Brandon Wales, Acting Director
Cybersecurity & Infrastructure Security Agency
U.S. Department of Homeland Security

Cyber Media Forum
Project for Media and National Security
George Washington School of Media and Public Affairs
Howard Baker Forum

13 May 2021

Mr. Ensor: Good morning everybody. I'm David Ensor, the Director of the Project for Media and National Security and on behalf of the George Washington University project and also on behalf of the Howard Baker Forum, welcome to our conversation today on cyber media related issues. I'm going to introduce our moderator today who is my friend and colleague Frank Sesno. Many of you know him from television days but he's also been until recently the Director of the School of Media and Public Affairs at George Washington University. Frank is going to ask a few questions of Mr. Wales and introduce him, and then he'll open the floor for questions from all of you.

Moderator: Thank you very much, David, and I want to start by thanking David for all of his hard work as the Director of our Project for Media and National Security and certainly national security is right center stage these days and the notion of national security [inaudible] very dramatically as we think about the cyber threats that we confront.

We're here to have a conversation with Brandon Wales. He's the Acting Director of the Cybersecurity and Infrastructure Security Agency. Mr. Wales, good day to you. Thanks for joining us.

Mr. Wales: Thank you, Frank. It's great to be here.

Moderator: Well, it's great to have you.

Mr. Wales, why don't we begin, obviously there's no shortage of news these days. The President's signed an executive order. You've already put out a statement on that. We know the Colonial Pipeline remains, it's coming back but is impaired and we've certainly seen the effects throughout the Southeast and Eastern Seaboard all the way up to New York. DarkSide has claimed to attack three more companies. So can I just start by asking you what is the status of this thing as we now know it? And what do

we know about what's happened to Colonial?

Mr. Wales: What happened to Colonial is something that happens to companies in all sectors, in public sectors across the country on an all too frequent basis. Their systems were compromised by criminal ransomware organizations working to monetize cybercrime and they were able to disrupt their business network. According to the company out of an abundance of caution and fearing that there could be compromises to their operational technology network they shut down the systems that actually control and monitor pipeline operations. Now we've seen over the past several days the impact that could have on critical functions that enable our economic well-being and other segments of society.

This is a problem for Colonial today but it's a broader problem for the country.

Moderator: As I mentioned you put out a statement following the President's executive order this morning. You call it an important step forward. What will be the practical effect for you and CISA from this executive order?

Mr. Wales: I think this executive order is absolutely critical to our ability to continue to make advancements in cybersecurity at the federal level. When Secretary Mayorkas took over as Secretary several months ago, one of the first things I told him was that we needed three things to make improvements based on what we had seen in the aftermath of the SolarWinds compromise and what we had observed over the last several years of working to support cybersecurity for federal agencies.

We needed additional authorities to be able to deploy the right technology and to be able to more proactively work through threats in the federal space, and we received most of that in the National Defense Authorization Act passed earlier this year.

We needed additional resources that serve as a down payment for critical advances in technology that had been lagging behind where they needed to move.

And third, we needed the entire government to be moving in the same direction. We needed clear direction from the White House to the federal agencies that cybersecurity of federal systems was a priority and to outline some of the essential steps they needed

to take. This executive order checks that box in a really big way. I think it's going to be critical for our ability to work with our federal interagency partners to more secure networks, architectures. It will be critical to ensuring we have the right monitoring of federal networks given an occurrence threat. And importantly, it's going to be using the federal government's procurement power to drive software development in a more secure direction. That will pay huge dividends for beyond the federal government for all customers of those same software and hardware vendors.

Moderator: What this executive order doesn't do, however, is create a process by which a Colonial Pipeline which share the information with you that arguably you should know if you're going to protect critical infrastructure within the government and elsewhere. What's needed to make progress on that front?

Mr. Wales: I've said publicly that CISA to do its jobs and for the federal government to broadly execute the mission that the American people want it to do which is to protect critical infrastructure broadly, we need information from victims of cyber incidents so that we can share that information and raise the baseline of cybersecurity. But to do that we need Congress to take certain actions to require cyber incident notification. There appears to be a move in some directions, Senator Warner has legislation he's working at and others, and we are extremely eager to work with Congress on what that looks like and how to do so responsibly. I think this is designed to help industry. It's not designed to be onerous. But the more information that is shared with us the better job we can do protecting critical infrastructure.

Moderator: At the outset I should have said to the full group here that our conversation obviously is on the record. It is not for broadcast, however. I also want to point that out. Lots of questions in the chat and anybody else that's got one just let me know. I'll come to those in a few minutes.

In your statement you point out that the executive order the President signed puts CISA squarely in the middle where it belongs. You said it will bolster your efforts to secure the government's networks, it will provide greater visibility into cybersecurity threats, and it will drive improvements in security practices. You talked about catalyzing progress in all of these areas and more. How quickly will these changes start to take

place?

