Evolving Threats, Stagnant Policies: A Conversation on How to Secure Critical Infrastructure for the Cyber Era

Featuring Mary Brooks, RADM (Ret.) Mark Montgomery, and Kiersten E. Todt, Moderated by Martin Matishak
Introductory remarks by Dr. Samantha F. Ravich

RAVICH: Good afternoon, everyone. Thank you for coming out to today's event hosted by the Foundation for Defense of Democracies. It is Monday, November 13. Today's panel will discuss how the federal government and private industry work together to secure critical infrastructure against escalating cyber threats.

I'm Samantha Ravich, Chair of FDD's Center on Cyber and Technology Innovation. On behalf of FDD, we're happy to welcome you here, both in person and on live stream for this timely discussion.

Today's event is hosted — co-hosted with CSC 2.0, an effort FDD is honored to house, in collaboration with the rest of the former commissioners of the Cyberspace Solarium Commission.

Since the end of the commission's congressional mandate, CSC 2.0 has endeavored to preserve the legacy and to continue the commission's work, and that is what brings us here today. Few things more directly impact Americans' security and wellbeing than the reliability, availability, and safety of our critical infrastructure.

And our adversaries know that, so they are targeting our energy sector to try to put us in the dark. They are targeting our hospitals to try to weaken us. And they are targeting our banks to try to cripple our economic wherewithal. And that is not just hyperbole.

FBI Director Christopher Wray recently warned that Iranian cyberattacks against U.S. critical infrastructures may escalate as the war between Israel and Hamas rages. DHS [Department of Homeland Security] has urged critical infrastructure to get shields ready. And with Russia's ongoing war against Ukraine perpetually threatening to spill into a broader cyber war, public-private collaboration to secure this critical infrastructure is more important than ever. It is a scary world for sure but that is the world we live in.

So we are pleased to have on our stage today to discuss critical infrastructure security Kiersten Todt, Senior Advisor and former chief of staff at CISA [Cybersecurity and Infrastructure Security Agency]; Rear Admiral Mark Montgomery, Senior Director of FDD's Center on Cyber and Technology Innovation and the former executive director of the Cyberspace Solarium Commission; and Mary Brooks, public policy fellow at the Wilson Center, where her work focuses on the nexus of foreign policy, cybersecurity, and technology.

Our discussion will be moderated by Martin Matishak, senior cybersecurity reporter at *The Record* by Recorded Future. Thank you, Martin, for moderating what I am sure will be a fascinating discussion.

So one last thing before we dive in, a few words about FDD. For more than 20 years, FDD has operated as a fiercely independent, non-partisan research institute exclusively focused on national security and foreign policy. As a point of pride and principle, we do not accept foreign government funding. For more on our work, please visit our website, FDD.org, and follow us on Twitter @FDD.

So that's enough from me. Martin, please take it away. Thank you.

MATISHAK: Thank you, Samantha. Thank you for having me and for allowing me to host this great panel. Thank you all for being here and joining us online.

So let's just jump right in. I'm going to start farthest on the aisle, over at Mary. First question is to you, and I have a bit of a wind-up for it. So this weekend, my wife, I, and my 15 month old daughter are getting on a plane and flying to Illinois for Thanksgiving.

I'm going to see my extended family and they're going to say "how's work going?" I'm going to be like "it was great. Just last week, I moderated a panel about critical infrastructure security and how the administration is updating a policy framework that's a decade old."

Now, these people love me but they're going to fall asleep. So what do I tell them when they say this is why it matters, this is why this is a big deal that I did this?

BROOKS: I think that's actually a really important framing of the question because while the people in this room very clearly understand that the protection of critical infrastructure is national security, I don't think the people outside of this room have fully grasped that yet, nor have they grasped how much of, you know, Americans' national security is held in the hands of the private sector — the, you know, airline companies, the utility companies, hospitals, private healthcare systems.

And so, you know, when we are kind of talking about the centrality of these policies to our security, we are talking about policies that are, at this point, a decade old, like you said.

And the ones that we'll kind of talk about today – you know, PPD [Presidential Policy Directive 21, 41, 8 – these all date back to the second Obama administration for the most part, and they set up the relationship between the private and public sector and how the private and public sector should kind of manage this shared responsibility for protecting Americans.

And, you know, as we look at these issues and we say OK, they're 10 years old, any policy that's about 10 years old is going to feel outdated. It's going to — and the particulars have missing information about CISA, for example, or key organizations that have been updated over the last 10 years.

But why we're here today is not just because these policies mentioned the wrong organization or because there are some small particulars that need to be updated. We're here because, in the last 10 years, our understanding of the responsibility between the private and public sector and kind of the balance of responsibility and the authorities for protecting Americans has shifted.

And the point that I like to bring up is back in, I think it was 2009, when President Obama gave one of his first speeches about technology, he said, you know, we — we're the government. We're not going to regulate the private sector and basically you wouldn't want us to.

Well, fast forward to 2023, you've got this National Security Strategy that says no, we are going to establish minimum requirements because we understand how important this is, we understand that our understanding of this has shifted over 10 years.

And so as we're sitting up here now, we're not just arguing about small, boring things that would kind of spoil the mashed potatoes, if you will, but what we're – we are talking about is we have fundamentally changed how we think about these issues, and so fundamentally we need to update our security policies because we aren't protected by our oceans, and cybersecurity is something that impacts every American on a daily basis, and the physical security also of this critical infrastructure is something that we need to take into consideration as well.

MATISHAK: Before I ask you my next question, thank you for saying CISA[si-sa], not CISA[see-sa]. It is CISA. I've seen people out there and online, including my editor – it's CISA.

So you wrote a — you actually wrote a paper with Mark on this topic earlier this year of – and you mentioned PPD 21. I think the plan is to have that done by the White House by — they're doing a rewrite of it, a blow out of it, if you will – by, like, the end of the year.

Your report though, you mentioned some key principles that the administration should follow as it does this – rewrite this revision. And I just wondered if you can walk us through some of those?

BROOKS: Yeah. So let me rewind it just a little bit and talk about PPD 21. Or Mark, you look like you want to say something.

MONTGOMERY: No, no. I'm just waving to Jim Lewis

BROOKS: Oh, OK. Hi, Jim.

(LAUGHTER)

TODT: Hi, Jim.

