizations and companies and technology providers and all the others come up with a set of best practices that are maximally aligned with the way those organizations run. And for that to happen it had to be basically a document that was a product of industry. So what NIST did was actually adopt an approach that we use very often in standards setting to act as the convener and to act as a facilitator, if you will, of a very broad multi-stakeholder -- you know, getting the band together to sort of have that critical discussion.

But, you know, because it had to be aligned with business, it means that the framework in the end was both what you would expect and, I think, something new. And the what you would expect is the set of controls and technology solutions and standards that were drawn from best practices across all the sectors. We call that the core. And that's in the framework in a very indirect way because it points to a whole set of standard and reference standards. And that's where a lot of the meaty details are.

And the other part of the framework was really a structure to put all of those things into practice and, in particular, to integrate those practices into the way the organization runs. And so it's specifically designed not only to talk to the technologist within an organization, but to talk to the leadership, and so it's designed to align with risk management. It's designed to provide tools like profiles where you can basically self-assess against all the various functional areas that constitute risk management for cybersecurity. And it was also designed to look at your maturity as an organization because one thing that's very important is that like many other risk mitigation behaviors in

an organization, you get better. And that was important to acknowledge that.

And some have drawn the analogy with safety management. You know, you would start things by implementing certain rules and doing things in a particular way, but in fact what you're after, in a higher maturity, is an ability to recognize risk and be adaptive and to be more proactive. And so the framework embraces some of that as well.

So that, for me, is what the framework is. It's both the practices and the structure with which to support implementation. And I think the reason this is promising has to do with those attributes. The fact that it's owned by the stakeholders who have the most to gain by managing cyber risk. That it can be aligned with business practices and integrated with the other types of risk management that organizations do. And the fact that it is itself dynamic and adaptive to the changing way we will use this technology and the way the technology itself is unfolding.

In terms of the process -- by the way, it's not over. We met the deadline of one year that was given in the Executive Order, but we've stated from the beginning that for this framework to make sense, what we're really talking about is kicking off a continuous process. And so the finish line here is not being done, it's being normal, where this is just part of the breathing and operating that we do routinely. And so what we're looking for is a normalcy of operation, not an endpoint.

And the process has been one that was based around industry ownership and participation. We used every trick in the tool book we knew how to do by putting things out publicly. No one, I think, was surprised by the final shape of the framework. It was multiple workshops across the country that built on each other; extensive public comment, every draft being up for comment. And we would anticipate that as we move into the next phase of the ongoing framework process we would maintain that approach.

MR. WALLACE: Thank you. Plenty to dig into there, but before we do,

we'll move onto Cam. Cam, you were there at the creation, the beginning. You now have had the opportunity to step away and look at the process from the outside, which is almost a unique position to be in. Perhaps you could touch on sort of three things.

Firstly, if you could just give us a sense of how things have changed as a result of this process and where we came from. I think it's important to remember exactly how things felt just over a year ago before the President spoke at the State of the Union and issued the Executive Order. And particularly, as the former general counsel at Commerce, give a little bit of an insight into the privacy discussions that sat alongside the development of the framework. There was a draft privacy annex which drew some comment during the process and that has changed in the final version, but if you could talk to that.

And third, I think it might be interesting to get a sense of what you think the administration has learned from this process.

MR. KERRY: Well, thanks, Ian. And, Pat, congratulations, both on the framework and on the University of Pittsburgh announcement. Both terrific things. NIST, Commerce, and the country, I think, will miss your hand on public policy issues.

So, we are, I think, in the outcome of this framework in a very different place than I think any of us would have predicted when this policy discussion started three and a half, I don't know, four years or more ago. And at that time the sort of conventional wisdom was that the way to approach this issue was through some form of government prescription, using authorities of the Department of Commerce or of DHS, or somebody, to address cybersecurity by conventional rulemaking. And it will go out and adopt a set of rules that would create a standard that people had to meet.

And this is a very different framework. What Pat has outlined today, what the NIST framework does, the model that it implements is something very different. And some of that certainly is a product of the Congress' inability to legislate on this, but part of that failure was a lack of consensus about the right model, the right approach

here. And I think more than anything, the model that reflected in the framework reflects an evolution in the thinking about policy in this area and appreciation for the complexity of the issue, the speed with which the technology is changing, both on the company side in terms of what it is that you're protecting and what the risks are out there. This is constantly evolving, evolving at a pace that's simply much faster than convention rulemaking can deal with.

This has been a long process, but getting this done in a year is a lot faster than the pace of, you know, classic note-and-comment rulemaking. And this is also a model that is far more adapted to the technology space, to the world of digital communications and technology that really is at the heart of cybersecurity.

And I think that's an important piece to stress here, that this model, as Pat described it as a living document, is version 1.0. This is an iterative process of policymaking, something that, as Pat says, has been taken and moved over from standards setting, which is really why NIST was charged with the responsibility here because that is in NIST's sweet spot. It has done the guidance for federal agencies in the 800.53 documents that inform the framework.

And part of the evolution of the model doesn't reflect an appreciation for NIST's success in developing standards, its engagement with industry, its role as an honest broker in the process. So what we have is something that will help to move the needle in some important respects.

Cybersecurity has emerged as one of the critical boardroom issues that companies of all kinds need to address in today's digital economy. This framework provides a set of benchmarks that corporate managers, boards of directors, and others can apply to ensuring that companies are meeting cybersecurity goals in ways that are going to protect their assets, that are going to be cost-effective and are going to meet the expectations of shareholders, customers, and other stakeholders in that environment.

The other piece that I want to underscore in the framework is that it has

been designed as something that can cross borders. So here the United States has taken a lead in establishing a framework, establishing some standards, and doing so with a model that can be used around the world in this space. You know, it's been difficult in the current international environment, in the wake of the Snowden disclosures, to do that. But it is important that the United States continue to lead here, that it continue to advocate for a model of regulation and governance in the digital space that is adaptive, that does not operate by government prescription, that, you know, can transcend borders.

So this framework does that and that's an important thing.