Mr. Wales: Some changes can take place starting immediately. Things like notification to CISA and the FBI when contractors for the federal government start to see disruptions or cyber incidents on their networks. Other parts are going to take time to develop and roll out. New technology, new routing requirements. And then some will take even a little bit longer. How do we change the culture of software development for the large number of vendors that provide information technology to the federal government. But we think that there is work underway right now that this executive order will kind of accelerate progress and we're really happy to see it.

Moderator: You told the Homeland Security Committee this week in testimony, you were talking about the cyber response and the recovery from that [inaudible] that has the resources and the capacity to respond rapidly to what you called a catastrophic cyber incident. Is the Colonial Pipeline a catastrophic cyber incident?

Mr. Wales: When we look at a catastrophic cyber incident, one of the factors that we're looking at is does it overwhelm our ability to provide response support. And an attack on a single site, even if we were asked to provide incident response assistance to that entity would not likely overwhelm our ability to provide that kind of support. I think what we were envisioning is the kind of incidents that would affect multiple entities simultaneously with a large number of requests for assistance across the country that would begin to strain our ability to provide incident response resources to those entities given our organic capacity and the kind of surge support that we already have built into our programs.

So I'm not sure that Colonial will meet – it's certainly a significant incident but I don't know that it would necessarily meet the kind of criteria for the activation of the fund which also requires us to be kind of, which strains our ability to respond.

Moderator: How real do you then consider the possibility of a catastrophic cyber incident?

Mr. Wales: My sense is that the likelihood is increasing almost every day. We are seeing more broad-based cyber incidents from

our adversaries who are growing more aggressive. When you think about the scale of incidents like SolarWinds affecting almost 100 entities across the country, you think about the scale of what we saw another set of actors do exploiting vulnerabilities in Microsoft Exchange products, impacting thousands and thousands of exchange servers around the world and in the United States. So the kind of broad-based attacks that we're concerned about, we're seeing the prelude to that today.

Moderator: DarkSide has claimed it's attacked three more companies. What do you know about that?

Mr. Wales: I'm not prepared to comment on that right now.

Moderator: Do they remain active?

Mr. Wales: DarkSide ransomware operator is showing no signs that they're stopping what they're doing. I think we have held consistently that as long as the business model for ransomware remains viable, it will continue to be used. They will continue to grow. We have seen that the sophistication of ransomware operators is increasing. The pace of attacks is increasing. The severity of attacks is increasing as they go after more significant targets. We've seen in the middle of the pandemic ransomware operators go after hospitals, a particularly egregious attack. We've seen them go after schools, given the move to remote learning. We've seen them go after manufacturing sites, local police departments like right here in DC. And so this is a scourge that is not going to be easily eradicated.

Moderator: The President said there are DarkSide operators in Russia. What's the connection with the Russian state?

Mr. Wales: I'm going to defer that question to folks who track the threat actors in a bit more detail, like members of our intelligence community and the FBI. But what I can say is that these operators have typically operated from areas where in times the nation states have not cracked down on the cybercrime coming from their territory, and that kind of exacerbates the challenges that we're facing here.

Moderator: It sounds like a yes.

Mr. Wales: I will let others say yes, but this is a significant challenge.

Moderator: Let's talk about the funds for a moment and how that's going to work and how the $20 million pending in the Senate bill could possibly be enough to stand up to the challenges that you face.

Could you start by talking about how the fund will be deployed and determined with local, state and private entities?

Mr. Wales: The first thing I'll say is the fund is designed to provide additional resources on top of the baseline capacity that CISA has to respond to significant cyber incidents. We do have a fantastic group of individuals who work in response to cyber incidents every day in the federal government, in the state and local government, in the private sector when we're requested to do so. As part of the America Rescue Plan Act we actually got additional funds to bolster our capacity to perform hunting incident response. So we already have a fair amount of resources dedicated to this effort and rightly so.

The fund, and again this is just the first year, was designed to see how this would operate, so we worked with our Office of Management and Budget last year and earlier this year and as part of the FY22 President's budget request we'll see an initial $20 million for cyber response and recovery fund to basically allow us to kick its wheels, see how it would work, and prove the concept. But you're right, in future years, it may not be sufficient to deal with the scope of the problems and the kind of cyber incidents that we are grappling with.

But today I cannot tell you exactly how it's going to be used between federal, state, local and private, it's really going to be based upon the incidents that we're faced with. When we have significant cyber incidents that's affecting multiple entities, we want to make sure that we have the right resource mix to bring to bear, that we're able to deploy the right types of protected technology or the tools and sensors that we use as part of our incidence response kit. And we want to make sure that we're there to support the recovery effort.

That being said, given the types of entities that most often come to us for assistance like public sector entities, local communities, state governments, other federal agencies, these are ones that may not often have the kind of organic resources or the ability to tap into top tier cybersecurity incident response

firms. So this fund will provide needed resources to ensure that we can provide those entities the response at scale that may be needed.