BROOKS: Devastating. So Presidential Policy Directive 21, it was issued in 2013 by the Obama administration, and what it does is it continues a legacy of establishing certain critical infrastructures within the U.S. government and basically segmenting up the key issues areas and saying OK, there are certain members, certain government agencies, certain departments that are directly responsible as kind of a federal interface with the private sector on these issues.

And so it comes out and it establishes what are called at the time sector-specific agencies. Those are the federal interface with the private sector. Over the years, those have kind of shifted. They've been under Cyberspace Solarium recommendations, put into law by Congress in the 2021 NDAA, National Defense Authorization Act, basically that must-pass military/defense spending bill that comes out every year.

And what they say is, OK, if you are a sector risk management agency, you are in charge of a certain number of tasks – you know, helping your sector establish resilience. You're in charge of helping making sure that people know that they're going to do in an emergency. You're in charge of helping them think through how they can talk to the other entities in the federal government when something goes wrong.

So that came out in 2013. Everything shifted since. It was announced in, I believe, November of 2022 that the administration was going to rewrite this policy.

So what should they do with it? And I know that — I don't want to get too far ahead of us here because I know Mark and Kiersten will have a lot of comments as well – but one of the issues that we've seen is that many of these sector risk management agencies are simply not well-resourced. They don't have enough of kind of protections – excuse me – they don't have enough authority, in some cases, they don't have enough money, in other cases. They don't have enough guidance, they don't have enough personnel.

And so one of the really great things that this kind of rewrite could do would be to include extra capabilities to kind of help these SRMAs [Sector Risk Management Agency] do a better job of protecting the private sector, of working with the private sector to protect critical infrastructure.

And I think we'll get into some of those more as we go but I don't want to kind of do all of them here because they're boring.

(LAUGHTER)

MATISHAK: Gotta leave something for Mark's talk actually, so tight-lipped.

Mark, turning to you, you know, as far as federal bureaucracy goes, the rewrite is speeding along apparently, could be done by the end of this calendar year, though I think the original deadline was September but we're well past that.

Are you optimistic about this revision? Do you have any major concerns about what you're hearing what might be in it, what might be left out of it, that sort of thing?

MONTGOMERY: Yeah, so first, I want to absolutely agree with Mary that, you know, it does appear boring, right, talking about how the government works with the private sector to protect critical infrastructure.

But it is insanely important, right? It's about how do you protect your – I mean, there – another way to describe it is how do we protect military mobility? How do we make sure that the rail system, the port system, the aviation systems are fully functioning during a crisis? Most people would say hey, that's pretty important.

Another is how do you protect economic productivity? You know, how do you — how the financial services work so we get paid. How does, you know, how does electrical power generation work so that all of the other infrastructures are there? That's pretty important.

And these are the kind of systems we're trying to make sure are protected against an adversary. And the National Security Agency has said recently in what are clearly, like, intentional leaks or statements, that China and Russia at a minimum have placed — you know, have done what's called operational preparation of the environment. They've placed malware into those systems I mentioned. You could probably put telecommunications in there as well. So there are adversaries working very aggressively to undermine these infrastructures.

So I just want to say, at the very highest level, the critical infrastructure of our country is important and the public-private collaboration that underpins that, undergirds that, it is – it has to be done correctly.

And I am concerned. I'm concerned because, look, PPD 21, the Biden administration was not responsible in January 2021 that it was eight years old and not rewritten. That was on the previous administration.

But somewhere around January of 2022, they were accountable for this problem. It's now nine years old. And look, no policy that governs your emerging technology and how you work with it should be nine years old. Well, now it's almost 11 years old.

I think there've been three or four deadlines we've heard from them over the last bit of time. I think the Cybersecurity [and] Infrastructure Security Agency sent them what's called a 9002 report over a year and a half ago, maybe two years ago, to the White House.

And the White House sat on it for — that was a report required by Congress to say hey, how should we better envision this private sector — private/public collaboration to secure our critical infrastructure? So they've been — I wouldn't say they're sitting on it but they were taking no action on it.

After six or eight months, they sent a letter to Congress saying, hey, you know what, we're going to go ahead and upgrade PPD 21. So now we're almost three years into the administration, they haven't done it. A lot of people probably – you know, a number of people in this audience and myself have said, look, you really need to get hot on this.

And now, I'm afraid that this is – the flip side of government is — the first side of government is why do anything I can't wait to do till tomorrow? Well, we've been experiencing that for 11 years in this. The flip side is let's do the lowest common denominator to get something through the interagency process.

And I think we've rapidly shifted to that. What I mean by that is, if anyone disagrees in the interagency with a significant issue and you can't resolve it pretty rapidly, it gets tabled and taken out of the revision. And I think we're going to see that in the description of — first and foremost, in the description of critical infrastructures.

We've made strong arguments here at FDD that space, along with Auburn's McCrary Institute – we did a paper together – that space systems should be a critical infrastructure. But that's not even the most important one that I think is missing. Cloud computing industry is clearly a critical infrastructure. Whether it's a sub-sector of another sector or it's its own sector, who knows?

I don't blame the Obama administration when they wrote, you know, in this legislate — this PPD 21 in 2013 it didn't exist. But it exists today. Almost all of us would say it's potentially the— either the biggest challenge or the biggest opportunity in securing our critical infrastructure.

The other day, Brad Smith, you know, President of Microsoft, who — and Microsoft has been very careful not to take a position on this in public – said in public, hey, cloud is a critical infrastructure.

We're at that point where pretty much all of us recognize the – A.I. Executive Order recognizes cloud as critical to – the security of the cloud as critical to the proper development of artificial intelligence.

And finally, the administration's own National Cybersecurity Strategy said that cloud computing issues is one of those that had to be looked at for regulation.

So clearly, it's a critical infrastructure, but for some reason, I get the feeling – you know, I'm getting all indications that this administration is not going to tackle that hard issue in this version of the – of PPD 21 rewrite, and that is completely unacceptable.

I mean, if you do not do this, if – you're not addressing the most important challenge and opportunity in securing our national critical infrastructure.

MATISHAK: Sticking with PPD 21 and the rewrite, Kiersten, turning to you, I know you can't really comment on an ongoing process, but from – from where you sit, you know, could you provide some more in terms of what the government is hoping to achieve with this and how CISA and also the private sector are participating or not participating in this?

TODT: Sure. Thanks, Martin, and thanks very much to FDD and to Solarium for the opportunity to talk about this because I think for those of us that have been in this space for so long, critical infrastructure is something that we've seen the evolution from information sharing and analysis centers in the late '90s to, as both Mark and Mary have talked through, both PPD 21 and Executive Order 13636, which came out in February of 2013.