MR. WALLACE: Thank you. And I think that is an extremely good lead-in to Dean. Dean, you represent a private sector perspective and not only the tech sector, but presumably those people who your members support. And I would be grateful if you could give us a sense of what you're hearing from the private sector about the framework. Are we going to get consent and evade? Or is this something that's going to get into the bloodstream?

And if you could also pick up Cam's point about the international dimension. You represent a global industry. Does this framework have the weight to build up an international following or is it going to bump up against European notions of a more regulatory approach?

And thirdly, as part of your role, you'll talk to people on the Hill. Wouldn't it be great to be hearing from legislators about how they're feeling about the framework?

MR. GARFIELD: You know, I'll try to address all three. On the first question, I actually think it's the latter, that it will get into the bloodstream, for two reasons. One, in part due to the process; and, two, due to the substance.

On the process, the way Pat described it, it made it seem quite inevitable and quite logical and linear, which, in part, it was. But it was that way because of the process that Pat had put together -- and the folks at NIST did as well -- which was quite open, transparent, and collaborative. And I think he and the team at NIST is to be

complimented for that.

On the substance, I think there are three reasons why it will become a part of the bloodstream and it will also speak to the question about the global impact. One is that the framework is actually quite flexible and based on risk management, so it's not prescriptive. And I think because of that and because of the collaborative nature of the process, folks will feel as if they had input into it and feel as if no matter what your business is like, there is something in there that enables you to integrate it.

Second, the foundation for a lot of what exists in the framework are global standards that were developed through consensus-based, multi-stakeholder processes, as Pat pointed out. And because of that, because they're global, because they're multi-stakeholder and open processes, I think the likelihood of success, particularly globally, is high. This is certainly, I think, a model for how these processes should be run internationally, both in the process and in the substance that results.

And finally, as far as the preliminary comment, the fact that it's iterative, but not iterative without a pathway forward. I think the inclusion of a road map that speaks to nine different paths or work streams, including international, is critically important. We all benefit from an open, integrated, interoperable Internet, and Cam alluded to it. There's lots of efforts and initiatives globally to shift that to make it more vulcanized. And I think this framework is a step in the right direction away from that, and I think is quite helpful.

As far as Congress, much of what we've heard thus far is twofold. One is, how can they help create a pathway for success for the framework which, literally, on the day that it was being released at the White House, we got calls from members of Congress saying this is a positive step forward? We concurred. And how can we help?

I think the second, which a year ago, after the President's statement and promise of getting this done -- literally, the week later -- we were in California at RSA, which is a big cybersecurity conference, and there was a lot of participation and energy

and concern around what is Congress going to do? My hope is that because of this framework, it creates a motivating force or an action-forcing event to get Congress to take on the elements of this that still require public policy. And soon we intend to do everything we can to further encourage that.

MR. WALLACE: Just a quick follow-up, Dean. When Congress staffers and Representatives and Senators phone you up and say, what can we do to help, what are you telling them?

MR. GARFIELD: You know, that's a great question. I tell them I need to talk to Danielle, who takes care of these things on our teams. (Laughter) Much of what we've been focused on what they can do is, one, there's still the issue around making sure that we have real-time access to information and information sharing, and so heavy emphasis on that.

The second part of it actually relates to something that we published on. The Department of Homeland Security has an important role in this process going forward. And so what can we do to bolster what DHS and NIST is going to do to enable the success here? And I can get back to each tangible step that DHS should take.

MR. WALLACE: We'll come on to that, but just before we do, you also mentioned the road map. And Pat, this is, I think, a very welcome part of the document, but it's perhaps a piece that will be less well understood because I think most people expect government to produce documents which then sit on shelves and gather dust. What you describe, setting up a living document, an ongoing process, and the road map, to a certain extent, is the guidebook for that process.

Could you just go into a little bit more detail on aspects, like the workforce, the federal agency alignment, the international aspects, and how you see that working?

MR. GARFIELD: Sure. Well, we're pretty good at writing reports that can sit on a (inaudible) shelf, too. (Laughter) But remember, this is not a government

report. This was an industry document. And in your opening comment you talked about the Executive Order laying out a year, which was an interesting timeframe that was put in the Executive Order because, depending on which perspective you had, that was either hopelessly too fast or completely unresponsive to the national need to protect critical infrastructure, right? So everyone was unhappy at some level. (Laughter)

And so, from a very pragmatic perspective, as we went through the process, we built on existing foundations. It was about pulling best practices from everyone and then quickly identifying those gaps and putting those on the To Do list, so as the process continued to unfold we had some focus.

So we were trying to pull the learning we were getting out of going through the process the first time to make sure that we had both everything we could capture from best practice and the identified gaps. So, part of that To Do list is pointing to the sun going, a framework process, and it was things that were identified as part of the first go-through that are gap areas.

They fall in two areas. One are things where the policy or the standards work needs to be advanced. Privacy is a good example there, where there was a lot of work to continue to identify those. And some of those have to do with the framework process itself: governance, adoption, and things of that type,

So, things like conformity assessment or government adoption or international are issues that really go to how do you provide a framework structure that's conducive to the widest possible adoption? And I think that list itself is still open.

I mean, as we go forward we'll be having new workshops; I think the first privacy workshop is actually in April. We'll be continuing sort of the full-throated engagement we had through the framework process, and at each one of these we'll be continuing to ask the group about gap areas. And that work list itself will be a living thing as we continue to revise and check things off.

MR. WALLACE: And as people in this room and in the country at large

pick out bits of the framework they would like to comment on, is there a mechanism in place to receive those comments?

MR. GARFIELD: Yeah. So the framework website is still up. We still collect comments continuously and we'll be feeding those, as we always do, sort of acting to compile and provide those to the group as we go forward. And then every new version, as they unfold, will be subject to the same kind of public comment.

The one thing that's important to keep in mind with an ongoing process, though, is that -- and this is really an important point -- that if you're waiting for this to settle down before you do anything about it, you're going to miss the train, right? That's not what this is about. In fact, my view is that the framework will actually be driven by those who are the users and adopters of it because most of the learning we're going to be doing from the framework is going to come from the hard-knock lessons about trying to put it into practice in your organization, and finding out where it worked and where it didn't and feeding that back into the process so it can be improved.