Moderator: Take for example the attack the city of Atlanta experienced. They would come to you and say we need some money for some of these things and that would be available presumably? And to what extent? Because that was a very substantial, very significant act.

Mr. Wales: Exactly. I think a lot of this will be dependent upon the exact contours of what the cyber response and recovery fund legislation that implements it looks like. The kind of authorities.

Today CISA has the ability to use that fund to deploy additional resources organically from CISA to support those kind of sites. Some of the legislation that's introduced in the Senate would give us additional authorities, for example being able to potentially reimburse states for some activities that are done consistent with our guidance. So it's really going to be dependent on what the ultimate contours of this bill and whatever legislation looks like. And I think the program will absolutely evolve over time. If you look at kind of a corollary, the Stafford Act and FEMA's disaster relief fund, that has changed substantially over the 20-plus years that it has been utilized as it's had to respond to different incidents and as people learned more about the best way of managing complex natural disasters. The cyber response and recovery fund will need to be as adaptable and we'll need to work with Congress over time to make sure that it can continue to meet the needs as the cyber threats and incidents that we see are evolving.

Moderator: You just said a couple of important words. We'll need to work with Congress. This bill hasn't been passed yet. How important is it? You worked in the Trump administration, you're now working in the Biden administration. How important is it that this is a bipartisan, fully supported bill, and how likely is that?

Mr. Wales: What I can say is CISA has enjoyed extremely bipartisan support over the last several years regardless of administration, regardless who's been chairing the various committees that oversee us. Congress has in a bipartisan fashion worked to provide CISA substantial increases in resources over

the past several years. It's provided us substantial new authorities to deal with cybersecurity challenges. So I have no doubt that legislation related to the cyber response and recovery fund and other issues critical to the cybersecurity mission will be done in a bipartisan way and we will continue to use what I think are our excellent relationships with both sides of the Hill to advance the critical work that we're doing.

Moderator: If it passes and you have this fund, who decides where the money gets spent?

Mr. Wales: I believe under the drafted legislation that the President would be the one who would make the ultimate decision on whether the fund is able to [tapped] which is consistent with other similar programs like the disaster relief fund. And then once the President makes that determination CISA would work in concert with our federal interagency partners to make sure that we're bringing the right tools and capabilities to bear.

Moderator: We have a lot of questions. I'd like to go to the group now, and you and I can come back. But I see Cal was the first one in to say Frank, I have a question. So Cal, go for it.

Journalist: Hi, Brandon. Thanks for doing this. Cal Biesecker. I'm with Defense Daily.

Th $650 million in the American rescue plan, you've kind of outlined in sworn testimony sort of the broad buckets where that money would be spent, but could you be a little bit more specific in terms of the percentages of where that money is going? And also update us from the status of actually spending any of that money. And then finally, just on end point detection and response, which has been a subject in a lot of the hearings. Where are we in the early innings, in baseball terms, where are we in terms of maybe deploying that kind of technology to the extent that you envision? So a three-part question. Thanks.

Mr. Wales: Sure. I don't want to get into too close in percentages because we're still working some of the details in our kind of conversations with the appropriators and also figuring out the right acquisition strategy for some of the capabilities that we're looking to deploy. But I would say it's pretty close to the four buckets that I've outlined in previous. Maybe the first three are a little bigger than the fourth if you look back at my testimony from earlier this week.

In terms of where we are in terms of implementation, we got authority to actually execute the money only in the last several weeks as that money makes its way from Congress through Treasury and gets loaded into the account at the department. And we have been working on as we indicated, kind of our acquisition strategies for the various different proposals. In some cases we've got existing contracts that we can use to put that money on quickly. In other cases it's going to require new contracts be put in place and that will obviously take more time. That funding's got kind of a two and a half year life span but we're working aggressively to try to get the majority of that money out the door in our first year of operation, at least for those that have major contractual requirements.

In terms of EDI, this is an area where you're likely to see substantial differences among the agencies. Some agencies have already started to deploy various types of [import] detection tools on their networks. Others have not yet. That's obviously one of the kinds of capabilities we want to bring to bear using the money in the American Rescue Plan Act and we're starting to work through what exactly that will look like. But importantly, we need to make sure that we understand the kind of architecture that would work with things agencies are already doing. How do we tie that together on the back end to ensure somebody has the right level of access, that agencies can benefit from it.

So our goal is to get this money out quickly but it's also to get it out right and to execute it smartly, to make sure that we have the appropriate plan in place, that we have the appropriate back end prepared to receive the kind of information that will come out of these new tools and sensors.

So there's a lot of work ahead of us but I'm confident that the team is going in the right direction.

Moderator: Eric Geller.

Journalist: Thanks, Brandon for doing this.