If we take a moment just to sort of work off of what both Mary and Mark have said about where we were in that space and what the language was in both of those, you'll see a lot of language in 2013 that we could apply to it today.

But what's interesting is, if you look at, particularly PPD 21, it talks about critical infrastructure but it talks about the cyber impacts on critical infrastructure.

So there was a time when we were differentiating what was physical and what was cyber. That was where we were in 2013. We talked about the need for resilience, all concepts that I know we're going to talk through further today.

But the evolution of this and where we are right now is really not just what is happening sector by sector, because that is certainly urgent, but this cross-sector engagement. If we see an event today, it is not going to be an event that only happens to one sector. An event is going to cut across a community, it's going to cut across multiple critical infrastructures.

So the urgency for the rewrite in PPD 21 is to ensure that the policies that we have today, as Mark was talking about, truly align with the threats, with the environment, and where we're seeing opportunity for engagement and for resilience. And this has never been, again, more critical than what we're dealing with today.

When we look at CISA, to Mary's point, CISA wasn't even a – a thought in 2013, or if it was, it was deep in the dark caverns of Congress. But where it is today is national coordinator for critical infrastructure and resilience.

What that means is it's not just responsible for the sectors for which it's – the SRMA, and Sector Risk Management Agencies is an evolution from sector-specific agencies, because it's very much talking about what do you do to manage the risk by sector?

CISA is responsible for coordinating across critical infrastructure, so across all of the sectors, being able to raise the baseline of security so that there are consistent resources and capabilities. And I know we'll go deeper into this because we still have this huge disparity across critical infrastructure.

So a rewrite is not just representing where the threat is today, but importantly, what is required by sectors, what is required by the agencies to ensure that the baseline is raised but that the — we have an interrelated and a connected and an integrated approach to cross-sector resilience that we've never had before.

MONTGOMERY: Can I jump in on that for a second?

MATISHAK: Sure.

MONTGOMERY: First, I agree with everything Kiersten said. And I just want to emphasize that when , you know, we say, like, the Biden administration's missing its opportunity, we don't mean the whole administration.

I mean, clearly CISA, Jen Easterly at CISA, Secretary Mayorkas at DHS, described what needed to be done in their 9002 report. And generally, I'd agree with 90 percent of it. I think Anne Neuberger's tackled this issue on a sector-by-sector basis, has really looked at critical infrastructure inside that part of the NSC. And I think the ONCD clearly believes this, if you read the National Cybersecurity Strategy and the associated implementation plan.

The problem we have is there's another part of the NSC that deals with homeland security inside what's called #Resilience. And I think in there, they've been slow to take up this mantel. They don't have the right relationship with the private sector. So I don't think we're getting the right private sector input.

I know we're getting some from what are called Sector Coordinating Councils, something we'll talk about later on, I'm sure, but the — they're not getting that — they're not doing that kind of broad outreach that I think would get the right kind of private sector input into this, in addition to tackling, as I mentioned earlier, cloud, space, and other — and understanding what is the national critical infrastructure today.

It would be quite a shock if the national critical infrastructure, as described today, is 90 or 95 percent similar with 2013. It shouldn't be. We've evolved. We've developed. I mean, how we communicate with each other. How we live our lives. How we bank. How power moves. How – all of these things, they have changed dramatically over a decade.

And it's OK for that document to reflect that. The problem is I think they're trapped by the interagency and by their own ability to get moving. If they just listen to Director Easterly and Secretary Mayorkas' original report, they'd be in much better shape. And I think if they reached out to the private sector, they'd get that final polish on it that would make — that could make a really good product.

So it's not the whole administration, it's a part of it, but it is the part that's in charge, and that's why we have to move aggressively, I think.

TODT: Just one point on this, because I think this is really important, is in 2013, there was the establishment of Section 9 companies. Section 9 were critical infrastructure. And if you asked a company if they wanted to be critical infrastructure — if they wanted to be Section 9, they would say absolutely not.

So in 2016, I ran President Obama's commission. We had the CISA of Uber on the commission at the time. Uber, at that point, was really absorbing transportation infrastructure. If you talked to them about what the vision was, it was to be able to help control traffic flows in major cities across the world, but particularly in the United States. And somebody said, well, don't you want to be a Section 9? Don't you want to be critical infrastructure? And they said no because that is all about penalty, that is not about opportunity.

And so if we fast-forward to today, to 2023, is what Mark said, what you've seen is a real evolution between industry and government, and there is a trust there that is better than it's ever been. It's not — you know, this isn't a – pollyannish, everything is perfect, but we have an understanding that the threat picture and being able to respond and to be resilient is a comprehensive industry/government effort.

And so when you ask the question about are we working with industry, that's obviously the NSC's [National Security Council] role in the rewrite, to reach out to industry, but we appreciate now the — more than ever that this is not about somebody imposing a penalty on a company, it's not government versus industry, but this is a comprehensive effort that's really looking at what does it take to be resilient?

BROOKS: I just want to follow up that with one small point, is there is a trust between the government and industry that didn't exist before, but there is also a tremendous power in industry that I think has only grown over the years – and just in terms of the information that the U.S. domestic industry has, information that the NSA [National Security Agency] can't always see because they can't look internally.

And so we — when you speak to a lot of the officials who are kind of working and structuring kind of these partnerships and they're sharing, they say, look, for – there was a time at which when you wanted information, you looked at the government. Now, when we want information, a lot of the times, we look to industry. And you're really seeing industry take the lead in a number of areas.

And so I think that the relationship is improving, but it's also improving because the government is really realizing we need the carrot, not just the stick, because industry has something that we don't always have.

MATISHAK: Before we turn to another topic, I just want to say with PPD 21 and this —rewrite, you've both — Mark and Mary, you've both sort of touched on this a little bit, but what should the administration be trying to achieve? Like, what — what it — what – should they be trying to expand out the definition for critical infrastructure? Should they be trying to change people's minds on what that is? Should they – be just something else? Should it just be just CISA exists now, these things exist now? They're not great, they could be better, that sort of thing. How — what —what's the goal?

MONTGOMERY: Well, I'll start. We gave a bunch of recommendations – and Mary can jump in, because I won't remember them all – but, I mean, most importantly, they have to properly describe the environment, and this gets at what Kiersten was saying, that, you know, things have changed, and you have to get the environment right, you have to get the sectors right.

