THE BROOKINGS INSTITUTION

FALK AUDITORIUM

THE FEDERAL CYBERSECURITY FRAMEWORK
FOUR YEARS LATER:
WHAT'S NEXT FOR CYBERSECURITY?

Washington, D.C.

Wednesday, February 14, 2018

CAMERON KERRY, Moderator
Ann R. and Andrew H. Tisch Distinguished Visiting Fellow, Governance Studies
The Brookings Institution

JEANETTE MANFRA
Assistant Secretary for the Office of Cybersecurity and Communications
U.S. Department of Homeland Security

ANNIE ANTÓN
Professor
Georgia Institute of Technology

TOM WHEELER
Visiting Fellow, Governance Studies
The Brookings Institution

* * * * *

P R O C E E D I N G S

MR. KERRY: Okay, well, good morning everyone and Happy Valentine's Day. I'm Cameron Kerry. I'm the Ann and Andrew Tisch distinguished visiting fellow here at the Brookings Institution and I'm glad to welcome you here this morning. Today is -- it's not just Valentine's Day, it's an anniversary. It was four years ago that and NIST released the Cybersecurity Framework and we actually had an event here at Brookings. Pat Gallagher, the then Under Secretary at NIST, came at sort of the first public discussion of NIST. I had the opportunity to have my first appearance as a visiting fellow here at Brookings to talk about the framework. And having been sort of par of the hatching of it at the Department of Commerce; have been pleased to see its release; to see the uptake of the NIST framework in the intervening time. Gartner estimated a couple of years ago that about 30 percent of companies in the U.S. sort of now are using the framework. The President's executive order last May reaffirm the framework and directs federal agencies to use it. And, of course, we're now in the final stages of NIST doing, that I guess is version 1.2 of the framework which will be out sometime soon. And just today is launching some new features of the website to make the framework more accessible.

So that sort of sets the scene for our program today. To look at where we have come in terms of preparedness and resiliency in those four years. And what still needs to be done. So, we have a terrific group of panelists today of people who have been deeply engaged in this issue, certainly over the past four years, but beyond. So, we will kick off our program this morning with some remarks from assistant secretary in the Office of Cybersecurity in Communications at DHS, a part of the national programs and protection directorate. The cybersecurity operational arm of DSH and after that, I will introduce the other panelists and we'll have a Q&A. So, please remember to silence your cell phones. Don't necessarily turn them off because we encourage you to tweet with the hashtag up there and invite your questions after we have some of the panel discussion.

So, let me introduce Assistant Secretary Manfra who has been in public service since she went into the army as a communications and an intelligence officer and has been in a variety of cybersecurity jobs at DHS, at the National Security Council and particularly, focused on critical infrastructure. She was appointed as the assistant secretary last June, so please join me in welcoming Assistant Secretary Manfra. (Applause)

MS. MANFRA: Thank you. Thank you, Ken, for that kind introduction and thank you, all of you for being here. I was -- as I came here, I was thinking, it was a little over 10 years ago that as a grad student across the street, I used to come here and listen to various different events and it's pretty amazing to be standing here actually presenting at one of these events with such distinguished colleagues that we'll talk of later on the panel. And I think, one of the things I love about the events sort of taking a look back at how far we've come, my own career almost sort of tracks how cybersecurity has changed so much. And so, for me, personally, it's often very interesting and I think rewarding to think about how much has changed over the years. When I joined the army in the late '90s, we sort of had the early days of thinking about net-centric warfare, a term that folks still think about and, you know, I was learning how to, you know, put patch radios together and figure out how we can connect to these new-fangled fax machines to use in the field and then, you know, sort of spending the time that I did in the army and seeing how that changed through the wars and how we thought differently about communications and networks and what it means to both defend and take advantage of those capabilities from the military and when I got out, decided to go to grad school and kind of continue those national security studies. And somebody came up to me and was like, there's this new office that's starting at the Department of Homeland Security called the Office of Cyber Security and Communications. And we're helping them stand it up and we think that you kind of have the right background and I had spent most of the time overseas, so I was like, "What is this new department? I'm not exactly tracking all of this." But I was able to -- I decided to just take a leap and I was like, "Cyber security? That sounds like something I could, you know, get into." And so I started with the department actually standing up for the office that I know have the honor of running.

And I will tell you that if you ever have the opportunity in your life to be the ground floor building an office and then be able to work through all of the different ways and thinking about -- had the opportunity to serve with Secretary Johnson on the National Security Council in a variety of areas and seeing this issue from so many different perspectives. We used to joke that, you know, when we first sort of started, nobody would pay attention. We're trying to tell people about the importance of cyber security and defending our networks and most people would just sort of say, "I got some IT ladies and men working on that. I'm not really sure. It's a little bit confusing. What does that actually mean to my business? Or what does that mean to my agency?"

And look where we are now. You know, I had the privilege of working with NISH on the cybersecurity framework and we're now at this point where throughout the country, and frankly, throughout the world, people are recognizing that cyber is not some niche technical thing that they can just trust and hope that somebody in a closet somewhere is working on and addressing. But it is actually something that needs to be considered as part of their enterprise risk management approach. Whether you're an agency in the federal government; state and local entity, or in the private sector. And that it really challenges much of what we think about; what the role of government is; what the role of the private sector is and managing that risk.

And so I want to talk to you very briefly about because I want to make sure that we have enough time for the panel, is sort of where we are in the administration and where DHS is at in thinking about how we manage that risk and the role of DHS and the role of companies in managing that risk. So, as I assume all of you know President Trump did issue an executive order in May of last year on strengthening the cybersecurity of federal networks and critical infrastructure, as was noted, a key part of that was requiring federal agencies to adopt and implement at the cybersecurity framework and reinforcing that agency are accountable for the cyber security of their systems and their networks. And I believe that, that's a very important message, just like an industry CEO is ultimately responsible for the risks to include in the cybersecurity risks to their systems. We are equally accountable within the government for the risks to our systems and networks, but there is risk to an individual organization that they can manage and they have insight on. But there's also what we call in sort of that broader enterprise or sometimes also systemic risks. And that's where DHS often comes into play, particularly, with starting with the federal cybersecurity, what the executive order really tried to look at was transitioning from thinking about agencies managing individual risks individually to thinking of the government as an enterprise. That we have enterprise risk as a government; that we need to improve our visibility on and improve our ability to manage. So DHS plays in that place. We provide tools and capabilities and we're increasingly providing more. We're looking at shared services; looking at how we can have more cost effective and efficient ways of deploying those capabilities and services, but what that also allows is DHS to have visibility on that -- what is that enterprise risk to the federal government and what can we do to better manage our vulnerabilities that an agency may have one perspective, but there may be some gaps and seams across the organization. Again, thinking about the government holistically that way.