I want to ask about the EO. This is obviously not the first EO to push agencies to improve their cybersecurity practices. It's not the first one to set ambitious deadlines. But when you look at the culture inside the agencies a lot of employees and even senior managers just don't care about IT or cybersecurity and

they just don't see why they should have to do these things. Why is this time different? Why should we believe that this is the time that OMB and CISA are finally going to overcome the recalcitrance inside these agencies?

Mr. Wales: I think that's a good and a fair question. What I can say is the following. One, I think there is far more focus in the current White House in terms of achieving, getting positive outcomes out of this executive order. There has been substantial focus before the executive order was signed kind of laying the groundwork with agency leadership. There was a lot of support for getting the resources through things like the American Rescue Plan Act that will help to accelerate a number of the initiatives within the executive order. And I think there's just going to be a lot more diligence in follow up. I think the combination of leadership at both the White House inside of OMB using their power of the purse to push agencies in a positive direction and the work that CISA is doing to support them means that I think this time is different.

Moderator: Jason Miller, you're next. Federal News Network.

Journalist: Brandon, thanks for taking the time. And actually, a follow-up from Eric's question.

It seems like when you read through the EO, and I was talking to some folks in industry, they're like I was looking at all the deadlines and they stopped counting at 70. I was like oh, this was before I saw the EO. It just seems like what this EO is trying to do is eat the elephant in one bit, drink the ocean in one swallow, use the bad analogy that you like.

Was there any thought to do a cyber sprint? Like similar to what happened in 2015 after the OPM breach where OMB and CISA or NPBD at the time, said we're going to do two things that are going to make a big difference. Then we're going to do two other things that are going to make a big difference. It seems overwhelming for agencies, and I can see them going I just can't keep up.

Can you walk us through the thought process of why not take smaller chunks versus this large chunk?

Mr. Wales: Sure. What I would say is the executive order is ambitious but it's ambitious because what we have seen is we don't have time to continue to wait. This is not a, the

cybersecurity challenges we face today are not going to get better in two or three years unless we make significant changes to our approach and really push agencies in a more positive direction more quickly.

I think the White House is seized by that urgency and this executive order reflects it. As the lead agency for implementing a large number of the items in there, I'm acutely aware of the challenges that that poses. We have been working all along as the drafting process for the executive order has continued to make sure that we are prepared and we're beginning to move out on various of the tasks even while it was still in development, to make sure that we're primed and ready to go. I think our first deadline in CISA is 15 days from signing, so that stopwatch has already been – I guess the firing gun in the race went last night and we're moving out aggressively now.

I think the community is right to say this is ambitious, this is big. But I think that just reflects what's needed to confront the cybersecurity threats and risks that we face right now.

Moderator: Justin Katz, you're up next.

Journalist: Justin Katz from Federal Computer Week.

Following up on Jason's question, I wanted to specifically call out the deadline for, I think it's a six month deadline on multi-factor authentication, end point detection and encryption. I believe it calls all across the federal government, To call that ambitious, just from my purely lay perspective, that's almost an understatement.

I guess I just wanted to hear, how confident are you that in six months all of those technologies can be laid out across the federal government? I just wanted to call attention to that deadline in particular.

Mr. Wales: What I can say is, although a lot of tis is ambitious, we're not starting from scratch. There has already been a significant move towards multi-factor identification across the dot-gov. Already more than 95 percent of all network traffic in the dot-gov is already encrypted. So the idea of getting to a more kind of, of hitting the targets identified in this executive order are a lot different when we're starting from the space of having worked a lot of these issues over the last

several years. But this executive order allows us to kind of finish the work.

That being said, you're right. Some of the things in here are going to stretch the system. They're going to require us to push hard. And the federal government needs to be ready to respond. And we're seeing some things like [inaudible], but what the consequences are if we don't.

Moderator: I just want to follow up very briefly these couple of last questions.

To get these gigantic agencies, departments and others into compliance, you can issue EO's as you've done. You need carrots and sticks. What are the sticks and are you going to use them?

Mr. Wales: Sure. And CISA has already been working with OMB in this area for a while. We started issuing binding operational directives I think going back five or six years now, requiring agencies to make targeted improvements in their information security practices. Everything from closing vulnerabilities to removing certain high risk software. What we found is the type of approach we've taken, collaboratively working with agencies, we've been able to achieve adoption of our approaches in rapid time, both over long term, more sustained kind of issues and kind of quickly during significant cyber incidents like SolarWinds or the compromises of exchange vulnerabilities.

I think partly this is the White House holding folks accountable. It's OMB using the power of the purse. So I think there are both carrots and sticks that we are using to achieve the goals of the executive order.

Moderator: Kimberly Underwood from Signal Magazine.

Journalist: Thank you, Mr. Sesno, for moderating. Thank you, Mr. Wales for your time today. I'm Kimberly Underwood from AFCEA International Signal Magazine. I wanted to ask you a little bit more about CISA's increased responsibilities under the EO. Specifically in regard to contract terms and language to aid incident response. Can you talk about kind of your initial thoughts there, of how you'll help strengthen the language of contracting. What are the considerations. And I guess how it will be different than kind of what's happening now. Thank you.