You know, the — we — there's — right now, there's 16 critical infrastructures, but there's seven or eight sub-sectors, like rail or air or ports that are just as important as some of the sectors. They've got to get all that language and terminology right. And it's OK to change a few things in there.

They then have to get the rules right. Like, we wrote a law— or the — we wrote a recommendation for a law and Congress enacted it for sector risk management agencies. That's great, but you need policy, you know, Executive Branch direction along with that, the president to say, "Here's how I interpret that."

And little things like designate a coordinator for sector risk management at this level in your agency. In some agencies, it's a — you know, basically an undersecretary; in others, it's an assistant secretary. In some, it's a deputy assistant secretary. In some, it's an office director beneath that. That's completely inconsistent and unhelpful. So they need to get things like that right. So it's standardization of how you do this.

Some rules about the updated policy. I — I'm fairly certain that there's a national infrastructure protection plan ready to go, that's probably been written for two years at CISA that's waiting on this PPD. And there's some rules for sector-specific plans. So those are the plans that an individual sector has.

The existing ones we have are almost all from 2015, and they're almost all a template of one. One really nice one was written, and the rest were plug-and-played in and the word "energy" removed. You know, delete all energy, add all water. And you go through that, and, you know, that's not helpful.

So, you know, they need to get the — you know, a system for keeping that up-to-date. Describe the environment right. Get the coordinators right.

And then I think it's — it's under — describe how the private sector's engaged. You know, we've argued for something called — in something called Continuity of the Economy, that the private sector needs to be more deliberately involved in the decision-making, not just the information sharing, not just the – "what do we do ahead of an incident?", but when an incident's happening, they're part of the discussion and the solution, maybe not under what's called a principals meeting with the president, but at meetings below that. And they have no system. We don't have a good system for that.

You probably don't need it in submarine warfare — you know, in some kind of kinetic war with an adversary, but you definitely need it in a cyber economic warfare or in a —or during a significant cyberattack. So figuring out how you get the private sector properly integrated into that.

There's a lot of opportunity in this PPD 21 rewrite. I think, instead, we're going to really get a lowest common denominator product if we're not careful.

BROOKS: Humor me for a minute to talk about the unsexy topic of report methodology. So, you know, as Mark and Annie Fixler and I started to look into this report and — and kind of to piece together, OK, there's going to be a rewrite of PPD 21, how do we issue these recommendations for what we think it should look like? And kind of as we went through this report, relying on public information, especially from the Government Accountability Office — the GAO has some really excellent reports – CISA's done some really good reports internally through its Section 9002(b) but also through its advisory councils, as well.

And then we started talking to people. We just started calling people in industry. We started talking to people in government and kind of, you know, feeling things out that way.

And as we wrote this report, we kind of settled on a few things. First, there needs to be kind of a strategic, conceptual change. Like I said, we believe that the relationship between the government and private sector has transformed in 10 years. The rewritten PPD 21 should reflect that.

But once you go beyond kind of that strategic level and say, OK, we are understanding that there are — there's going to be more accountability, there's going to be a clearer delineation of responsibility, what do you actually need to accomplish in these SRMAs?

They say, you know, make sure that you are helping the sectors resource themselves. What does that mean? You don't have to be so prescriptive that — you know, for one industry that you kind of lock everybody else into place, but you do, I think, need a little bit more guidance as these SRMAs trying to help their sector out.

So that's the — kind of, like, the conceptual strategic level. We — you know, what are the minimum standards? Is there going to be liability? Like, how do you kind of deal with that shifting interface? But then there's the more low-hanging fruit.

Low-hanging fruit, to me, things that should be resolved in this, is one, what is the role of an SRMA? Again, you have one definition in congressional law, in the National Defense Authorization Act, and you have another one in PPD 21.

Now, when you ask CISA in their report, they say, oh — "they say to do the same thing," basically. Both types of requirements are — they say the same thing. When you look at the GAO, they say, "no, Congress added, you know, some additional responsibilities into this."

So the — the first thing that I would love to see in — in a rewrite of PPD 21 is to really make it clear, these are SRMA responsibilities and this is what they should look like.

Other kind of simpler ones are designations. Mark was saying, you know, you should add cloud, maybe consider adding space as a sector or a sub-sector. Right now, the process for it is basically fiat of the DHS secretary, which has been used one time before to create the elections sub-sector.

And there doesn't really seem to be much of a process, kind of a structural process or a theoretical process for, like, what determines that something is important enough to be included in this critical infrastructure production paradigm.

The CISA report that came out did a good job of kind of explaining at a high level, OK, these are the kind of things that would make a sector or a sub-sector important enough to be considered, but it's still really lacking the – and then you do what logistically to kind of make that happen?

So those would be kind of the first things that I'd like to see, in addition to the — the strategic layer. And then honestly, I would love to hear Kiersten on how CISA can kind of play a stronger role in this, because everyone that we talked to said that there was this hunger, really, for CISA to lead more without owning more, to really kind of give that guidance and kind of give some more direction without saying, you know, my way or the highway. So I would love to hear kind of more from you on that.

TODT: And I'm — might preempt the next layer of conversations. But in fact, this had shifted. It's no longer just for the Secretary. So in the last year, there's been a re-energizing of the Federal Senior Leadership Council, the FSLC, which is a representative body across interagencies which in fact is chartered with identifying what should be critical infrastructure, what requirements make it critical infrastructure, and what agencies should then manage that.

That is something that CISA initiated and launched last fall. Again, it's an entity that's been around but it was reenergized. That's been very effective. In the last year, CISA has established an SRMA liaison for every sector and sub-sector agency, even for those for which it's not the SRMA.

And because it's a fun fact, the eight sectors for — that CISA's the SRMA for are nuclear, chemical, communications, critical manufacturing, commercial facilities, elections, IT, dams, and emergency services. That's a lot of disparate entities but it is the SRMA for that.

But the key element here is that CISA is the national coordinator across all of them. That's why the FSLC [Federal Senior Leadership Council] is so important, because it's a consensus body to look at these issues. And I think how the FSLC feeds into PPD 21 is going to be really interesting, and seeing — is to look at what requires — what mandates an entity to be critical infrastructure.

I mean, the cloud question is — I think everyone's been forward leaning. You've said that about Brad Smith and cloud being a critical infrastructure. It had an eerie relationship to Mark Zuckerberg, saying social media should be regulated, but we won't go into that because I think it's — we put it out there but then what actually happens to it, what does government do with these big grenades that say "hey, we need to do more with it" — I think that this is a really important time.