So, as many of you hopefully, read the IT modernization report looking at how we transition both modernizing our IT; the systems themselves, but also modernizing how we think about governing and for clearing. How we think about managing security; modernizing how we manage security on the government side. And we're looking at really how -- what are the best practices in industry and how can we apply those to the government? This is a monumental effort for the government to undertake. It's one that has, you know, we've had various different efforts previously and we have made progress. But this, I believe highlights that this -- the need for this to be a priority. The priority for resourcing, modernizing our systems, but also again, modernizing and thinking differently about how we do security.

So, that's a key part in much of what DHS is focused on, but again, always going back to that sort of cybersecurity framework as our touchpoint of this is how you need to think about cyber risk. And when we think about industry, what we have been focusing on and it actually started in that same executive order that required the cybersecurity framework, was also tasking DHS to think about and analyze where are -- where do we have the potential where a cyber incident could have catastrophic consequences? And doing that analysis to refine our understanding of what are those critical services and functions that, whether they reside in industry or in government, federal, state, local, what are those critical services and functions and who performs those? And how do we ensure that those entities have the information, the resources, the capabilities they need to defend against what is, again, both an individual company or agency risk, but also a national risk. And what that -- we're continuing to refine that. We're continuing to work with industry, but I believe that this is on the critical infrastructure side, probably our most important work that we'll be doing and will continue to do that we've been building on for the past few years.

We can all say, okay, we want to have trust and ensure the integrity of the financial system. We want to ensure that we have access to clean water, that the electricity system continues to run and that there may be actors out there who are interested in disrupting those capabilities. So, how do we, as government and industry, refine our understanding of what those services and functions are; who provides them; who are those stakeholders that need to be a part of that conversation and how does the government, again, ensure that we have that sufficient understanding to where we're able to use all of the capabilities that the government has available to it, to one, be looking out for those who are trying to disrupt those and provide appropriate alerts and warnings. But also, be able to collaborate with industry to prevent somebody or some group of somebodies from doing that. But if we can't prevent it, which we have to recognize we're not going to be able to prevent every sort of cyber incident that happens. For those of you that work in this space, there's a lot going on and it's hard to detect and prevent everything.

But if we understand the business of industry and we understand the mission of those agencies and what it is they need to continue to operate and who those service providers are and who those entities are that are a part of that overall delivery of those services and functions. And then we start building those contingency plans to ensure that, should we have some indication that something anomalous is happening and again, for those of you who work in, you know, sort of particularly in cyber response, usually, you have no idea what's going on in the first few moments and often probably a little bit longer than that. But collaborating together when -- I've talked before about WannaCry and the notion of collective defense, that the government doesn't know everything; industry doesn't know everything; our international partners don't know everything. But together, if we come together and we're sharing, this is right down to, this is a piece of malware.

I think this is what it's doing. What do you think? Here's the product I want to push out from DHS. We just issued a product around what we call HIDDEN COBRA, which is the North Koreans malware -- the latest one was malware but we've also issued products around infrastructure that they're using. So, we're working together as a government saying, here's information that we have. We're putting it out. We do work with industry even before putting out some of these products so that they can check it. Make sure that this is what they're seeing. We're complementing each other's resources, authorities and capabilities and then, we're all working together to take action. That is easy to say. Very, very hard to implement, but what DHS does have is the authorities and the infrastructure to be able to do this.

And what I will say is we have an enormously committed and dedicated private sector and state and local governments who are willing to do what it takes to work with us and the other elements of the government to solve these challenges. But for us, it really has to come down to, how do we really understand that systemic or potentially catastrophic risk and what are those pieces that we're putting in place to ensure that collectively, we're best prepared to defend against those. So that's what we're working on going forward and again, I'm so honored to be here and look forward to continuing with the panel discussion. (Applause)

MR. KERRY: Well, thank you, Jeannette Manfra. It struck me as you were talking about your communications background and putting together radios and I didn't plan it this way, but we have here a group of panelists who really understand in a very deep way the technologies that we're dealing with.

So Annie Antón is maybe the Grace Harper of our time. She is a computer scientist, a professor and former head of the Department of Interactive

Computing at Georgia Tech. She also served on a range of advisory boards of public, private and non-profit for -- in issues of defense of cybersecurity of privacy. And in particular, was a member of the National Commission on Cybersecurity Resiliency that about 18 months ago took a look at the issues of cyber security; made a series of recommendations for the next administration.

Tom Wheeler to her left, is, like I say, a Washington institution, but a --

MR. WHEELER: Right.

MR. KERRY: -- but an entrepreneur at heart. So, Tom headed both National Cable Television Association and then, the Cellular Telecommunications and Internet Association. Well, both of those were upstart industries. I am -- in between he's been a serial entrepreneur, venture capitalist and author of history books. And, of course, was chairman of the FCC and brought, I think, to the chairmanship about the depth of his experience in communications and that same sort of entrepreneurial spirit. So, delighted to have both of you here today.

Let me first invite you, if you have any comments in response to Jeanette Manfra's remarks and Annie maybe if you could look at a little bit of where we are 18 months down the road in terms of the recommendations of the national convention.

MS. ANTÓN: So, at a very high level, when I was on the Cybersecurity Commission, we count with six different imperatives that were basic high level recommendations for the federal government in terms of how we can enhance cybersecurity. And at a very high level, I think I'm very pleased to say and thanks to Kevin Stein over at NIST, who is our key staffer on the Cybersecurity Commission. Kevin and I had a nice chat yesterday looking at those imperatives and seeing what's been done on each of them. And so, at a very high level, something has been done on all of the imperatives, some of which is currently in place. So, there was a report that went to the White House, I believe, a week ago that's not public yet about IT Workforce. Once that becomes public, there will have been some action on everything imperative of the six that were presented by the Commission. And so, we're not there yet, but there has been action and activity. I know that there's a lot of vulnerabilities and a lot of concerns nationally, but I think that it's very gratifying to see that we are making progress and we are taking it seriously.

MR. WHEELER: So, I think if we're going to celebrate the fourth anniversary, we need to also begin by identifying what are the leading culprits in the establishment of the framework was. Again, the blue suit at the end of the line here and recognizing your role in that game for which we shall integrate for.

You know, as I listened to the Assistant Secretary talk, my thought was, thank God for DHS. Thank God you're there and that this kind of pullover writing structure is being put in place against the government in working with the private sector. My experience coming out of both industry and the FCC is that cyber is not something, it's everything. And that my concern is I see policy progressing, particularly looking at it from my former agency's point of view is that the agency chartered by Congress with the principle responsibility for overseeing the security of our commercial networks is AWOL. Do you -- an Army term, it's an old Army person here, and I think have been walking away from a responsibilities that many times can only take place in a regulatory structure. And so, hopefully, as a whole of government approach to cyber, we can begin to see some changes insofar as the oversight of the commercial networks themselves.

MR. KERRY: Jeanette, any thoughts on that and particularly, there's maybe -- there are conflicting messages in the legal authority who's in charge of critical infrastructure?