Mr. Wales: Again, this is an area that we have worked historically. For example initially several years ago we started working on contract language related to cybersecurity requirements for government contractors. I think this language in the executive order focuses, for example on making sure that the federal government and CISA and the FBI in particular are notified when vendors or other contractors for the federal government have incidents that they're seeing in the federal government. That's directly coming from our experience with some of the challenges we had in the early days of the SolarWinds incident.

But I think that we have experience in terms of working with the Office of Federal Procurement Policy, the GSA and others, OMB, who have responsibility for federal contracting to work to promulgate better guidance to agencies as they put in place contracts or if contracts need to be modified to ensure that the federal government is aware of the cybersecurity risks that they face.

Journalist: Have you had any initial feedback from industry as far as kind of what kind teeth or strength that this contract language may have? The responsibility on their side.

Mr. Wales: I think that we're still working through that and I'm just not prepared to get into the level of coordination we've had with the private sector on questions like that.

Moderator: Dmitry Kirsanov from TASS.

Journalist: Good morning, Mr. Wales, thank you so very much for doing this, for taking the time.

I wanted to ask you about Russia, not surprisingly. This states against states cyber operations, spy versus spy, would not go anywhere I think. We would hardly see stuff like that disappear. But I think that does not necessarily preclude that even the adversarial states from cooperating in fighting cyber-crime.

So my question is, why is the United States refusing or ignoring Russia's [inaudible] to maybe trying and cooperate in fighting groups like the DarkSide? Or am I reading this incorrectly? Is the Biden administration ready and prepared to work with the Russians on things like that?

Mr. Wales: I will defer some of that question to law enforcement agencies that have the responsibility for dealing with international cyber-crime. What I can say is that the administration has worked in partnership globally to take on cyber-crime. That comes from the Department of Homeland Security, Secret Service, ICE, Homeland Security investigations that go after international money-laundering operations and others. And what I can say is there are real questions about the level of cooperation that we get from some countries when we have identified the cyber criminals operating from their territories. And until all countries are willing to take aggressive action against people who are using their territory as a safe haven to launch cyber-crime operations against the American people, against our critical infrastructure, against our public institutions, we are going to have real challenges and those threats and risks are going to increase.

Journalist: Do you mean that Russia is among those states that --

Mr. Wales: I'm not going to answer that question. I'm going to let the people who are better prepared to discuss the specifics, so I'd refer your question to the FBI.

Journalist: Has CISA had any direct engagement with the Russians, with your Russian counterparts over this matter? Do you plan to reach out? Do you plan to --

Mr. Wales: That's not our role. I will say historically we have had contact with Russia on certain cyber-defense issues and certain information is shared with the Russians related to indicators of compromise that we have observed.

Moderator: Presidents Putin and Biden have spoken. Is there any reason to believe that there's any progress that's been made as a result of those conversations and some of these issues you've just discussed?

Mr. Wales: I'm not going to answer that question.

Moderator: I thought you might not, but I thought I'd ask.

Aaron Schaffer with the Washington Post.

Journalist: Thanks. I had a few questions mostly focusing on

critical infrastructure and the Colonial Pipeline.

First, I guess I was wondering if you could confirm whether CISA's policy is still to not recommend paying ransom, and whether you could confirm whether Colonial Pipeline has paid a ransom.

Mr. Wales: I can confirm that we recommend against paying ransom because it just feeds the business mode. I cannot confirm or deny whether Colonial paid the ransom. Only Colonial would be able to answer that question.

Moderator: Geneva --

Journalist: Good morning. Hi, Brandon, thank you for this and thank you for having us all.

You had mentioned that you haven't yet received technical information about how DarkSide or the affiliate had gotten into Colonial. Have you now gotten that technical information? And if so, what has it shown you and what would you want from that in order to warn other operators that this could happen to them?

Mr. Wales: Late last night we have received some indicators of compromise from the incident at Colonial. We are working with the FBI to get that information out today in a more broad way. It doesn't tell us the complete story yet but it does provide at least initial indicators of where and how the attack took place. And we're again working to share more information publicly and we're looking to do that as soon as today.

Journalist: Can you give us any hints?

Mr. Wales: No.

Journalist: What's the reasoning of wanting to get that information out there?

Mr. Wales: Again, the number one question that people have is what were the tactics that the adversary used? How did they get inside the network? Was it a fishing email? If so, how was it constructed, how was it designed? Did they exploit a vulnerability in a piece of software. All of that information allows other critical infrastructures to better protect themselves. People are looking for kind of indicators of

compromise they can load into their network intrusion detection and intrusion prevention systems. So we want to get as much information about the tools and the tactics that the adversary used because all of that is used to prevent and to actually find additional evidence of compromise.