When we think about also the NDAA from 2021, it gave specific roles and responsibilities for SRMAs. So we have to remember that when we're having this conversation cause there has not been this gap over the last 10 years, there has been progress. And Mark led a lot of this effort with Solarium.

So in those roles and responsibilities, it talks about assessing risk, it talks about information sharing, contributing to emergency response, building incident response plans. So these are the actions that the SRMAs have to take and are important for what comes next.

If we evolve this other element about what's critical, there's something else going on at CISA, the identification of systemically important entities. And I raise that because there are three critical factors that go into what is a critical entity, a systemically important entity.

That — the first is really looking at the size. So what's the volume of the service and function? And it — in other words, is it statistically significant? The second is looking at the lack of alternatives. Are there viable alternatives to this entity? And if not, then obviously it has to be systemically important. And the third is looking at the systemic relevance of the entities. So how do other entities rely on it?

And I think that's particularly important because we are talking sector-specific, which — you know, to the point that Mark made about the National Incident [sic, Infrastructure] Protection Plan, looking at the sector work, we have to understand how every entity is playing a role in the systemic relevance of the whole system. When we look at critical infrastructure, you know, the disparity between energy and water. EPA can go into a community but it doesn't have the ability to actually look at the role of sanitation, when it comes to water.

So we've got all of these interdependencies that are building out in critical infrastructure, and that, as we see what is systemically important, has never been more important than it is now.

MONTGOMERY: If I could jump in, I agree, Kiersten, your...

TODT: And I know I said your buzzword, "water."

MONTGOMERY: Yeah, your three things...

(LAUGHTER)

... your three things on what should be a critical infrastructure, I mean, cloud was, you know, 777. So how the White House can continue not to think cloud is a critical infrastructure is beyond me.

Also, I do have to say, on the FSLC, the Federal Senior Leadership Council, I kind of — the idea that it is consensus, it makes me think of, like, you know, the Imperial Senate, you know, in "Star Wars," you know? Emperor Palpatine doesn't really need them, right? I mean, they have no value, no decision making, no resources.

All they can do is slow things down, and I think they have. I think they killed the space as a — space systems as a critical infrastructure cause no one at the meeting wanted — you know, would raise their hand and say "I'll take accountability for that." But more importantly, no one else would say "my piece of the Empire, you know, my little silo could be impacted by you being picked."

So I think these consensus-based —the federal government does not work on a consensus-based system, it works on the president making a decision. And the president — the National Security Council should bring him a decision about cloud that he makes, about space that he makes.

I think Ali Mayorkas has already told him what he thinks, and I think that's actually the person he should be listening to, not the FSLC. The FSLC's a great place for putting out information. They can go back and send their notes out to everybody about what the federal CISO thinks is going on. It is not a decision-making body. It has very few, if any, elected officials in it. It's not — it's absolutely not the way we should do anything. And the fact that the NSC's relying on that to do nothing is extremely irritating.

TODT: Well, we have the challenge, right? So I don't disagree that when we look at this — so the challenge with PPD 21, to your earlier point, it's going to be a consensus-based document. So the challenge there is then agencies and entities are going to protect the authorities that they have. So how do we disrupt the system?

I don't — I'm not totally aligned with you on the FSLC because I think that reinvigorating that as a body to bring together input and to be able to say what's important here, how are we looking at this across the agencies, is very important. What you're saying then is how do you take that and bring that up to leadership, have somebody make an asserted decision, not have the ultimate decisions be based across the agencies.

I think there's a happy medium because you're not looking for a dictator to all of a sudden just say these are all of the things, unless you're talking about an informed decision process that brings it to a senior decision maker — and whether that's the Secretary to the President and looking at all of that — but all of these are information opportunities because I think where we have failed in the past is when we haven't had appropriate representation across sectors, where we haven't had appropriate representation to understand where are the challenges, where are the vulnerabilities?

How those decisions ultimately get made is another layer to this. And I think there's a bigger discussion around FSLC because I do think that there's a lot of value there, particularly for CISA as the national coordinator.

The government hasn't truly embraced CISA's role as national coordinator for critical infrastructure and resilience. It has to be that body. It's not a risk manager, it's a coordinator. So if you're a coordinator, you need to bring — you know, it's —if you're a coach, you've got to have all of your players in front of you. You can't just do this by these one-offs.

So the FSLC is playing that role. How these other decisions are being made and looking at what is critical infrastructure, perhaps there are more — there — there's more steps in the process, but as coordinator, I think CISA absolutely needs that body to understand what all of the sectors are doing. Also so that it can share lessons learned to raise the baseline for sectors so we don't have this continued discrepancy and variability between energy and everybody that, you know, did a find and replace in energy and looking at what that looks like.

MONTGOMERY: The one thing I'd say on FLSC though is that, first of all, there's a reason it went away, that it needed to be reinvigorated, which is that it was unable to handle complex, large decisions. And so we're now reinvigorating it to give it a complex, large decision.

But the other thing is if an FSLC Rep. actually was able to talk to his or her Cabinet member before he went and after he came back, which I don't think happens, he would get two — he or she would get two pieces of guidance — don't sign me up for anything that I don't get the resources for and don't let anybody take my stuff, not "Hey, what's the best interest of the American national security coming out of this meeting," right?

So my problem is we know this, we know what I'm saying is true. This — a consensus-based organization of dozens, if not scores, of federal officials looking to protect their turf is not a way to solve a complex problem, and giving this to the FSLC was tantamount to kicking it to the lowest common denominator.

Literally, I think these guys — the fact that they can't get to the — and I — answer on cloud says everything you need to know. You — cloud met every one of your tick points. Cloud meets every — whether or not — I agree, Microsoft, Google, and Amazon have not leapt into cloud as a critical infrastructure cause they fear regulation, but they're starting to see enough of the rest of government's reliance, the rest of public-private sector's reliance on the cloud, to understand that they either need to have some kind of organized standard setting or they're going to get regulation.

Anyway, I just — I...

TODT: I agree. I mean, I think that the FSLC — when you're talking about defining critical infrastructure, where I think in some ways we're talking past each other — because I do think you need the FSLC for CISA as a national coordinator. Should the FSLC be the sole body determining what is critical infrastructure? I think that is for further discussion.

MONTGOMERY: I'll agree to agree on that, yeah.