MS. MANFRA: Hmm, who's in charge? I would say the Department's that frankly, is endured through multiple administrations is responsible for orchestrating overall the strategic framework for critical infrastructure, in addition to sort of some of the specific sectors of many of the sectors that we have responsibility for. But the secretary of Homeland Security is really responsible for that overarching approach to some critical infrastructure. Everything from cyber to national hazards to counterterrorism, that entire suite of issues that we have to work on with critical infrastructure. I don't know love the term in charge because, you know, it --

MR. KERRY: Fair enough.

MS. MANFRA: -- sort of implies that we're directing others and it's all a partnership, but yeah, I would say the Department has that sort of overarching responsibility to ensure that the entire sort of critical infrastructure community and that the government are focused on the priorities that we have this mutual understanding and that we are connecting national risks that cuts across sectors, those sorts of things are our responsibility.

MR. KERRY: Mm-hmm. By the way, Tom, thank you for your kind compliments, but I think the real -- I have some championship, I guess, with the NISH framework, but the real work was done in the agency and I will tell you that one of the best decisions that we made in the Congress department in the Obama Administration was to make Pat Gallagher the director of NISH and eventually, the undersecretary. And he, of course, was part of the National Commission as well, has just been a tremendous leader. He was a career scientist at NISH and I think, I see in Jeanette Manfra, as well, so what Tom said, the virtues of having professionalism and experience and we need that in cybersecurity and fortunately, we have that. And I think that's a reason we see a surprising amount of continuity.

Let me ask you a question on that because I had a conversation with a policymaker in the executive branch on the continuity that we see sometime last year after the executive order and he said, yes, that's true, but we need to do more to make people do things. Particularly, maybe about the critical infrastructure. Is there more that's in the works that's always there? Is there going to be in some form, or is the government going to make people do things?

MS. MANFRA: I would say that what we're looking at is are all the incentives aligned in the right way? And what I see is a lot of willingness and a lot of benefit on the voluntary work that we're doing and that a lot of it has to do with DHS stepping up to do more. More collaboration, more leaning into the authorities that we've already got to ensure that industry understands the perspective that we have and can make their risk management decisions based off of information that we have.

We have used the authorities that we have to direct federal agencies to indicate publicly risk tolerances that we have and we've seen that, that has an impact on the market as well. So, I would say that's a good framing as fundamentally, all of the pieces, the policy framework, it's there. What we're looking at, are those incentives aligned in all of the right areas to ensure that we have, again, those critical services and functions. The right organizations taking the steps we need to take. So, I know that's somewhat of a broad answer, but it is because we're looking across the landscape and in thinking differently about how we incentivize action, I would say. So, I know you were talking about regulations. Personal opinion, I think that there is a tremendous amount of work that can be done in voluntary partnership and that I believe that DHS just -- we haven't just brought the full capacity to bear that we have and so that's where I believe that I'm very much focused on. We just -- I want to ensure there's a use for regulations and there's a use for other incentives that our government has and I just want to make sure that we're very smart in how we apply each of those levers that the government has available to us. But that's my personal opinion.

MR. KERRY: I think you spot on. The points are, you know, in particular in a field that is evolving so rapidly in which you do something and the bad guys have all kinds of incentive to move fast to undo that. The regulation becomes very difficult.

What we tried to put in place was what I call agile regulation like the agile software development that is always trying to respond, but there's two components to that. One is that you have to say and you're going to do this. We're going to do this together, right?

MS. MANFRA: Mm-hmm.

MR. KERRY: Because there are consequences for not. And secondly, is there needs to be leadership in helping to get to those voluntary solutions. So, for instance the standards for the new Fifth Generation Wireless Network. When we left office, we had proposed a notice of inquiry that said that there need to be included in the 5G standards, cyber as a forethought rather than the way we always do, is oh, my God, afterwards, we go running and have to do patches. And so, we teed up a notice of inquiry that asked the whole series of questions for industry, for academics, for folks to say, these are the kind of things that ought to be included in the 5G standard which is still in process.

The Trump FCC killed that inquiry. And so it didn't come as a great surprise to me when all of a sudden, you see the NSC floating the idea of we're worried about the security of a 5G network is going to be and we've got to look at what I consider major coding and solutions. But there is this balance that we have to work out and no place is it more important than in cyber but a key to that balance is, excuse me, there is a watchman, a watch person on duty here.

MS. MANFRA: Mm-hmm. There are other ways also of trying to entrust this, so I understand -- I'm embarrassed I can't remember the name of the name of the bill, but there's a bill that's being worked on now about IOT device security. And the idea there is that the federal government would only procure from companies with devices that meet a specific level of standard security, so that's one way that I see the current Administration trying to do things differently is just to really -- and through the federal IT procurement process by which we were talking about earlier by setting up standards. It's just another approach.

MR. KERRY: I totally agree.

MS. MANFRA: Yeah, there's absolutely role for regulars, I mean CCs, as you well know and dependent bodies and they would go through their decision-making progress -- process. I think that we believe there's a very critical role for regulators and we've partnered with FCC, with a variety of different regulators and sort of their role in how they assist in managing that risk. But exactly as you said, there's always this sort of delicate balance of how you best incentivize. And so to that point, the areas that we can sort of have more authority over is looking at how does -- DHS is -- because if you don't know, we've appropriated a decent bit of money to go through a process where we procure tools and capabilities largely around continuing monitoring for other agencies. And what that model allows us to do is not only have a consistent set of tools that are deployed, but it also leverages the purchasing power of the entire government so we get better rates. It lowers the cost, but it also -- we have a set now of related to this program, approved products list, so product that go through review that we can say, these are the products that are approved to work as a part of this program, the Continuous Diagnostics Mitigation Program. And then importantly, though less relevant to this, particularly a discussion, but it actually provides us with operational insights because the benefit to us, of us buying those tools is then we require that the agencies send that data back to us and so that is what allows us now to have that picture.

So there's a lot of different things like that. Procurement is a huge one that can have -- it won't change the entire market. I don't pretend to think that the government has that much market space, but it can incentivize it; it can provide some indications of what the government is looking for. But I completely agree, the regulars need to be a part of this conversation and they have a very critical role, but I don't pretend to speak on behalf of those independent regulators, so.

MR. KERRY: Yeah, Tom, how broad are the -- of CCU's authority is on device licensing and to what extent could the FCC, by rules or otherwise, deal with some of the issues of IOD devices through those authorities.

MR. WHEELER: So, after the dime (?) attacks in, what, ’16, right, I got a letter from Senator Warner asking a whole series of questions about specifically on that point. Because the FCC licenses -- I'm sorry, it doesn't license, the FCC has to type accept every emitting device in the country, whether it's your cell phone or your coffee maker that connects to the internet, okay.

MR. KERRY: Yep.