So what we've been trying to be careful about is, don't wait for perfection. We've been really asking -- what we most value are those companies who are rolling up their sleeves, are going to give this a try, are putting it to use, and are willing then to participate in the framework going forward to help refine it from that perspective. That turns out to be the most precious perspective of all.

MR. KERRY: That's particularly apt in that there's a lot of discussion around incentives and the role they should play in getting people to adopt the framework. And we could easily spend all of our time focused on that and whether Congress in going to enable it or whether it can come with Executive Action and yet do nothing else. And I think the idea of moving forward while continuing to grow and improve is the apt approach.

MR. GARFIELD: Yeah, I think the lesson of this document is cybersecurity is not a state, it is a process. And this really helps to lay out a process to

get there, but it's a continuous one.

MR. WALLACE: I mean, the question of incentives is probably one worth spending a little bit of time on. The Executive Order actually did focus on incentives and the administration put out some work on incentive. Perhaps not as forcefully as they might have done, which reflects perhaps some internal discussions about how that ought to work. But I think what I'm hearing from you, Dean, is that you'd rather take the discussion away from incentives and focus on other aspects.

MR. GARFIELD: I wouldn't say ignore it. I would say -- I can't articulate it. Wow, this is a process. And it's a process that's iterative where we'll continually improve. And so, where we have improved mechanisms for incentivizing people, they'll get integrated into this like everything else. But in the intervening time, let's do the baseline work that we know is achievable today rather than waiting.

MR. GALLAGHER: Yeah, let me make a quick comment on the incentives. You know, the perspective I've taken through this whole discussion on the incentives was that the challenge to industry was its international interest as a country to protect critical infrastructure. This is a clear national need.

We think it's also in your business interest as organizations that run elements of critical infrastructure to protect these assets. And the best outcome of all is when it's totally aligned, when it's great business to be protective. And that's the premise under which a market-based, standards-driven, internationally deployed framework makes the most sense.

As we start to exercise that, we may find areas where there's a misalignment, where business interests aren't quite aligned, where there's unnatural -- that's going to be the place where Congress needs to help us pay attention. And so, in some sense, it's not so much that any caution, I think, is not about internal skirmishes, it's about really a question of timing. That, again, I think the incentives debate is going to be really informed by those organizations that are putting this into practice because what

you really want to zero in on is, what are the barriers to using this?

MR. KERRY: Well, I mentioned that this has been an issue of great concern in corporate executive suites over the last several years. That's a reflection that there are some powerful incentives to address this issue, some powerful business interests. Ask the Target Corporation. Ask the hundreds, if not thousands, of companies that have had intellectual property stolen through cyber intrusions.

As standards move forward -- you know, the SEC has guidance out there for assessing and disclosing cyber risk. By giving a set of benchmarks, it helps to inform that process. So there are plenty of good and important business reasons for companies to address this issue. Most companies know that now we have some tools to help that.

MR. WALLACE: And one of the challenges, of course, for big companies, including Target, is -- and it will be interesting to see how the framework helps this process -- that some of those threats are getting more and more sophisticated. And that even if they take cybersecurity seriously, the cost of dealing with those high-end threats is challenging. How is the framework going to help deal with those advanced persistent threats that are hitting the headlines more and more frequently?

MR. GALLAGHER: So, I think, in a couple of ways. One of them is that a lot of those advanced persistent threats are enabled by the same moving parts that the framework addresses. You know, it's failures in authentication, failures to understand your assets, failure to -- having the wrong behaviors within an organization that provide the sort of latent vulnerabilities that these threats are designed to tackle. Now, they get a little bit more sophisticated in how they do it, so that's one piece of it.

I mean, there's a lot there that -- I think some of the statistics show that some 80 percent of these are really addressable by pretty basic application of well known controls. But the other part is that the process is pointing to a continuous improvement process. Remember the way that risk management framework works is to have the capacity to being able to identify what's happening on your system.

In other words, one of the behaviors you're looking for, for organizations that use the framework, is their self-awareness gets better and their responsiveness to an unidentified problem gets faster. And so those kind of behaviors are specifically addressed.

And then, as I said, to the extent there's actually gaps in the framework itself. Let's see, the technology space opens up and you have brand new issues, let's say in the mobility space right now or in large data. The reason the process has to be continuous is that there as to be an ability to adapt in there as well.

MR. KERRY: So this is one place where Congress could help. I mean, legislation can help to facilitate the sharing of information about threats, sharing among companies, as well as sharing one direction with the government can take place. In the other direction is more complicated, so legislation would certainly help to make that easier to do.

MR. GARFIELD: It's a known market failure. All the participants in the market have identified it and so the question is, what do we do about it? The one other thing that I would add is, much of the conversation thus far is focused on big businesses. We're small business representing big businesses and we've actually talked to our outside vendor, looked at the framework and identified ways that we can improve, even in our organization, using the framework.

And so I think the great thing about it is that no matter your size of business or where you sit or which industry you fit within, it's sufficiently flexible and risk-based that you can find use out of it and I think good use.

MR. WALLACE: The other area where people have critiqued, if not criticized, the framework is those industries where the market doesn't dominate. So, particularly, regulated industries and those where there is a less obvious financial driver. How confident are you that the framework will be able to deliver on its national security objectives in those industries where the bottom line might never get you to the level of

cybersecurity that are required to deal with the grave threat that the President was talking about?

MR. GALLAGHER: Well, I think time will tell, ultimately, how effective this is in those kinds of markets, but I should point out that those organizations operating under those market conditions were a part of the full process from the beginning and it was an explicit part of the discussion to make sure it was responsive to their needs and their issues as well. In fact, even up to and including the regulators themselves were part of the discussion.

So we were actually -- in an effort to make sure this alignment was real, that was a key part of the engagement that had to be there. So I hope that that's not the case because the way I've articulated this to the companies themselves is that if you think of regulations in addressing a market failure, then this is your chance to make sure the market has every opportunity to work, which is, I think, in everyone's best interest. And it has a number of intrinsic advantages, including the ability operate a market scale; including overseas, the ability to be much more nimble and be able to change with flexing technology. And so I think everyone's bought into that theory of the case and, hopefully, those alignment issues have been brought in.