(LAUGHTER)

MATISHAK: Well, in that back and forth answer to all my other questions — so we're done now.

(LAUGHTER)

Actually, Kiersten, I'm going to come back to you in a minute, but, you know, I sort of also want to take a step back. We're talking about SMRAs [sic, SRMAs] and new boards and SRMA liaison, but Mark, there have been inconsistencies in the first place. So can we talk about the SRMAs and their inconsistencies? And have there been real world examples that you can point to on this? And then for them to be successful, what do they need — and you've talked about this before — but what do they need, what are the pillars that they need?

MONTGOMERY: So I think that's fair to say. I don't think anyone would disagree with your statement, that the performance of federal agencies as sector risk management agencies is inconsistent.

I think there's a couple on a curve — and I teach at a — Georgetown as an adjunct, so I — I've learned a curve — you know, put a pretty hefty bell curve in — you know, there's some A's out there. I think the defense industrial base, I think energy, telecommunications, financial services are probably at the top end of it, some of them because they've spent a lot of money.

You can't ignore the fact that the big eight banks spend close to $1 billion each year on cybersecurity. They do that because they've been under attack. Other ones because they're heavily regulated, like portions of energy, particularly the nuclear part of it, and financial services again.

The — and some because they have a relationship with NSA, and that would be the defense industrial base, and to some degree, telecommunications. So there's reasons why they're there.

The — then there's the great unwashed, right, the have-nots, and the have-nots are pretty extensive. We've written a report on water, you know, the most critical infrastructure, which we pretty much call a dumpster fire. And it's not just EPA's [Environmental Protection Agency] fault, it's also the water utilities are — don't have access to resources, cause we as voters don't vote rate increases and we don't vote bonds, and they can't raise capital cause they're generally, you know, 90 percent publicly owned, you know, state and local utilities.

So — and they didn't understand, when we automated water 25 years ago and went to automated, you know, pumps and valves and chemical injection systems from linemen operating all of those things, there was no threat — cyber threat. So we took all of the savings of automation without making the investment in cybersecurity.

So for all of those reasons, water's like that. To some degree, pipelines was like that. We see that in the port system — has gone to a heavily automated environment without thinking about military mobility as a cyber risk.

So you can go through each one. And definitely there's haves and have-nots. The ones that I find disturbing are when you have something like water and energy — and Kiersten brought it up, it's a great example — look at the resources.

The — both the administration and Congress collectively, together, as a team give energy about $200 million for natural disaster and cybersecurity, right, together. The same kind of office inside, called Water Security, inside EPA gets, you know, around $15 million.

Well, one of those numbers is right and one of them's wrong, and I'll tell you it's not the $15 million number. You know, that water one needs to come up. It's working with even more utilities than energy. Still protecting 370 million Americans' access to that — you know, to that utility, to water or energy. And we're just not making those same investments.

So a lot of it — some of it's resources, some of it's history, but there's this massive disjuncture, and both the administration and Congress need to tackle this together. PPD 21 won't solve that. It will have zero dollars attached to it, like any good PPD. Well, it'd be an NSPD [National Security Presidential Directive], whatever it's called at that point.

But the administration needs to work — and here's one last thing I'd say on this — the Office of National Cyber Director, this is where they need to step in. They have some budget — they got both from law and from a good relationship with Shalanda Young, the Director of OMB [Office of Management and Budget].

They have a strong budget role and they have a Deputy National Cyber Director named Drenan Dudley who's reviewing federal agency budgets. And she — I think she's reviewing for both are you adhering to what the federal CISO [Chief Information Security Officer] says you should and CISA says you need to be spending on cybersecurity to defend yourself? That's your down and in. And are you doing your SRMA job? Up and out.

And, you know, then we can get some good pass back to agencies and say "you talk a good game, that you're committed to cybersecurity or you're committed to being a good SRMA, but you fund a poor game. And, you know, let's have the rhetoric — you know, the actions match the rhetoric — or the budget match the rhetoric."

That — long way of saying that we're very disjointed.

MATISHAK: I kind of want to go back to your water dumpster fire...

(LAUGHTER)

... which is an interesting image when you think about it. So the EPA tried — they tried to instigate — institute new metrics, and it was challenged in court, and then the EPA just sort of folded, they're like "we're not going to do this." Anne Neuberger says — from the White House says "we're going to turn to Congress and they're going to probably do something on this."

Mary, I'll turn to you and then we go to Mark, and I don't think you want a piece of this, Kiersten, but are — should we be holding our breath for this, that Congress is going to step up...

BROOKS: I can't take water from Mark — I can't take water from Mark.

MONTGOMERY: Yeah, I'll jump on that. So...

(LAUGHTER)

... I think they're going to — you know, this is, like — what did Winston Churchill say — you know, I mean — about democracy? We'll try all of the wrong things before we do the right one. You know, the — they — I think they went on the wrong path with that — with trying to pass — look, there was a — they inherited — this administration did not cause the problem at EPA. It's 23 years in the making. I mean, they were initially made the sector-specific agency back in 1999 and they have done poorly for 24 consecutive years. This is not the Biden administration's fault. They inherited this.

But they — there was not a good solution at EPA for how do you rapidly change the performance of 55,000 water utilities and protecting that critical infrastructure. What they tried to do was pass the problem to 54 states and territories who are equally ill-equipped to do it. And they — there were some legal challenges with that related to how they did the rule-making, related to separation of federal and state powers.

I'm not a lawyer. I'll just say it became pretty clear they were going to lose, so they pulled the rulemaking, which I think was really smart. And I think Anne's next response was exactly right. This needs legislation. And our paper on this — FDD's paper on this, we've very clearly laid out, we need legislation that recognizes EPA can help provide standards but they probably can't enforce them, you know, with the five man shop, you know, and 55,000 utilities. I'll just say that's — mathematics, it doesn't work.

And so I like the idea. We've written legislation — or we've provided sample legislation. I've seen it's been picked up in the House and being pushed around, and hopefully the Senate will as well.

But basically, the right way to solve this, when you don't have a federal regulator and a position to do it, for the exact reasons that Kiersten mentioned earlier and the resources – I — reasons I mentioned, what you do is you create a public-private partnership, a — we call it a Risk Resilience Organization, where EPA would set standards, A, they'd hire a –you know, a non-profit probably from, you know, kluge from the water associations who would go out and do assessments of the water utilities, provide them with feedback. They would then have some period of time to correct those.