MR. WHEELER: And that's for very logical reasons. It's for RF interference and let's make sure the airwaves aren't going to get all screwed up with spurious emissions. I responded to Senator Warner and said, if we think that protecting the airwaves from interference is important enough that there should be type acceptance of products, why shouldn't one of those inspections that have to be made be a cyber assurance for that product? Because we all know, in the dime situation, I mean, there is a market failure here. When you're making the chip that goes to the board that goes in the camera that goes to Best Buy that goes to the consumer nobody in that supply chain is asking any question about cyber security. Mostly, they're saying, talk to me about price. So, if, as a part of this kind of assurance on products to make sure they don't interfere with the airwaves, why shouldn't we be asking the question, has something been done to mitigate concerns or anticipate concerns about cyber threats?

MR. KERRY: Yeah, you'll see changes in that supply chain ecology that are events forcing that.

MS. MANFRA: So, you know, I'm not privy to insights on supply chain, however, I will say that it was a major focus of the Commission. It's something of great concern and one thing you did mention also is just on -- at the end of user, the consumer who doesn't know whether or not a device or a system that they've purchased is secure. And wouldn't know how to and so that was major thrusts also, is how do we make sure that we're educating not just the workforce, but consumers at large on how to use secure devices and how do you make sure you can trust the -- a system? So, you probably have a lot more insight into the supply chain than I do.

MS. ANTÓN: Yeah, so supply chain is something that we're really spending a fair amount of time. We have stood up an internal supply chain initiative around how do we -- how do we tackle what becomes a really quickly, really complicated, that much we've learned. And you have hardware; you've got software; even then you've got this sort of IOT piece and it's -- but I do believe that we can't sort of all just throw up our hands and say, "It's too complicated. I'll never know where the code's coming from." But at some point, we will know. We can figure it out or we collectively, not just government and so what we've been working on is how do we kind of scope the problem? How do we ensure in really focusing on -- particularly on government, how do we assist in working with GSA on ensuring that the right due diligence is done for contractors or for the products that folks are doing that has that sort of cyber risk in addition to other risks that the government's more used to, kind of thinking about. So building that cyber risk into those assessments and particularly for -- on the government's side, what we have been calling high value assets. So, those very systems that would have a high impact to the government if somebody did something with them. So, we're standing that up and scoping what are those -- how do we advise on supply chain risk both to government entities, how does the government sort of procurement system which we don't definitely need to go into any detail about the government procurement system. But it is not designed to think about supply chain risks from a cyber perspective. It's thinking about other types of risks that the government is trying to manage like financial risks and all those sorts of things. So, we're working with the procurement community; with the counter intelligence community; with folks like GSA; with NISH; a variety of folks to think about the government needs to internally do better to understand its own supply chain risks just from its own providers.

Then, we've also had a lot of really great conversations with manufacturers, software vendors. A lot of different folks. The mobile community and working really with that -- more with the engineers to understand this is what we think the risk looks like. Is this what you think the risk looks like? And try to get that sense of, "Okay, if we can have an understanding of the risks of whether it's companies or products that we're concerned about," maybe we kind of get to that mutual understanding, then try to have a conversation, "Are there ways to technically mitigate that risk that everybody can be satisfied with?" And then on the IOT, that the -- we talk with one of the Cyber Commission is, when you have our microwave or you've got your little UL symbol that says that it passed a certain level of testing that says that this product does what it's supposed to do. So, is there some mechanism to do that for IOT because, yeah, it is a cost and we're not under any illusion that we're going to somehow convince every consumer to really think hard about cyber security before they buy that one particular product? So, again, how do you get those right pieces in the market thinking about programs like underwriter laboratory that do that for existing consumer devices? So, those are the different strains of work what we're doing.

MR. KERRY: Mm-hmm.

MS. MANFRA: So, as perhaps one of the only or handful of engineers in the room, I actually have a question for you --

MS. ANTÓN: Oh, boy.

MS. MANFRA: -- which is, when you were looking at -- when engineers look at the vulnerabilities sand when the government looks at the government vulnerabilities, are those aligned or are you seeing that there's some misalignment or gaps and that maybe that's where we should be focusing?

MS. ANTÓN: I think -- well, so sometimes, there's differences of opinion on the technical side just because government has a certain amount of visibility of how something is actually engineered or something is actually architected on the industry side, so it's very useful for our technical folks and industry technical teams to get together to say, "Well, we're basing our risk judgments because we think this is how these are deployed. And if they're not done that way, then that's very useful for us in thinking about risk." The other -- a lot of what we come to is are risk decisions aren't always because of a technical scenario, it's because we're thinking about the broader sort of --

MS. MANFRA: The enterprise.

MS. ANTÓN: -- geo-political, the enterprise, all these other pieces and so we've been having, I think a lot of very useful conversations where you can say, "Let's help you understand where the government comes from and when we're thinking about supply chain risks." And most companies, we sort of -- we're all on the same page generally, I would say. It's more about how we think about managing it. And a lot of companies will come and say, "We believe we've mitigated this through technical means. Let us walk us -- walk you through and oftentimes, it's we're okay, yeah. We agree, that's a good way to mitigate that and we're comfortable, but let's kind of keep talking as maybe the risk profile changes.

Other times, you know, there's sort of broader kind of industry issues. There's not many other players. There's not many other, you know, sort of companies that are manufacturing these devices. So it's much more long-term issues that we have to think about in terms of how do we ensure that we have the right R&D in places that we would like to see more development of different types of capabilities, I guess, in systems and products. So, that's kind of a long answer, but I would say that's sort of how it generally falls out.

MR. KERRY: Yeah, you know, there's an interesting change that I think that I see in this area. I remember in Deputies' Committee, meaning quoting a maxim from a NISH document that it comes from President Kennedy's National Security Advisor, McGeorge Bundy, that "If we protect our diamonds and our toothbrushes equally, we will save a lot of toothbrushes, but we will lose more diamonds." And certainly that's, I think, been the operative approach in terms of focusing on critical infrastructure, but that was before the internet and things.

MR. WHEELER: That was before toothbrushes were connected.

(Laughter)

MR. KERRY: That was exactly where I was going. We've got a lot of connected toothbrushes out there, quite literally, so maybe there is more work we need to do to protect the toothbrushes. So let's talk about election systems because that's been designated as critical infrastructure and the states seem to have come to an understanding. That doesn't mean that they're being federalized and so, Jeanette, your testimony to the Intelligence Committee last year said that, I guess, it's what, some 21 states were targeted and some number were compromised. I guess that, that's a fact at this point. What do you mean by compromised? What does --?

MS. MANFRA: Trying to think --

MR. KERRY: -- what do you get from targeted to compromised?

MS. MANFRA: -- right, so some of the -- unfortunately, this is a bit nuanced which is not always conveyed, but it's -- first of all, let me just say scanning by bad actors happens on the internet all the time.

MR. KERRY: Mm-hmm.