One part of the Executive Order that's raised a lot of questions because it mentions the word "regulation" in the context of a voluntary program is that, you know, there are regulated sectors here and what we were trying to do is not end up in a situation where everybody worked together on this framework of practices, but then you were driven to do something different than that market solution by the regulation. So this is really an effort by the existing regulatory entities to have an opportunity to align against the framework, and that's the spirit in which they have been participating in that as well. And think that would be a constructive thing.

MR. GARFIELD: I completely agree with that last point. Some of that, though, will be determined by what was outlined in the road map, how DHS, as well as all

of the related agencies, align behind the framework. And that's one of the big question marks going forward.

MR. WALLACE: And that's a good last area to focus on before we open it up to the floor. Implementation of the framework is going to be key. Having the industry involved in the framework puts a little bit of the onus on them, but within government NIST will now be passing this process, to a certain extent, over to DHS and others. How, Pat, is that process going to work and what are you going to do to make sure the good momentum you've created continues once DHS take on the implementation?

MR. GALLAGHER: So, I actually don't view the implementation responsibilities passing to DHS. So I think that it's important to keep in mind there's three things happening here. One is the framework process, and this continues to act as the convener and will lead that. So nothing has changed on that front at all.

What DHS is doing is establishing -- has established a voluntary program that's there to support and promote adoption. That includes acting as a clearinghouse for best practices and a whole set of other things that, you know, within current authorities it can do to promote and support adoption. They've been working with us since the beginning, so we think we've done everything possible to make sure their efforts are aligned with what the framework is.

But I want to end on sort of the final point. The most powerful force driving adoption are the companies themselves. And we see that from their discussions as they put this into use. This is not just about what you do internally; this is about your relationship with your vendors, your suppliers, your supply chains, other companies that you work with in your sector. This is the way the sector community organizes to it. You can consider how this is going to look for them. And those are actually more powerful than anything we've been discussing that we can do from helping on the government side.

So I think sometimes people have construed a voluntary program as toothless and I just don't subscribe to that. I think they're very powerful. In fact, every product safety standard in the United States is basically self-regulated by industry through standards and these can be very muscular approaches. And I think that's really going to be where a lot of the lift comes from in driving adoption.

MR. WALLACE: Cam?

MR. KERRY: I'm ready to go to questions.

MR. WALLACE: Just before we do, didn't you mention you had some thoughts on DHS's role in promoting the framework. Is there --

MR. KERRY: Yeah, I think much of it is -- some of it is already contemplated. And so I know that there are a number of workshops that have been scheduled already and think Pat mentioned one of them, so part of it is education, doing what we're doing here today, but on a much larger scale and a more sustained scale.

Two is making sure we're measuring the right things, developing clear metrics for evaluating the success of this effort.

Third is -- and we've alluded to it earlier -- the focus on incentives. I think they're important, but we shouldn't make them the only thing. And then the collaborative process, the final part, which is the collaborative process that NIST has adopted, is one that's worked exceptionally well and it's critical that we keep that as a part of the work going forward. It's truly the way to ensure that it becomes broadly integrated and how businesses operate, and so I hope it will not be forgotten.

MR. WALLACE: I'd like to come back to what success looks like at the end, but since we have so many people here I'd like to open it up for questions.

We have some microphones going around. The usual Brookings rules apply. Keep your question short, end it with a question mark, and please give your affiliation when you ask it. So, down here at the front, please?

MS. DIVIS: Good afternoon. Thank you for this opportunity. My name

is Dee Ann Divis. I'm with Inside GNSS. I wanted to ask a question about a critical element as identified by the Department of Homeland Security across all 16 of the critical infrastructure sectors and that's position, navigation, and timing information; GPS, which is essential for a lot of networks, for example.

And DHS appears to be looking at the 16 sectors to implement protections with regard to that data, so the GPS data that they require. And I'd like to hear from the panel what you see through the road map coming up down the road with regards to standards or other actions to integrate the PNT -- the position, navigation and timing -- data to make sure that organizations have what they need when they need it.

MR. GALLAGHER: So anyone reading the 39 pages of the framework would not see PNT showing up as a -- and that's going to be one of those examples of an issue that's imbedded in the standards sets that are in the core because it points to a particular class of time-critical, position-critical data, and I think what the framework attendees were terming a dependency, and making sure that that's been addressed.

So without getting into the specific threat or vulnerability that DHS is worried about, my guess is since NIST has a lot to do with the time basis for that, we're probably working at a technical level with them already. But, you know, the framework becomes a vehicle for -- and this is why the federal agency participation was so important for threat informing the process. If there really is a new class of vulnerability that's essential to critical infrastructure, particularly cross-sector like that, then we're counting on DHS as a participant in that process to flag that and make sure that we take that back to industry as part of this process and make sure that the framework process doesn't have that as a gap area, right? That that's something that's explicitly addressed.

MR. KERRY: Actually, if I can add one thing which is maybe lost in this, is that as a part of the Executive Order all of the federal agencies are supposed to cascade the framework and I think -- or to come back with their ideas around it as well within a defined time period. And so I think that work is incredibly important as well. So

it's not isolated to DHS or NIST, but is cascaded broadly within all the relevant agencies.

MR. GARFIELD: We get to eat our own cooking.

MR. WALLACE: And so, at the back? Sorry, further back. You there.

MR. MOORE: Brian Moore with the Coast Guard Contingency Preparedness and Consequence Management. When you used the safety model as an example, it triggered something in my mind. Do you see in the future a credit rating agency or an ISO-type of third party to provide an audit function on companies, how well they've implemented the framework, and then provide a grade, something of that sort? So that, like you said, so the suppliers can know, okay, I'm only going to work with Grade A suppliers and if you don't meet that mark, then you can't do business with me, or something like that?

MR. GALLAGHER: So the way I would answer your question is to pick up on the last point you just raised. What we call these are conformity assessments. In other words, you've developed a set of practices and it may very well be critical to give an organization, from a business to business perspective, to know that the people they're working with conform to some level within those standards.