But in addition, it would steer them towards the grant programs that – it can help them, particularly on the smaller and medium-sized ones, either at the — at EPA through state — what are called state revolving funds, and CISA, who has some programs for this, or Department of Agriculture who helps water — rural utilities, through any of those three agencies to get access to funds to correct the problems.

Or, in some cases, the assessment team can correct the problem if it's just an administrative thing on the spot. That's how you slowly but surely fix 55,000 water utilities. You're not going to do it with state and local government.

But that legislation, I think, is critical, and it – it kicks — and it does have a little bit of appropriations, I think about $10 million in it to get the program greased and running, till dues can kick in and make the problem work, dues on the medium and larger-sized companies.

But then it – over time, if EPA evolves into somebody who can regulate this, then this kind of — and this is – I would call it a NERC-like [North American Electric Reliability Corporation] body, could evolve into something else. But right now, let's just get that done and help these 55,000 water utilities out.

MATISHAK: So, stay tuned is what you're trying to say?

MONTGOMERY: Yeah. I will say one other thing. We've been tackling this with the Cyber Resilience Institute, which is – Kiersten invented or developed — you know, birthed. And – and ...

(LAUGHTER)

BROOKS: Founded — founded.

MONTGOMERY: — I guess invented is better. We'll leave it at that.

And then – and now run by Karen Evans, and then — and with Microsoft Foundation, to go work with several hundred water utility – just to go find small, rural water utilities, grab them and start doing cyber hygiene work with them.

We can bottom up this. That Risk Resilience Organization can bottom up it, work like the — like CRI [Cyber Risk Institute], Microsoft and FDD are doing, can bottom up it. But we are not going to top — there's not going to be a great top-down law. I think that was very aspirational of EPA and NSC. And I think we're now on the — we'll probably get it to the right track here.

TODT: Can I just had one quick thing, because you just made an – a really important point on sectors and protection that we are sort of talking past, which is really the role of state and local governments and regions and communities.

We talk a lot in DC and inside the Beltway, we're talking about federal policies, absolutely critical, it drives it down, but Mark's point I think is so important, which is the work that the federal government can do at the state and local level to ensure that there is that almost chaperoned approach and experience to just raise the baseline to get into the communities.

CISA has evolved with its regional offices, which are aligned with the FEMA [Federal Emergency Management Agency] offices. They have cybersecurity advisors, physical security advisors – is building out. I think what's representative there is the work at the federal level to say, hey, we've got to get into the communities to make sure that we've got the relationships so when something happens, there's a call to somebody right next to you. And that's where we — CISA has done most of its responses.

But I think, particularly when you're looking at water, if we just talk about the resource-poor sectors being able to be at the community level, to share the resources, the cyber hygiene, the basic practices, this isn't rocket science as far as what just needs to be invested at the beginning to be able to raise the bar for the sectors.

It – we can't miss that point when we're talking big policies, federal agencies, that we've got to get into these communities and make sure they've got the knowledge and the information and the training to do the basics to raise the baseline for sector security and resilience.

MONTGOMERY: Let me —one last thing that I didn't think about legislation, because that was a great point. There's one other piece of legislation that came out of our report that Representative Davis from North Carolina has championed. I think it's likely to get in the farm bill — the eventual farm bill, not any interim one. And that's a — that's to create cybersecurity riders.

Right now, we have a program at the Department of Agriculture and CISA run with the National Rural Water Association to have circuit riders. You know, these are like 150 men and women – or more than that, 250 men and women who ride – who go work in rural areas, helping people figure out, you know, is your waste pipe too close to your water pipe? Let's separate it. And they — I think they drive around in, like, F-150s with PVC piping.

Our idea is to fund another 50 to 100 cybersecurity circuit riders. So these are people who drive around in a – like, in a Prius, and they show up at the royal entry and they say, hey, you're running Microsoft Windows 7, that's not going to work for you, you know, or hey, they're – here's how you do a patch update, things like that.

That piece of legislation, I think, would be very useful. And I think getting the farm bill – and again, it's attacking 8,000 or 10,000 small, rural water utilities. But that — you know, that's 20 percent in the — of the target set.

So we can do this with some legislation. That's a very small bit of appropriations, and I think it adds about $7 million into a $15 million existing program for circuit riders.

So to me, there's a lot that can be done if we — if the administration can work with Congress over the next year.

MATISHAK: It's funny we're talking about, you know, things sort of on the ascent right now with this water legislation, potentially the farm bill, but there is a sort of glaring failure in the past couple years involving ransomware and Colonial Pipeline.

And TSA was sort of out of the loop, according to many and according to, like, a lot of reports, but now they've been given credit as sort of maturing and sort of getting it more and devoting more time and resources to this.

So Mary, turning to you, because I knew you wouldn't take water from Mark. So let me give you TSA [Transportation Security Administration] instead. Much easier. Is this a good news story, that TSA is – has learned its lesson, and it's something that policymakers, decision makers can point to and be like we don't want another Colonial Pipeline where an SRMA is completely out to lunch?

BROOKS: I mean, the easy answer of any improvement is a success story.

The other point that I would just make, because this is hard stuff – I mean, you've got Mark and Kiersten up here throwing around the, you know, FSLC, you know, Federal Senior Leadership Committee, and you've got them exactly, you know, weaving into the details of what authorities EPA has and how those differ from, you know, what agriculture has.

I mean, the scope of — the scope and breadth of how much you need to know in order to actually effectively respond to some of these challenges is really, really, really hard. And I just really want to give credit to the people in the federal government right now who are working so hard on this and who have individually, sometimes even just boot-strapped their SRMAs to improve. And I – I know some of the folks over at – at TSA, and they are really, really hardworking and they are really making progress.

And the point I would make about Colonial Pipeline – so just a quick run-over of the facts. This was May 7th, 2021. A pipeline operator came into Colonial Pipeline, which, as you, I'm sure, all know, runs about 55 percent of the jet fuel up and down the Eastern Seaboard, among, you know, other gas and other items. And said, OK, around 5:00 am, there seems to be some kind of ransomware incident. Within about two hours, the pipeline was shut down.

Why was it shut down? There was different answers. Some people said it was because, OK, with the IT software down from this ransomware attack, we wouldn't — you know, they wouldn't be able to bill their customers, so why – why give away free gas? Others said it was more of an issue of would it jump over from the IT to the OT because, as was said later I believe by TSA or GAO [Government Accountability Office], there were some very basic security mechanisms that were just not installed to make sure that something in the IT [information technology] side couldn't jump over into the OT [operational technology] side.