MS. MANFRA: All the time, so that's one important point for those who aren't in this space where people don't understand. What we saw was in partnership with an organization called the Multi-state Information Sharing Analysis Center, which provides -- so, I talked about sensing capabilities that we provide for the government. We also provide some grant funding to them and they provide seven sensing capabilities for state and local organizations. And what we saw was the Russian actors that we were concerned with targeting in scanning state and local systems. So, that was -- that set the nature of the 21 states.

Now, the important thing to understand is again, as I think we all know now, these systems are run by state and locals. The government doesn't have perfect visibility into these state and local systems. We had what we had at the time and we notified the targets of those scans at the time. When we talked about and we talked about the testimony that there was a small number that was accessed, again, is, as some of you know, you can get into a system, that doesn't mean that you're successful in your ultimate mission, whatever that may be. So, it still stands that again, systems may have been accessed, but there's no -- there is no evidence old or new that any votes were actually manipulated. Those systems were not related to vote tallying systems. So, I think it's important for the public to understand some of those distinctions and that's what I was talking about and what I think is also very, very important for the public to understand is how much progress has been made since former Secretary Johnson designated that sector's critical infrastructure.

We have now what we call a government coordinating council which is just government's sort of speak for a forum that exists under the DHS protection for having non-public conversations. Representatives from state and local official community we meet with on a regular basis. We're working through how do we ensure that when the government -- just like the other sectors that I talked about no different here. It's just a new sector that we haven't engaged with previously. How do we make sure that if the government has information that it's getting to the right people at the right time. So, working with all of the states to have those right points of contact to ensure that, again, if we have anything that it gets to the right people and that they also have the plan within the states to manage that. Similarly, if they see something, how do they get that information to us and then, how does DHS ensure that it's getting to the right organizations within the government and that we're collaborating to work on that. We've been able to issue clearances to those individuals so that we always try to declassify everything that we can, but in some cases, that's challenging, but we still need the information to get there. So, these state and local officials were working through and we've been able to issue some clearances we're continuing to work.

We've also worked with industry. We stood up again, we call it a sectoring coordinating council. This is, again, the term that we use for industry coming together under critical infrastructure. So, this is voting machine manufacturers. Those that work on voter registration rules. Those that think about even kind of analytics, election night reporting. Those sorts of things because we're trying to take a very holistic view in thinking about election infrastructure and how do we protect those. So, there's -- I know the work that we have done and importantly, the work that the state and local officials are doing doesn't get as much play, but there has been --

MR. WHEELER: Mm-hmm.

MS. MANFRA: -- just tremendous -- I would -- I've worked with a lot of sectors and a lot of really great sectors. I've never seen a sector come together so quickly to be able to organize itself around such a challenging issue and being able to have very productive conversations and like you said, there's no oversight, there's no sort of federalization or nationalization of systems that's not remotely our intent at all. But what all these things have allowed us to do is work through again, how do we build that system where those defenders, those people that are responsible for managing those systems have access to everything that they need, whether it's services that my organization has to conduct assessments or it's information that the government has to protect their networks.

MR. WHEELER: Mm-hmm, so, Annie, Tom, thoughts on protecting our election systems?

MS. ANTÓN: No, there were hearings yesterday --

MR. WHEELER: Right.

MS. ANTÓN: -- from -- on elections and our intelligence leaders are telling us to expect a tax on the mid-term elections and we need to get ready for it and it's part of our structure and we look at risks. I would say that the risk of undermining our democracy is very high. That's a -- that's something we want to avoid.

MR. WHEELER: Mm-hmm.

MS. ANTÓN: So --

MR. WHEELER: I can add anything other than to go back where I started and say, thank God for DHS. Yep.

MR. KERRY: So, I -- fair to say that the attackers have learned a lot, so people -- they may not have manipulated systems, but they've had a lot of opportunity to map systems, to explore vulnerabilities, to test reactions. I think that this is an example of the challenge of cybersecurity, that you're always playing a defensive game and you can up your defense, but the attackers are -- get to be a step ahead. So…

MS. ANTÓN: Unfortunately, just the mere fact that we're even scanning and that the American public that doesn't understand computing hears that back in itself can undermine --

MR. KERRY: Mm-hmm.

MS. ANTÓN: -- their trust and credibility in the election system, so it's a broader, bigger problem than just a technical one.

MS. MANFRA: Yeah, I was used to saying that just because it happens on the computer, doesn't mean it's my problem. I'm not sure I can say that anymore. (Laughter). But, you know, helping the public, helping people understand sort of the difference of what we think about cybersecurity, protecting infrastructure, defending infrastructure versus an organization or an entity using what people might refer to as cyber to have other effects. That is something that we distinguish within the government. I'm not sure that everybody sort of fully appreciates that distinction, but I will say to Annie's point, if we have to be conscious of ensuring that what we're doing in all the work that we're doing is about protecting our elections from any ability to manipulate them and I think it's important that we also ensure that anything that we're saying or doing doesn't undermine that public confidence. I think that's just something that we all need to be very conscious of and our number one goal is to, again, ensure that those who have those systems and run those systems have what they need to do their job. And that we need to ensure that we're continuing to do it collaboratively and transparently, so that the public understands that there is -- there's no reason to not have confidence in those systems.

There's more work that we can be doing and we are working on shoring those up, but there's no reason to now have that confidence and I think that is a collective challenge. We work very hard to continue to --

MR. KERRY: Mm-hmm.

MS. MANFRA: -- work, but that is a collective government, private sector, civil society sort of challenge that we need to work through together as a country.

MR. KERRY: So, just because it's on a computer, it's not your problem. It reminds me of that whole diamonds and toothbrushes thing came up in response to people at DHS thinking that if it happened on a computer; if it happened on a phone, it was their problem. So, I -- why don't we turn to the audience for questions. So, if you put a hand up and identify yourself, you are first in my line of vision, so you get the first question.

MR. BIESECKER: Yeah, hello. Cal Biesecker with Defense Daily for Jeanette. The budget came out the other day and there's a request to transfer from DHS Science and Technology, the R&D funding, maybe a lot of it, if not all of it to your division. Why is that? I think the senior administration officials talked about the need to align the R&D funding with operational requirements, so what wasn't being done that you think you can do better? And do you even have the authorities to do R&D right now? The fact that you're not a -- you don't have the SIPA Act or whatever that is. It's been -- it's been approved.

MS. MANFRA: Thank you for mentioning the act that we hoping to get approved. That did go through the House with what you're referring to is the legislation to change our name from the awful National Protection Programs Directorate to the Cybersecurity Infrastructure Security Agency and the --

MR. SECTOR: Mm-hmm.