And importantly, in a lot of cases ransom operators will often compromise a system and then several days later actually execute the ransomware attack. So there could be potential victims that have initial indications of compromise that they don't know about yet, but if they were to see that, could prevent the actual ransom from being executed. So getting that information quickly is absolutely essential. Even a couple of days delay could be the difference between other entities having the ransomware activated on their networks and not.

Moderator: Lamar Johnson.

Journalist: Thanks for having me. My name's Lamar Johnson. I'm with MeriTalk.

My question is based off the last six months of the last year and what we've seen more and more attacks, SolarWinds, Microsoft, as well as all the ransomware. To what do you attribute the increased attack frequency, and beyond, what's in the [inaudible]? How does CISA plan on decentivizing these sorts of attacks from adversaries?

Mr. Wales: The first thing I would say is the last six months we have discovered a lot of cyber incidents, although in a number of cases those cyber incidents actually started much earlier.

But I think it shows a couple of things. First, it's showing that our adversaries are growing far more aggressive and far more sophisticated. They are looking for and finding or in some cases stealing information on critical vulnerabilities in essential software. When you think about what they did, just looking at three recent incidents - SolarWinds, Microsoft Exchange, and vulnerabilities being exploited in pulse connect secure devices, our adversaries have identified critical pieces of technology that oftentimes are areas of concentrated risk within networks, and have targeted their efforts to find vulnerabilities or in the case of SolarWinds to create a vulnerability within those critical devices.

And we need to be prepared to respond. We need to be prepared to identify those devices more quickly and develop ways in which we can ensure a greater degree of protection or additional controls and monitoring around those devices. And there are elements within the executive order that ask us to do that for the federal government. Identify those areas of concentrated risk. Identify those critical pieces, those critical products and software that could be of areas of concentrated risk, and then work with agencies, work with NIST to ensure that we have the right level of security controls around them.

Moderator: David Jones.

Journalist: David Jones from Cybersecurity Dive. A couple of quick questions.

I wanted to get a sense, the government's been encouraging companies to be more forthcoming in talking about their experiences with intrusion attempts, that type of thing. And I'm wondering, have you gotten a lot more feedback from companies, critical infrastructure providers, about issues, vulnerabilities, intrusion attempts, that type of thing, over the last few months since SolarWinds? And I'm wondering what are you telling them in terms of are they not practicing good cyber hygiene or do they need better technology? Can you give us a sense of that?

Mr. Wales: Your question is challenging to answer in a general way. What I can say is that we have in a lot of cases developed strong operational partnerships with critical infrastructure entities, in some cases who are sharing unique information with us that is allowing CISA, the FBI, the intelligence community and other [inaudible] companies to take more aggressive action to protect our networks. But that is not consistent enough. It's not broad enough. Which is why we support efforts to require more cyber internet notification to the United States government.

When it comes to kind of our engagements with companies, we're not there to point blame, to say you failed at cybersecurity. When we go in and work with a critical infrastructure entity we are there to support them and enable effective cybersecurity practices. Sometimes we get asked to provide reviews of their network architecture, their cybersecurity practices, conduct pin testing or look for exposed vulnerabilities and we'll do so. And then work with that entity to provide advice and recommendation on how they can make improvements. But for us, this is a matter

of kind of close partnership and collaboration. This is not a matter of kind of us trying to revictimize or blame the victims of cyber incidents. They're already dealing with enough challenges within their own organization. So when they come to CISA we're there to support them.

Journalist: There's a report that just came out from Bloomberg that Colonial did pay a ransom of $5 million, according to the report. And according to the story it says it was paid on Friday. IS that something that you were aware of? That has been confirmed on your end? Can you say anything about this?

Mr. Wales: As I said, I have no knowledge of whether a ransom was paid, how much was paid, if it was paid, when it was paid. So I can't answer that question.

Moderator: Generically on the ransom issue, I mean there are hundreds of millions of dollars that are flying around because of this, and is there anything that you or the government can or should be doing that isn't being done now to cut off this funding? Or is this just sort of the wild, wild west and if somebody's got enough pressure in enough places these ransoms are going to continue to get paid like this?

Mr. Wales: Unfortunately, right now we are in the latter category. As you said, hundreds of millions of dollars are being paid to ransomware operators and that is feeding this business model. It's causing more ransomware incidents to happen. And it's why we're in the position we're in now.

I think there is active discussion in the federal government about what more we can do to disrupt that business model. What more we can do to disrupt that financing model. Because we recognize that companies are often in a very challenging circumstances, that paying looks like an extremely attractive option to get their networks back up. But the long term implications for our country are profound. So we do need to look for additional tools to tackle this problem.

Moderator: Is the we the United States of America or is the we some new and forcefully constituted international, multilateral group that is going to have a meaningful impact here?

Mr. Wales: There are certainly multinational dimensions to this problem. We've signed communiques with foreign partners on this

subject. It is not a problem that is isolated to the United States, although we tend to be the center of gravity for targeting by ransomware operators. This is something that affects countries throughout the world. It's going to take a multinational solution to really address at the scale and complexity that this problem is.