So this is a voluntary program, so the government's not going to be setting up a grade, but, in fact, something we have posed to the framework process is you may very well find that for this to work, you need that kind of conformity assessment. And there's a lot of different types, going all the way from self-attestation, all the way to third-party testing and accreditation.

And the trick is there's not a right or wrong one. The question is, which is the right approach given the market conditions you're facing? And so that's very much on the To Do list, actually, that was in the framework plan.

MR. WALLACE: And to take the question a little bit widely, one of the elephants in the room of cybersecurity for many years has been this question of cyber insurance. And there has been some suggestions that the framework might offer an

opportunity to the insurance industry, giving it a set of metrics to use. What sense do you have from your discussions about whether that's likely, possible, realistic?

MR. GALLAGHER: Well, I'm not sure my crystal ball is any better than anyone else's. (Laughter) But I will tell you there was enormous interest in participation by the insurance sector in this for that reason. Look, as soon as you put something into a risk management framework, the idea of all these assets we have for doing risk management come into play, including insurance markets. And my sense is that they have found the process very useful and I think there's some very active discussions. In fact, we've had a number of breakout sessions at almost every workshop on this particular issue specifically.

MR. GARFIELD: In addition to hearing from members of Congress and their staff about this, the other folks we heard a lot from are companies who intend or are examining whether to get into that space. Insurance companies, but also law firms are evaluating what this all means. And so I think that is absolutely right.

MR. KERRY: Yeah, I think this sort of audit process that you've mentioned and that Pat outlined is an example of how standards work in the marketplace. I don't have a better crystal ball than Pat to say that that definitely will occur here, but certainly part of the idea is in creating the tools, the benchmarks, is to inform that process.

So a number of the organizations they're involved in some of the underlying standards. ISO is one of them. There are others that perform audit functions. Some 40 percent of the corporate sector now has insurance against data breaches and that is triggering exactly the sort of engagement by insurance companies to take a close look at people's practices. This is a way to benchmark that look.

In the securities area, I mentioned earlier SEC guidance. I don't to this point -- you know, most companies have been able to sort of sweep it aside by saying that their risk is not material. I'm not sure after the Target or Neiman Marcus experience

that it's so easy to do that. And, again, for boards, for shareholders, for auditors, there's now this road map that people can look to assess those issues.

MR. WALLACE: So, Cam, do you see people making investments based on where people sit within the framework?

MR. KERRY: You know, I think that companies will have to take a more critical look at the disclosures that they make and I think that, in turn, can influence investors.

MR. GALLAGHER: I mean, the point you made earlier, Cam, about CEOs spending real time with their boards, shareholders, around these issues I think is indicative of how important this is and the creation of a real marketplace to mitigate those risks.

MR. WALLACE: Next question. At the back on the aisle? Sorry, not at the back. In the middle on the aisle.

MR. GOWARD: Thank you, Dana Goward with the RNT Foundation. I'd like to follow up on the question about PNT vulnerability. That's become quite the subject of late. A GAO report in November -- in fact, the U.K. and Russia and China have terrestrial systems to back up their PNT to ensure they're not dependent upon the faint signal from space.

So did I understand Peter to say that this has not been flagged as a problem by DHS or anyone in terms of cybersecurity, impacting the cybersecurity of the nation?

MR. GALLAGHER: No, I wouldn't characterize it that way. What I meant to say was that the extent to which PNT standards are found, or lack of redundancy, or whatever the specific issue is, would be reflected in those things that are referenced in the framework core.

What I am not aware of is whether DHS raised PNT as a specific issue as we were putting together the top-level framework structure. That's not to say they

didn't raise it as one of the constituent standards. So, in other words, you have a little bit of an onion here in terms of you have the overall framework process and then you have the constituent standards underneath.

I would expect, given the nature of PNT, that this would be one of the constituent standards discussions, not in the overall framework. But the NIST team is sitting in front, so if you want to direct follow-up afterwards -- (Laughter)

MR. WALLACE: This side, on the aisle. Please?

MR. KERNAN: Hi there. Todd Kernan with the Canadian Embassy. Looking globally, can you talk a little bit about the reception that you've had both from allies and foreign companies?

MR. GARFIELD: So I think, yeah, you might want to get a couple of perspectives here. You know, the overall reaction we've gotten from the very beginning was a combination of intense interest, wanting to wait and see what it looked like when it was done, and most promising of all, I think, an understanding that this can be used as a foundation for a variety of approaches around the world, even including those areas that we're considering more national response; even including a regulatory response. Because one of the things we point out is that, again, this is a global infrastructure, and it's really important that information and data companies be able to operate on that scale. That's what makes this technology so powerful.

Then aligning to -- just like we've asked our own internal regulators in the critical infrastructure space to align to this, it's something that can be done on the international scale. And we've had a lot of positive reaction to that. The most interesting one was coming from Europe and it had to do with the fact that in the same week that the President released the Executive Order, the European Commission was proposing some draft approaches that were going to be used for cybersecurity. And from the very beginning they've been quite interested in looking at this as a basis for moving forward.

MR. KERRY: Yeah, 30 percent of the companies we represent are

international, non-U.S.-based entities, and their reaction has been favorable as well. They operate in a world that's global, integrated, interconnected. They offer services, products, systems that they want to work on a global basis and so appreciate and welcome the framework.

They're also competing in a marketplace where increasingly their efforts to use cybersecurity or national security as a market access barrier -- so whether it's the multi-level protection scheme in China or some of the problems we had around preferential market access in India, and so having this framework that's built on global standards that are consensus-based and developed through multi-stakeholder processes is helpful to those international companies as well.

MR. WALLACE: Pat, this is something that NIST does across its business dealing with international standards. What would be the process to internationalize the framework or at least encourage its use internationally?

MR. GALLAGHER: So what we did in this case was actually something that was modeled after the approach we took with smart grid standards setting a few years back, which was we started with the premise that the framework process was immediately international. We invited international participation. I was meeting with delegations from around the world as this actually started. And we made a deliberate effort to look at international standards as one of the building blocks of the framework and asked companies to bring those forward.