MS. MANFRA: -- and the House did pass that and we're working with the Senate on that. So, yes, it's that we've a close -- we do -- we are authorized to do research and development. We do a very small piece of it. I would call it more what we do is much more applied research and development and what we're working through is how do S&T work together with our mutual authorities and our complementary authorities in infrastructure to do what you said, what other folks have talked about. Ensure that the RDT&E -- that the research and development testing and evaluation that's going on is directly aligned with operational requirements and the notion being that you put it closer to the operators so that we can drive that. But it's absolutely a partnership with our science and technology division.

MR. SECTOR: What hasn't been done that you feel that needs to be done now?

MS. MANFRA: Oh, there’s a tremendous amount that could be being done. It's not necessarily because S&T wasn't doing it. What we're working through is what those research and development priorities are. Thinking about some of the capabilities, for example, when we talked about deploying capabilities to the civilian government, there's 101 agencies that we're deploying capabilities to. Many of them are small. Many of them are very large. Many of them are very large departments that have many small agencies, such as DHS and the Department of Commerce and others. And so a lot of some of our challenges around and, again, I wouldn't -- for those of you who are more pure research and development, I would call this more in the applied space, but how do you think about whether it's existing technology that's available or soon -- R&D

that's happening. Our challenge is often scaling that across the entire civilian government. So, looking at R&D around emerging technologies that could be useful to our mission, but we need to scale them, so investing in that, which can also, often take a turn for some of those folks who are involved in that R&D.

MR. SECTOR: Mm-hmm.

MS. MANFRA: Also, looking at supply chain, where are those areas that we could be investing and this is the world of R&D, this isn't an enormous amount of money, but it's enough so that maybe we could start looking at some places in supply chain, applying some of those R&D dollars around some of these supply chain challenges. Challenges around encryption, you know, we sort of -- encryption, very important from the cybersecurity perspective, but how can you preserve the benefits of encryption and I'm not speaking from a cybersecurity side of it. I won't try to talk about what the law enforcement and other challenges, but as we see encryption, how do we ensure that we preserve that benefit of encryption, but also, have insight and we don't lose visibility and there's a lot of cool sort of research and development that's being done around that challenge. So, that's another area that it's very operationally relevant for us, but some of this R&D is in some of the early stages. So, that's kind of some of the examples of areas that we're looking at.

MR. KERRY: And I think there's also a billion dollars plused up for DHS --

MS. MANFRA: yes.

MR. KERRY: -- for cybersecurity. One --

MS. MANFRA: It's not a plus up -- it's not a plus up.

MR. KERRY: Okay.

MS. MANFRA: No, we -- there's -- we're already at roughly a billion.

MR. KERRY: Okay.

MS. MANFRA: So, I didn't want to --

MR. KERRY: That's right. It's about $200 million of the added funds, at least as I read it. What's envisioned for that span, the part from the R&D?

MS. MANFRA: So, a lot of our budget is focused on federal cybersecurity and so, it's really looking at advancing some of the continuous diagnostics and mitigation work; it's looking at some interesting things that we've identified as we've deployed some of these tools and capabilities. What we've identified as that a lot of agencies don't have the governance in place that they need to actually benefit from those tools and capabilities. And they don't have some of the engineering capabilities. So, actually building teams working with like, digital services and others is build some teams that can help them develop their governance plans. Some of the, that I would call softer stuff, but acts just as important as the deployment of the tools.

We're also very focused on our internal analytics, so over the years we've been built a lot of capability to collect information, particularly, from agency networks, but we also have programs for private sector information sharing and what we need to invest in, which we're investing in both previously, but really putting a lot more investment on the infrastructure to do better analytics that our analysts need, but also just the analysts themselves. Having these data scientists and these very sort of high end folks that can come in and say, "Okay, we've got all this data, what does it mean?" So those are the key areas that we're looking at.

MR. KERRY: Good, a number of more questions there. Yes, sir, on the aisle. Wait for the mic and --

MR. PESTAROC: Thanks for your presentation. I'm Bobby Pestaroc, a small business proprietor now, but formally a governmental public health official at the local, state and federal level. In efforts to protect the public health, there are a range of incentives and formal structures, also, regulatory, for example, that exist at each level of government and sometimes, and often, they're used at each level to improve the public's health and to seek better outcomes in public health. You've described one instance this morning of elections being an area where, particularly, state governments and local governments are active in the cyber area. I wonder whether you could describe efforts, particularly at the local level that you've seen where whole enterprise initiatives involving a community's industries or communities sector are working with their local governments to demonstrate examples of what you'd like to see at the federal level through your work.

MS. ANTÓN: We do see some of that, yes, definitely, we're seeing and we're very encouraged by sort of -- what we're looking, of course, is much more of that national profile, but we've been in -- we've got folks out in the field. We're deploying more folks out in the field. We are seeing that they're sort of, I guess, communities of interest just based off of location and so different cities that are coming together that are taking some of the work around information sharing and analysis organizations and how do we build either a regional hub for information sharing or a community, whether that's a city or some other kind segment where that -- those different businesses and local governments are coming together. So, we are definitely seeing some of that. It's sort of different and very dependent on where they are. I know that I've seen some work done out in the Seattle area. There's work that's being done in Chicago, Boston, Texas has got -- there's a lot of different sort of --

MR. KERRY: Mm-hmm.

MS. ANTÓN: -- there's a lot of different pieces and they're all very grassroots, which I think is great and what we've just been trying to do is encourage those and provide them with assistance if they need any assistance in figuring out how did it -- how to do that. How to stand that up and if they'd like to connect with the federal government, that's great, but they don't have to. It's really focused on their local.

MR. WHEELER: Can I pick up on a local point here. An incredibly important local activity is 911. The FCC sent to Congress its annual report on the state of 911 in the last week, I think. And buried in that report is the fact that only nine states and the district -- I'm sorry, 11 states and the District of Columbia have any cyber mitigation strategy for 911 systems. And as those systems go digital, they become invitations to digital bad guys. And this is something, again, where there is a need for a regulatory step up that says, "This is what should be expected in terms of protecting the ability to get to someone when they call 911." And this is something that is not being pursued. The report was setup and nothing has been said about this serious local public safety problem.

MS. ANTÓN: I think one of the challenges is that when we try to do risk assessment, sometimes we forget that there are the whole sectors of risk that we're not thinking about and so for this 911 example, I bet you there's a whole bunch of other ones that we've yet to uncover nationally.

MR. WHEELER: That's a great point, Annie. And what we have to do is start asking the questions. Is there?

MS. ANTÓN: Right, right.

MR. WHEELER: So, the only reason this was known is that during our period, we added to, as we tried to do with everything, we added to this survey of 911 answering points.

MS. ANTÓN: Mm-hmm.

MR. KERRY: Questions about their cyber preparedness.

MS. ANTÓN: Yeah, right.

MR. KERRY: If we hadn't answered the question, we wouldn't have known. Now, the answer is the tree has fallen in the forest. We do know. What are we going to do about it?

MS. ANTÓN: Yeah.

MR. KERRY: But you're right. There's something, but it's got to start with asking the question.