Moderator: So when you're saying we are looking at new things that can be done --

Mr. Wales: The United States government is looking at what can be done, but it's going to be done but it is going to be done in light of what our relationships are internationally, what tools we have and how those would work in collaboration with our foreign partners. We work collaboratively with a number of our international cybersecurity partners on securing information on ransomware, how to get ahead of these problems. Our law enforcement community is working in partnership with international law enforcement elements to tackle ransomware. So just because the United States government is looking at it doesn't mean that we're not going to be working in partnership with other countries on the execution and implementation.

Moderator: Luke Barr is up next.

Journalist: Are you frustrated, because you touched on in your testimony earlier this week, that I [inaudible] elaborate on sort of the information sharing in the sort of moments just after the cyber-attack with Colonial. Are you frustrated that they otherwise wouldn't have reached out to you if the FBI didn't bring you in?

Mr. Wales: No. My sense is that this shows that inside the United States government the system is working as it was designed. That a call to one is a call to all. And that it reflects the strong relationship that we have with the FBI to take aggressive action together when we get awareness of significant cyber incidents. There are many times when CISA is made aware of a cyber incident and we bring in the FBI. This was a case in the other direction and those happen often too.

My biggest challenge, my biggest concern, are those companies who don't report to anyone in the United States government, and the United States government is completely blind to what is happening. Because then we're in an extremely weak position.

We're not able to use the information from that incident to help and benefit other potential victims. That just weakens our overall cyber posture across our entire country.

Moderator: Alyza Sebenius, you're next.

Journalist: Thanks for being with us today.

CISA is in the midst of a ransomware sprint and I'm interested in how the Colonial attack might affect the end of that sprint and what you guys are looking to do.

Mr. Wales: I think it helps the sprint in the sense that a lot of what we are doing, particularly in CISA, is designed to raise awareness and push people to take the issue of ransomware more seriously and begin to deploy the types of protection inside of their networks that will make a ransomware operation less likely and less impactful if it does happen.

So an issue like Colonial that could really kind of galvanize the country into recognizing the level of risk that we're facing, that it could benefit us in the sense that more people may take this issue seriously and may begin to do the kind of things that we want them to do that we've long recommended that they do. So I think we'll see how that develops.

Moderator: There's been some writing about this specifically with relation to pipelines, where we're seeing this very dramatically paraded in front of us, the consequences of this.

Should the federal government, TSA or anybody else, be regulating pipeline security?

Mr. Wales: The Transportation Security Administration does have certain security directive, regulatory authorities related to the pipeline sector. What I can say, and this echoes comments that Secretary Mayorkas made at the White House two days ago, those conversations are ongoing. How do we best use all of the tools at our disposal for both [inaudible] as well as a regulatory perspective to provide a level of security that we need given the threats that we're facing. So I don't want to prejudge where those conversations are going, but there are a lot of conversations right now on that exact issue.

Moderator: But clearly what you're saying and what the Secretary

is suggesting is more needs to be done. We need to have more awareness, information and perhaps oversight.

Mr. Wales: More clearly needs to be done, absolutely. And I think the question is what are the tools that we're going to use to get those outcomes that we want.

Moderator: I know Cal has a follow-up.

Journalist: Brandon, we already pointed out that the executive order doesn't talk about breach notification. Another thing that has been talked about going back to the Obama administration to the Trump administration is a deterrent policy and of course there's nothing in this executive order about this and a senior administration official speaking to reporters last night didn't talk about deterrence either.

Can you speak to that at all? Is anything going on within the administration in terms of how to prevent these kind of things not just with better technology and best practices and what have you, but finding ways, whether it's a nation state or a criminal gang, to deter from it even happening in the first place? I don't know if that's in your lane or not.

Mr. Wales: CISA is involved in interagency conversations about using the beset mix of capabilities across all instruments of the United States' national power to deter and dissuade adversaries from conducting attacks. In a lot of cases that informs our response to cyber incidents that we face. It informs activities that we took in response to the SolarWinds incident, the actions that were taken against Russia in response to their election interference. So those conversations are active and ongoing, but I will let the White House talk to the broader work that the administration may be doing on a broader cyber deterrent strategy.

Moderator: Jason has a follow-up.

Journalist: I want to go back to the agency's effort. There's been a lot of work as you said over the last year or more to kind of really fine tune agency networks. When you look at the deadlines which you point out to federal CIOs and CISOs, this is, most important maybe isn't the best word, but here's where you really do need to start. If you can only do one thing in the

next 60 days, here is that one thing. I know it's hard, every agency's different. But like you guys have put out fire drill after fire drill after fire drill over the last three months with the emergency directives and now this. So how can a CIO or CISO really get their head around what do I need to do next?