So, in some sense, we've been international from the beginning. And by the way, I expect the international flavor of the framework process to actually grow as we go forward. That was actually identified in the road map, as we expect this to happen.

What will be interesting is maybe more on the adoption side. In other words, the extent to which conformity assessment, certification, or product identity, the extent to which those can be put into a global infrastructure or a global context will be very interesting. And then how do -- because you're dealing with critical national

infrastructure to an extent -- how do countries respond to that from their own national policy perspective to align and do something that makes sense there?

So I think that's going to be really the two issues there, is those matching between the national and this global market and, you know, how does the industry want to put in the muscle and the compliance piece itself? If it works, then it will be quite interesting.

MR. WALLACE: Who else? Second row, please.

MR. WEBER: Hi, Rick Weber at Inside Cybersecurity. Dr. Gallagher, could you speak a little bit more about the next phase in terms of when the framework or how the framework will be revised? So where and when will we know that it's going to be revised?

MR. GALLAGHER: So we haven't announced a revision schedule yet for the framework. In fact, what we've done is deliberately created a bit of a pause in our engagement in setting up the kind of workshop schedule that would point to any kind of revision for the very reason I didn't want to get in the way of the adoption piece. We really want companies using this and we've stated from the beginning we would like the follow-up discussions and the framework process to be informed by those organizations that are using the framework.

But we have set up a tentative schedule of workshops that are on the framework website. I think the first one is probably the privacy one in April and then I think there's another one in the summer, July.

And, again, there's really no surprise in what the agenda is because the road map was laid out in that process. I actually am not expecting major revision to the framework itself. I think the real impetus is going to be going after these gap areas and identifying those places where we felt there was some real work to be done.

And, also, I think maturing what we call the governance discussions. In other words, we should now start seriously taking on -- if this framework is going to be an

ongoing process and normalcy is success -- not that I'm looking for NIST getting out of the business, but how do we set up a governance scheme where all of these different companies can work together to turn this into an ongoing routine process? And, again, we've had experience doing that both in the cloud sector and in the smart grid and other areas. And I think we would like to continue those discussions as well.

MR. WALLACE: What does your experience in the smart grid sector and cloud sector tell you that we'll end up looking like?

MR. GALLAGHER: Well, I mean, probably the most mature of those right now is the discussions in the smart grid just because it's a little bit older than the cloud side. And the cloud effort was really focused on the government adoption side with FedRAMP. But in smart grid, you know, a smart grid interoperability panel, which is an actual 501-C3 organization, was put together because the stakeholder group felt that there wasn't an existing organization that could sort of help facilitate that process, so they established one of their own.

NIST has provided funding for the operation of that organization. We remain sort of working with them routinely today where you now have sort of a living cycle of, okay, here are the technical issues that are changing, here's the new ones, here's the top priorities to affix. The smart grid inoperability panel sort of does the triage and, in many cases, now works with all of the different standards organizations that are supporting that, trying to say, hey look, this is a key area to improve, and then making sure that the adoption side of that is worked out. Because, again, that was interfacing with a regulated industry as well. So making sure that all of that was put into shape.

I think it might look different. It probably will look different because this is a different sector. And so we're not going in with a this is what the answer looks like. But our view, and this may take a while to put together, but we think it's work continuing the discussions about how do we do this if this is not a one-time through process, but this is something that we do year-in and year-out?

MS. GARLAND: Thank you for this discussion. My name's Lynn Garland and I'm unaffiliated.

You've spoken a bit about how the federal government agencies are going to comment on this and react, and how industry has incentive. And I was wondering how are you going to get the state governments to adopt this and get involved because a lot of things are at state level that are very important?

MR. GALLAGHER: So that's a great question and I suspect a number of us what to jump in.

MR. GARFIELD: But we'll let you answer, Pat. (Laughter)

MR. GALLAGHER: So we've had strong interest from the states. In fact, a number of state CIOs were at the event rolling out the framework. I was talking to them about their framework process and they actually end up touching this problem at a number of different levels. Many of these critical infrastructure entities are actually interacting heavily with the states. In some cases they're regulated or involved with states themselves anyway and so, again, this harmonization issue comes right out for them, that this is an important building block because it's something that they can use as a framework for dealing with these organizations. Think of water utilities and others that are happening at this level.

The other place that this is very helpful to them is that the extent to which we see widespread adoption of the framework means that the technology providers that are providing technology and software and security solutions to support these companies are not creating a market of some scale that can help drive down cost and can improve performance. And that advantages all the states who maybe, in and of themselves, wouldn't have the market scale to drive this outcome.

And so, I think, again, we've encouraged state participation since the very beginning. They have been involved in the framework process from the very beginning and I think you're going to continue to see their involvement ramp up. Yeah?

MR. KERRY: Well, the only thing is, one of the reasons we've been pushing for legislation at the federal level is the fear that you would end up with the mish-mosh of state legislation that don't allow for these sorts of efficient, effective markets. I think the framework is helpful because to the extent that it creates a baseline that is collaborative and based on these sorts of standards, I think it's quite helpful in avoiding that.

MR. WALLACE: But, Pat, how do you see the framework being used at the federal government level? I mean, there are some clear examples of the requirement for improved cybersecurity within the federal government. And how do you see this being rolled out across that sector of government?

MR. GALLAGHER: So we actually, at the rollout for the framework, talked a little bit about this in terms of government use. You know, the most straightforward thing that every adopting company is doing right now is to use the framework to develop profiles of your current practice. That's what's laid on the framework. And one of the first things we'll be doing at the agency level using this -- very much like you did, Dean, with your organization -- trying to develop profiles where -- both where we are at today, where would we like to go.

That's part of that adoption support system that's built into the framework. I think this is actually going to be really interesting because the maturity model aspect of the implementation tiers that are in the framework could be extremely helpful to the federal government because they moved the debate past the application of controls and the notion that the only thing you can assess and measure is how many of the controls you put in place.

Under the framework, that's a tier 1 implementation level. And what this starts to point to is that you can move beyond that into a real risk management framework at a higher maturity level that has bigger advantages. And so I think it opens up the palette of really addressing this as a risk management exercise within the

government.