MS. ANTÓN: Yeah. That's where we kind of keep coming back to -- 911 is a great example. The communications half of my name actually is around the public safety communications mission that we have and kind of coming back to that, what are those critical services and functions that our country depends upon? 911 is one of those critical services and functions. And so while we've done a ton of work on the more traditional thinking about interoperability and operability of public safety communication systems and systems like 911. We're just sort of starting to do that work around, what about the security of those systems and we've done work with First Net doing work with some of the different providers. Working with Department of Transportation, around the next generation 911 and the FCC, so I agree that this is a great example of one of those areas where everybody's been focused on a few areas that quickly come up, but until you kind of go through that whole thing, it's what does our country actually really depend upon? And then start going through what do we have in place to ensure the security and reliability and the resilience of those systems. Many of them already have a lot in place from more of a traditional emergency management, but they're not necessarily looking at the cyber side. So, we're trying to bring those two together working with FEMA and a variety of other folks. That's a really great point.

MR. KERRY: Go to the back of the room over here. Gentleman in the white shirt there. Looks white from here anyway.

MR. MARKS: Close enough. Lavender maybe. Joe Marks from Nextgov. So, yesterday's worldwide threats hearing herein the Senate, there was a lot of talk about Wild Way and ZTE. There's legislation right now that would bar them from government contracts. After, I think it was in October that the Kaspersky band came out as a budding operational directive. Is DHS looking at more government wide bands of suspect companies?

MS. ANTÓN: This just goes back to I would say the supply chain conversation that we had is that the steps that we're taking right now is, what's our understanding of the risk? What is industry's understanding of the risk? Are there ways to mitigate it technically that the government feels is sufficient and then after we have those kind of conversations, it's also looking at, okay, well, what are the different tools if the government is not in the position to be okay with that level of risks? Then what are the different tools we have available to us? So, that's where we are in that process. I would say we're looking across the board.

MR. KERRY: Yes, over here. Yes.

MS. ANTÓN: Ladies first, definitely. (Laughter)

MS. TURPIN: Good morning. My name is Tasha Turpin. I'm from Richmond, Virginia, working for General Electric. I'm senior director for technology and risk. One of the questions that I had and what struck me is how we're protecting infrastructure with the emerging regulation, such as China Cyber that's already in effect and then, the upcoming GDPR regulations around data privacy. Are you getting any input from your partners in the private sector on how they are preparing to comply with China Cyber so that they continue to -- they can continue to compete globally and be successful in business and same with GDPR? Thank you.

MS. ANTÓN: Yes. I mean, yes, we absolutely are talking to --

MR. KERRY: Yeah. Go ahead, Tom.

MR. WHEELER: Well, GDPR brings up, I think as a pressing issue. I mean, one of the recommendations of the Commission was to increase international engagement and that's also reflected in the executive order. Why? And what's going on? What can we expect in terms of cybersecurity and engagement? Particularly, as Europe with implementing GDPR cybersecurity measures as it implements its network information security directive. It's a relatively green field.

MS. ANTÓN: I believe the Cloud Act was introduced last week, right which is looking at adopting the visa waiver as a way of handling mutual legal assistance treaties.

MR. KERRY: Yep.

MS. ANTÓN: And I believe it's supported by DOJ as well as it's set by partisan efforts, so I think there's some efforts that have been made there as well.

MR. KERRY: Mm-hmm.

MR. WHEELER: So, the privacy question and the whole GDPR and privacy in general, it's one of those things you look at and say, oh, this isn't the cyber issue. It's a privacy issue. No, excuse me. It's a cyber issue, okay and there are impacts of not engaging in the privacy issue at first. So, we had a privacy protection rule for networks that as a component. I said before, we tried to make sure that cyber was in everything. As a component, had a cyber part stipulating the responsibilities of those networks of collected information to provide security for that information and penalties if they did not. Well, unfortunately, the Congress threw out the entire rule. But the point of the matter is, as a result of dealing with the privacy issue, you have now, opened a cyber hole because there is no requirements that this data that's being collected has to be protected. And one of the things we had to do from an enforcement point of view was frequently levying fines against networks whose systems that were storing consumer data were being violated. And we need to be proactive in that, but again, it's back to the point, can you be proactive unless there's somebody who says, excuse me, you're going to be proactive and we're going to expect that you're proactive and we're going to inspect that you're proactive and that's a regulatory role.

Right and the other side of GDPR, of course, is that -- well, maybe we ought to be making rules in the United States for the United States because in an interconnected world somebody else makes the rules and suddenly they apply here.

MS. ANTÓN: You know, when we talk about GDPR, we're also talking about our allies, but China has a new cybersecurity law where you can't --

MR. WHEELER: So-called.

MS. ANTÓN: Right, so-called. And so you can’t have any data for any companies cannot leave the country.

MS. MANFRA: Right. Yeah.

MS. ANTÓN: And Russia is about -- my understanding is that they want to move their portion of the internet completely off the internet. So, we have grand challenges globally --

MS. MANFRA: Yeah, we could talk about this for hours, I think. But I think Tom sort of -- we've had that kind of privacy, security, debates for what I would call physical threats. We need to have that same conversation about online threats and I think you're exactly right. We've had, I think the Department's had one of the -- not the first, one of the first statutorily mandated privacy officers and we've had a privacy officer for a very long time. Since the standup of the department and we have privacy officials embedded in my organization that are looking at everything that we do that have a really -- they're privacy experts, but they now have deep cybersecurity expertise. And so they -

- we really have a lot of internal conversations about what are those tradeoffs for the different systems we're developing and all that. And I think that's not a conversation that has been very widely happening, but it is because of GDPR; because of these various different things we're now seeing more and more. And I encourage that conversation because I think it's not one or the other, but I do think that we can't pretend that they're two different things operating in two different paths. There's balance that we want to achieve and I completely agree that we need to really recognize that we don't want this fracturing of the internet. So, how do we work with industry, many of which are multi-national companies? How do we work with our allies and others, whether that's through standards bodies; through the various different international fora that exist to look at those more coordinated approaches which is to preserve that global internet that we've all frankly, benefited tremendously from.

MR. KERRY: Now, it's your turn.

MR. IGNACHI: Ignachi International Urban Alliance. Are we learning from the Russians? I lived under communism for 40 years, 40 percent of the border was the Soviet Union. Those guys are perverse, to put it mildly. Are we learning from the Russians?

MS. ANTÓN: I'm not sure I exactly understand what we are learning from them.

MR. IGNACHI: We, I must say, Americans are straight shooters, but when you fight somebody who's not, you probably have to learn some additional rules first, including cybersecurity.

MR. KERRY: So, we're certainly getting some training from them.

(Laughter)

MR. KERRY: Yeah, over here, sir.