Mr. Wales: I'm not going to be here today [inaudible] what aspect of the executive order is more important than the other. I think if you read the executive order in its totality, it is designed to be a kind of cohesive examination of the various things the federal government needs to do to make progress in our cybersecurity. I don't think there's any one piece that is more important than the other. They are designed to work together. They are mutually reinforcing. So the idea of improving log-in requirements is important, but if we don't have the tools and the systems in place to actually utilize those improved network logs, they're not going to be valuable. So it's all a matter of kind of how you bring these capabilities together to get the desired outcome. I think that the White House has been thoughtful and the interagency process has been robust in working through the executive order and the kind of timelines reflect what we think are achievable milestones in our ability to kind of get to the type of cybersecurity outcomes we need.

Moderator: Aaron?

Journalist: I had a couple of quick questions about critical infrastructure.

First, what steps is CISA taking to deter ransomware attacks specifically in the critical infrastructure sphere? And also, is it true that pipeline operators and owners don't have to have a cybersecurity plan or anything like that?

Mr. Wales: I'll answer your second question first, and refer you to the Transportation Security Administration who has the responsibility for pipeline security about any specific requirements that they may face.

What I would say is there are a lot of ways to deter malicious cyber activity and there are a lot of parts of the federal government that work on those various, who have those various capabilities and authorities. CISA is to work deterrence by denial, by improving the security and resilience of our systems. We make those systems less likely to be targeted because they

could defeat or respond quickly in the face of cybersecurity incidents. So that is the aspect of deterrence that we work. It is one that is extremely challenging, requires us to raise the cyber baseline across a complex set of critical infrastructure networks across this country. It's a problem that we have to work every day and it's one that will not be completed anytime soon. But I think there's a lot of work going on right now that gives me confidence that we are working in the right direction not just benefits that will come out of things like the supply chain aspects of the executive order but work that the White House has initiated related to industrial control systems, cybersecurity in the electricity sector and the pipeline sector was already up next, so we've got work that's about to kick off to make significant improvements in our ability to understand and protect pipeline networks, and then moving up to the water sector and others. So there are a lot of initiatives in this vein and our goal is to see them through.

Moderator: I'd like to give you an opportunity to make a concluding thought here. We bring these groups together and journalists together in forums like this so we can do much more than have a news conference, but have a real conversation. The Project for Media and National Security, we're committed to connecting the public with policy-makers through the journalists who do this as a living to enhance public understanding.

Is there a thought that you've got that we should all have in mind, what the public needs to know and be focusing on now as they're seeing this play out? They're the ones who are standing on-line at gas stations now. They're the noes who are hearing about ransom being paid for hacks like this. They're the ones looking to government for some degree of action and answers.

So what would you say, again, as a concluding thought to the public in this domain?

Mr. Wales: What I would say is, the problem is significant. The threats we face are real. And they're going to require collaborative action across the government with industry and with the American people. But it's not an insurmountable problem. In many cases, in almost all cases, basic cybersecurity processes would stop the vast majority of the kind of incidents that affect local communities and that affect people's lives in the most direct way.

Ransomware operators are not using [zero day] vulnerabilities to compromise networks. The Russian SBI are using model techniques. They're looking for the weakest link.

So in companies who oftentimes are doing the bare minimum to get their cyber systems and their cybersecurity to abate that level of cybersecurity, they will oftentimes be able to protect themselves against the most common forms of cyber-attacks [inaudible]. Which is not an insurmountable problem but it is a significant one and it's going to require our intense collaboration. That's what we're here to do.

Moderator: I want to thank you for your time. I want to thank all the journalists who are gathered here I want to thank Baker Donaldson. And I very much want to thank our colleague and my friend David Ensor who has been such a great leader with the Project for Media and National Security.

But Brandon Wales, thank you very, very much. And good luck with all you do. Godspeed and all that. Please solve all these problems.

Mr. Wales: No problem, I'll get on that right now, Frank. [Laughter].

Moderator: Thank you very much.

Mr. Ensor: Frank, thank you very much. And Brandon Wales, thank you. It's been a tour de force, it's been a fascinating hour.

Again, thank you to the Howard Baker Forum, Baker Donaldson, those folks there are making this possible and we've got another one coming.

Just one final personal comment. This is going to be my last Cyber Media Forum and I've only got one more Defense Writers Group to participate in because I'm going to ''retire'', sort of kind of retire June 4th. I'm not leaving entirely the world of work. I do consulting. I'm on a board or two. But it's been a real privilege to work in this area with George Washington University, with the School of Media and Public Affairs, with Frank Sesno and others there. I've really enjoyed it and I've so much enjoyed meeting all of you. Please stay tune for more.

My successor has been announced. He is Thom Shanker. He's the

current Deputy Washington Editor of the New York Times, a seasoned Pentagon correspondent, long time editor, terrific guy, and I know that these programs are going to grow and prosper under his leadership. So more on this later, but anyway, thank you for joining us today.

# # # #