And finally, the last one is, there's been a tendency to address cybersecurity performance issues in the government by just making the CIOs more and more muscular. And what the framework actually points to is a different answer, which is integrating it with the program lines, right?

This is going to the board rooms and to the CEOs. And I think it points to a very interesting outcome, which is it really starts with the cabinet-level secretaries and real accountability there and looking at this from an integrated perspective. So we've just started that, but I think that's going to be really quite interesting.

MR. WALLACE: Cam, you've been a cabinet-level secretary for a short time --

MR. KERRY: You know, I was privileged to have a wonderful acting deputy secretary, Dr. Patrick Gallagher, and one of the things that he has done in that capacity is to really take in hand the cybersecurity management at the Department of Commerce. I think you called it eating our own cooking, and to do that in terms of making management at the highest levels of the department accountable for cybersecurity and not simply something that our CIOs deal with.

MR. WALLACE: And would you see those profiles being published, made publicly available?

MR. KERRY: I don't -- you know, as a FOIA lawyer, there's no obvious exemption. There may be security issues in aspects of them.

MR. GALLAGHER: But let me go back to the point that the framework is not about the controls, right? In any organization you're going to have a dynamic set of controls. Our CIOs are drowning in piles of controls that they're to be looking at and, by the way, other mandates outside of the security space.

What's unique about the framework from the government perspective is the management approach to really integrate it into how you've run a department, and to

make those decisions, not just technology decisions, but skill set and hiring and cost allocation and all the other things that are just as much a part of cybersecurity as controls.

And so, in some ways, this is a very fresh perspective on the government approach and I think that management approach could be very public. And that's actually probably more important. That's where the real accountability lies.

MR. WALLACE: So we have two questions. If we could take them both, and then we'll -- I have two questions to finish. So we'll take both questions and then we'll answer them.

MR. INJERRA: Yes, I'm Majir Injerra, a security studies fellow at Georgetown University. I just wanted to come back on your comments regarding (inaudible) controls. If I understand correctly, the controls are a first step, tier 1 out of 4. Does that mean that the controls have been adopted, at least in the government today?

MR. GALLAGHER: So, let me be a little bit careful about what the implementation tiers point to. So there's controls at every level. I mean, controls are an important aspect of how you control a particular risk. So I'm not saying there's only controls at Tier 1 and then you can get away from the controls.

What the implementation tiers point to is, in some ways, your maturity in managing this risk. And so, I think of tier 1 as sort of being a rule-following culture. In other words, you create a To Do list and success is I got through the list and I'm doing all of this, I can do it reliably and repeatably. That's quite different than an adaptive or proactive type culture where, in addition to having the rules and controls, you're actually actively identifying new changes and new threats, and preemptively. So it's going from a set of static controls to almost an immune system.

So controls are everywhere, but you asked an interesting question. Where will the federal government end up as we start doing profiles? I don't know, but I think because -- my suspicion is because we've been sort of mesmerized by control and

control application and audit against control, we will probably not be too surprised to find ourselves near an implementation level that's really focused on that, which would be around 1.

But we'll see. And I think that will be quite interesting as we do that.

MR. WALLACE: Final question?

MR. SHAH: Garam Shah from Booz Allen Hamilton. One of the things the panel talked about was the alignment of the business interests with the national interest. So let me give a scenario and just see, you know, how would that really change in the corporate world.

We all talked about, again, Target and Neiman Marcus, and I recently read this study where the U.S. credit cards are like eons behind the European credit card. We still use the magnetic strip and everything. And I think that Visa and MasterCard and American Express, they did the study and they say, right now something like -- you know, they did their Target/Neiman Marcus scenario being losing, say, $7 billion a year.

But if we have to replace all of the credit cards, it's going to cost us more like $11 billion, right? So normally cybersecurity they don't really do. You know, they pick a financial ROI, but in this case they are not doing that. So how do we make sure that some of those, you know, financial interests does not overtake what you would call the national interest?

MR. GALLAGHER: Well, I think, you know, underneath your question is I think one of the profound issues that Congress will face. If these are not aligned, I think that's -- you know, because ultimately we're talking about something that if it fails under cyber attack, has grave harm to the country. And so, that's just going to get fixed somehow.

But I think, backing up a little bit, I'm not sure I would buy that the financial risk assessment that they were looking at was correct in the following sense. You know, you're correct that one of the issues that the United States has seen in this

sector is we were early adopters in card technology. We have a very expensive deployed technology base and it's been compared against much younger technology bases for card readers and so forth in other places. And with that legacy comes some vulnerability. And the question really will be, yes, that's why the risk management approach is so important. You know, to what extent does the refresh rate of the technology help us mitigate and control these risks? And that's a question that I assume a good framework following organization would be going after. But this is not just the direct financial loss of those customers that lost their information.

And that's certainly not what I'm hearing from the CEOs. This is a profound reputational loss. This is potentially going right at their market share. And I think what I'm hearing from CEOs is a very acute sensitivity that this is a big deal and this is why it's rising to the very top of the board rooms as a discussion.

So I'd be surprised if they were reaching that kind of simple apples-to-oranges comparison because that doesn't track with what I'm hearing from CEOs today.

MR. KERRY: Yeah, I think Pat is right that that cost-benefit analysis is, in today's environment, wrong. I think it reflects what has been historically the challenge of dealing with cybersecurity: that the CIOs, the compliance officers were worrying about it, but it was a cost issue, so it was difficult to get attention, I think, because of the reputational concerns, because of the impact if you are a company that has a significant failure. I think that is changing. That's reflected in the level of concern that Pat talked about.

And I think we're seeing that reflected in some of the demand from the corporate sector to change, for example, card technology, despite the economics that you talked about.

MR. GARFIELD: Yeah, I work in a highly disruptive sector where companies don't exist largely based on new innovation. And the key to the success of those companies are trust and integrity. And so, to the extent that we don't take

cybersecurity seriously, we're undermining that trust and integrity. And that's a principle reason why it is one of the issues that I hear perhaps most often from our most senior executives of the companies that I represent.