MR. WEBER: Thanks, hi, Rick Weber, Inside Cybersecurity. So, going back to the NISH framework fourth anniversary. So, we're not expecting big changes in this first revision to the framework. So, is the NISH framework sufficient for dealing with connected toothbrushes and IOT risks and artificial intelligence and 5G and all the new things that are going to be coming online?

MR. KERRY: You want to go first?

MS. ANTÓN: I think the NISH framework is not mean to solve every specific issue in cybersecurity. What it's meant to provide is an approach from managing cyber risk for an organization and if your risk includes some of those pieces, then, yes, that should be incorporated as a part of your cyber risk management. I would point to -- NISH has done work on each of those areas and published a great work on whether it's from an internet of things or artificial intelligence. So, there's a lot of great work that they've been doing. We're working on to up the NISH framework. I wouldn't want to try to have the NISH framework be the solution for every single one of those problems when within this framework is trying to do is get folks to think about cyber risk, whatever that looks like in their enterprise and manage it appropriately.

MS. MANFRA: I think the beauty of this framework is that you can tailor it too.

MS. ANTÓN: Yeah.

MS. MANFRA: And so, by making it so tailorable and so based on risk for every different organization or enterprise or domain that enables you to kind of grow it and evolve it.

MR. KERRY: Yeah, very much so and now I can't resist, by being in here, four years ago, I talked about the opportunity for the NIST framework to help to develop standards; to promote awareness and I think, from my standpoint, I think it's succeeded in that far beyond what I expected at the time in terms of the uptake, the adaptation in a variety of places in other countries; in industry sectors and so I think it's succeeded in doing that. And I think one of the other beauties available though was originally nominally named, directed at critical infrastructure. It's applicable beyond that and that's something that's more explicitly incorporated into the newer iterations. This can be used, as Annie said, in a lot of frameworks, but I think it scales very well and it adapts very well and that was the intent. Not have it be one size fits all. Not have it be a checklist. I remember talking to Pat Gallagher, he said, we don't want our -- we don't want to replicate fisma, which has people say we're doing a lot of reports, but not focusing on the outcomes.

MS. MANFRA: It's also elevated the discussion as an engineer. We're not -- there's an expectation that you have basic security in your systems.

MS. ANTÓN: Yeah.

MS. MANFRA: And that's -- we've come a long way in that regard over the past four years, I would say.

MR. KERRY: And there's a basis to talk about it. There's a structure.

MS. MANFRA: Absolutely.

MR. KERRY: We'll talk about it.

MS. MANFRA: Absolutely.

MR. WHEELER: Crucial in this --

MR. KERRY: And add, we're running short on time. We'll do two or three more questions, but I want to wrap this up. Wait, don't tell me style, so we'll wrap it up. It's Valentine's Day 2019, what are we going to be talking about in cybersecurity? What are good meaning of success is, what do you foresee as the challenges? Sir.

MR. FELTMAN: My name is Legger Feltman. I'm working for a consulting company, Jetu and NIST is our major client. So, I'm working on a cybersecurity framework on every day base. So, I like return back to cybersecurity and I have two questions. One question for Jeanette. What you expecting from this live, I would say, document in the future? What do you want from DHS point of view to be included in future cybersecurity framework publications, first of all?

MS. MANFRA: Well, we've been working with NIST in the current update and I think some of the areas were around thinking about control systems and thinking you've got enterprise works, but you've got control systems. How do they think about risk? There's a variety of areas. We've gotten a lot of, you know, NIST has gotten a lot of good comments that we're still working through, so I think it's sort of early to say -- to tell them what the next update, you know, what more we might want. I think I'm pretty pleased with how this is going. We have a very, very close partnership with NIST and we work very closely with them on this.

MR. FELTMAN: I hope we work with you in future, but I have a question for Annie. A very quick question.

MR. KERRY: Last question, please.

MR. FELTMAN: Yes.

MR. KERRY: We have another --

MR. FELTMAN: Very quick question.

MR. KERRY: Did you have a question? You get the last question, let's say. I was right. I got to make it one question per person because we're running out of --

MS. MANFRA: He said afterwards.

MR. FELTMAN: It's very important.

MR. KERRY: Okay.

MS. FESSEL: Thank you. Thank you very much for everything you shared with us. I'm Marina Fessel. I'm Afghan/American journalist. I'm wondering if you can comment about what are your findings pointing to in terms of the 2018 elections here. I read this morning in the paper about some of the election workers don't have the budgets or clearances necessary to make the adjustments. Are you concerned about this upcoming election?

MS. MANFRA: I think the intelligence community officials really laid out pretty clearly and then you have the World Wide Threat Assessment that's unclassified that can go into more detail. I can -- the areas that I can handle and have authority to handle clearances, again, ensuring that they have the ability to and the access to the information. The services, we have a lot of services that have been developed for federal government entities that are available to them, that many of them are participating in that can help those who may have some challenges around resources. So, I guess, I'm sort of sum it up with that.

MR. KERRY: Okay, well, we need to wrap it up. So, February, Valentine's Day --

MR. WHEELER: Are you going to start at this end?

MR. KERRY: -- 20, the 28th, I'm going to start at that end. Yeah.

MR. WHEELER: So, as I recall, wait, wait. Don't tell me. It has to be short and pithy.

MS. MANFRA: Yes.

MR. WHEELER: Right? More. (Laughter)

MS. MANFRA: And less. (Laughter) And somewhere in between.

MR. KERRY: Oh.

MS. ANTÓN: (Laughter) No.

MR. KERRY: All right, you got to specify. Well, first, I mean --

MR. WHEELER: I think that the reality is that I guess I said at the outset, cyber isn't something, it's everything. Yesterday, we heard the testimony that we are under attack. It is going everywhere and what will we be talking about a year from now? How it is in more everywhere? So, more.

MR. KERRY: Okay.

MS. ANTÓN: I hope that we are talking about the fact that we will have better attribution and that we will know exactly where our attacks are coming from and we can have some kind of consequences for that.

MR. KERRY: Jeanette, you get the last word.

MS. MANFRA: Pithy, I would hope that we've realized that collective defense model that we talked about and that we are raising the costs for adversaries and that we have defenders that have what they need to defend their networks and protect those critical services and functions.

MR. KERRY: Well, I want to thank everybody for being --

MR. WHEELER: Wait a minute. Wait a minute. Whoa, whoa, whoa, you don't get off (laughter).

MR. KERRY: I'm the moderator.

MR. WHEELER: Come on, give us one. I year from now when you're doing the fifth anniversary, Cam, what's it going to be?

MR. KERRY: I'm -- so, I guess my hope is that we see more adoption of NIST worldwide. And that we make some significant progress in working with like-minded countries on collective defense; that we've got shared networks; same threats; same technologies. We ought to be working together hand-in-hand. So, I was getting to the thank yous. Thank you all for being here. Thank you for your questions. I'm sorry we didn't get to all of them. Thank you to our panelists and especially to Jeanette Manfra for being here today and talking as much as you have. (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, 2020