It is truly one of their top priorities. And so it is right in pure analytical or quantitative sense, it may not show up, but the brand and identity damage is so significant that it's frontal to their consciousness on all of these issues.

MR. WALLACE: Pat, I'm going to take the moderator's prerogative to ask one penultimate question before we end up looking at what success looks like in this, and that's just to tackle the question of privacy, that this was explicit when the President issued the Executive Order that everything you produce needed to respect privacy.

And throughout the process, there was clearly concern from what you might call the privacy lobby to ensure that that was the case. And you have adapted what you've produced, in part, I suspect, in response to some of that. Can you just tell the story of that so that we have a better understanding of how the responses that you've had and how you have adapted the framework to reply to some of those concerns?

MR. GALLAGHER: Well, I think the short version of that story is the one you laid out, that privacy was an explicit requirement for us to consider as we developed the framework from the very beginning. It was actually part of every discussion and every workshop that we had, including the kickoff workshop. I remember having a discussion about the incorporation of privacy at that point.

What seemed to happen and, you know, we could, I guess, go back and have a discussion about what the psychology was, but it tended to be an issue where, first of all, the maturity on some of how do you implement, you know, what's the building blocks that you build implementation of good privacy protection, was less mature than what was true in a lot of the cybersecurity areas. And I think partly based on that, it was relegated -- even though we brought it up at every workshop, it was one that we kept pinging, saying this is one we need to work on.

And one of the consequences of that is that up about midway through the process, the privacy principles were basically in a standalone section as an appendix. And I think maybe that's what caught everyone's attention. When that construct was finally there, I think then the stakeholder group that was working on the framework -- all 3,000 of them -- jumped in and it was actually an interesting perspective on how the framework worked. A whole group of industries stood up and said, this doesn't really make sense to have this be a bolt-on attachment. You know, this is based on the same kind of data protection principles that are integrated and they made a counter-proposal to integrate those into the main framework. So now it's actually integrated and not bolted on and that's where we stand today.

MR. WALLACE: Cam, as Commerce's former top --

MR. KERRY: I think where it ended up is the right place. Security is an essential ingredient of privacy. It is part of the privacy principles. It is part of the White House Consumer Privacy Bill of Rights. So it's really not a standalone issue. There are privacy implications of some of the cybersecurity practices, particularly when you get into sharing information with third parties, in particular the government. So it's important to incorporate into the framework privacy practices as has been done, but it really is part and parcel of security.

MR. WALLACE: Didn't some of your member companies get extremely vocal on this?

MR. GARFIELD: Yes, so we were one of the stakeholders who were concerned with the bolted-on approach and so, like Cam, we think it ended up in the right place. I do note that it's one of the nine; I think, work streams and so we intend to continue to stay engaged and work to ensure it's progressed forward.

MR. WALLACE: Which brings me to my last question, which is, as we do progress forward, what do we think success is going to look like? And an important part of the framework, I hope I'm correct in thinking, is to access where there may be a

requirement for legislation or others to engage.

So, question for each of the panelists is, how will we know whether other action is required? But more importantly, what does success look like and how can we be confident that this is delivering what we think it should deliver?

And if we come down this way, we'll give Pat the last word.

MR. GARFIELD: Thank you very much. (Laughter) I think a big part of it is adoption, so the extent to which most businesses are looking at the framework and integrating it into their operations, much in the way we talked about CEOs making it a part of their board room discussion.

The second part of it is, if it, in fact, doesn't become a stale document that sits on shelves, but does become a living-breath iterative process as opposed to an endpoint whereby we're still working on it 10 years from now.

And then gaps with Congress, I think we've spoken to those and there are quite a number. The most pressing one that I think can be dealt with on its own is around information sharing.

MR. WALLACE: How much confidence do you have that that's going to have success?

MR. GARFIELD: A high degree of confidence. The question is when? (Laughter) And so my confidence -- I'm sitting in a discussion with Congresswoman Rodgers and Ruppersberger on Monday, and so I'd hate to say anything that's going to lead them to be upset with me, but just given the legislative calendar, I think it's highly unlikely that anything meaningful will occur in this Congress, but I do think there is a sincere interest in finding a solution.

MR. KERRY: So, I guess to put a metric on it, my answer would be a version 2.0 or else some 1. some significant number because I think that would be a reflection, as Dean said, that there is active engagement, active adoption. And that experience had lead into the iterative process and an indication that the model is working.

MR. GALLAGHER: So I always like it when the NIST guy gets asked the measurement question. (Laughter) I don't even know those things. We like that. (Laughter)

So, for me, the acid test of all of this is, is our nation's critical infrastructure better protected? It's also the hardest thing to measure. All right, that's going to be very challenging.

So I think of the success stories having sort of two elements. One is the near-term, and I think that's the adoption. And the way I've characterized it is, is this inevitable? If this is what everyone's doing and this is -- and we're struggling with those kind of nuts-and-bolts issues. They may be tough, but they're the kind of things that would only come out with organizations that are really trying to use this. That's a big success because that means this is actually being put into practice and you have a framework to improve and drive.

And then I think there's an intermediate set of metrics that I think are potentially very powerful, and it kind of goes to the safety comparison. So, while the final outcome may be something that we only learn retrospectively, looking back, I hope that we start seeing some very meaningful improvements of what I would call security behavior, and that can be the capacity within organizations to be able to identify and manage risk, that can be the capacity of staff, it can be skill level.

It can also be behaviors like self-awareness, you know, the fact that we know what's happening more. Our speed to respond improves. I think there's a set of security behaviors that are quite measurable that would point to a healthier organization in managing these risks.

And I think, you know, my hope is that we'll be working with industry. That's kind of a NIST thing to do, to try to identify some meaningful measurements along those lines.

MR. WALLACE: Well, thank you. We look forward to returning for

Cybersecurity Framework 2.0, 3.0. Perhaps having the chancellor of the University of Pittsburgh come back and comment on it? (Laughter)

And I would like to thank all of you for joining us here today, and invite you to join me thanking Dean Garfield, Cam Kerry, and Pat Gallagher for a fantastic panel. (Applause)

* * * * *

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