But as this crisis was unfolding — and I don't believe there have been any kind of play-by-plays where we can actually know who knew what when – but if you go look at the — the congressional testimony and kind of as, you know, Congress was attempting to figure out what had happened, it's pretty chaotic.

You've got FBI – you know, you – I guess Colonial Pipeline called the FBI. The FBI eventually contacted CISA. You've got the Executive Director of CISA going up there in front of Congress and saying, "well, FBI waited to call us. If they hadn't called us, we don't think Colonial Pipeline would ever have called us."

You had Colonial Pipeline refusing to talk to TSA. You had them previously refusing a number of opportunities to kind of test the systems, partly because of COVID but seemingly partly part of a broader system where they didn't want to work with TSA.

You know, Colonial Pipeline seemed to have a better relationship with the Department of Energy, which wasn't technically their SRMA in this case, although a pipeline carrying jet fuel and gas obviously has strong connections to the energy sector.

So what would we have liked to have seen? Well, we would have probably liked to have seen a quicker response, the government sharing information more smoothly, Colonial Pipeline much more willing to work with its SRMA – designated SRMA and other members of the government. We would have liked to have seen minimum standards in advance, so that kind of these basic resilience measures were input.

And we didn't see those things. We did not see kind of this smooth deployment of this crisis framework. Now — and a crisis framework also in PPD 41 as well, which is actually, I believe, currently being rewritten. So we could see where that goes.

So as, you know, we looked at kind of the fallout of Colonial Pipeline, you saw TSA come out with these pipeline directives within a matter of days. So clear — clearly, they were, you know, coming down the pike beforehand.

And at first, these regulations were not so well thought of by industry. There was a lot of concern that they were overly-prescriptive, they were not feasible, kind of the diversity of different technologies and legacy systems that these pipeline operators were dealing with.

But then you really saw TSA calmly working with industry, industry really engaging with the process. And what came out later, you know, was a revised directive that not everybody was happy with, but that was kind of a step up.

And then you saw this very detailed, you know, kind of sector-by-sector approach, as — as Mark was saying, kind of evolve, where it'd been, you know, Anne Neuberger in the NSC then tackled what — healthcare systems and water and – I forget which all – you know, all the entities that there were. But the point is clearly some of this was starting beforehand because of recognition that the system as it was, was not working.

So partially...

TODT: … can I actually …

BROOKS: Yeah, go ahead.

TODT: So I think it's a really important question because it actually bookends your first question.

When you're flying out with your family and they're asking about critical infrastructure, you talk to them about Colonial Pipeline because that was the first time — I live in the Commonwealth of Virginia. You saw a line at the gas stations, not because there was a shortage of gas but because there was the concern that there was going to be a shortage of gas. You saw JBS Food Systems happen right after that.

So the first time, we saw cybersecurity hit the kitchen table – the proverbial kitchen table. This was very much about where the concerns are.

But you mentioned a few things. So first of all, admirable — Admiral Pekoske – Administrator Pekoske at TSA has done an extraordinary job, from a — an appreciation of what happened and then how do you move all of these other issues?

But the other piece, when we look at critical infrastructure, going back to the catalyst for this conversation, is Colonial Pipeline didn't happen because a very sophisticated ransomware actor said “how are we going to shut down 45 percent of fuel on the East Coast?" It happened because of opportunism. It happened because they were able to get into a system. They did a scattershot, and they just happened to get this major critical infrastructure.

So when we're talking about critical infrastructure and resilience and we're talking about what we have to invest in, the key for the United States government and for industry, we do really well when something happens and how we respond. We respond with resources, we respond with efficiency, effectiveness. We bring the best and the brightest.

If you look at Obamacare, it took us two years to get that. It failed. In 60 days, we put together a system that far outreached anything that had been done the previous two years.

Where we have to focus as a nation is what happens before the event happens. So last week, Jen Easterly, the director of CISA, with Deanne Criswell, the director of FEMA, launched something called Shields Ready, which is an evolution of Shields Up, and it's aligned with FEMA's Ready Campaign, and it's very much about long-term investment in resilience and preparedness.

We talk a lot about response recovery, but we have to invest from a sector-specific approach, as well as from a government and industry in what we're doing to prevent what needs to be prevented. We talk about resilience to minimize disruption when something happens, but when we look at the threat actors coming from China, coming from Ukraine, and from Russia, we've got to be able to manage what's happening before the event. And I know there's more – I'm looking at the time, and I know you want to say something – but that, to me, is the priority for looking at critical infrastructure protection and resilience.

MONTGOMERY: So a couple of quick thoughts. One, I agree, Dave Pekoske being at TSA has been very helpful in recovering from that.

I do think — and I think TSA's in a better position and the pipeline industries are. I still think one of the overriding issues, which is the delineation of responsibilities between FBI, CISA, and Department of Energy, is not resolved.

And I don't think Department of Energy and CISA can agree the sun came up in the morning without the window getting open – you know — getting opened, you know, and that's just a problem we have in our government right now. And we need to continue to work through that.

I do think we'll look back on Colonial and JBS – you're right – these ransomware — major ransomwares as actually — with some silver linings. I think that ransomware has shown the complete monetization of data, and what that means is it's not banks that are responsible.

So I think over the last three to four to five years, we've come to understand that we have to protect all 10,000, 15,000 major utilities or companies involved in our national critical infrastructure, and that they need to raise their percentage of IT spending that goes to cybersecurity from the four to eight percent that it's historically been to the kind of 10 to 14 percent where the financial services sector sits.

That movement in cybersecurity spending is what's going to drive security, get — you know, from the private sector side. And then our job, circling all of the way back to PPD 21, is to make sure that the federal government has a good process for the public-private collaboration to support that increased investment in cybersecurity that I think is — you know, is upon us now. And then we'll have a more secure, resilient national critical infrastructure.

MATISHAK: Well, on that note, it's time for audience Q&A, it's time for you all to get involved here. I know you just all had lunch so you might be a little sleepy, but I need you to raise your hands and ask a question if you have one. And I guess I just — oh, there's a microphone. Oh, I didn't even know that. All right, good.

SAKELLARIADIS: Hi. I'm John Sakellariadis with *Politico*, and I had a question about systemically-important entities or critical infrastructure — there's been a couple terms to go around. Sort of a Wikipedia question, but I'm always confused.

To what extent is CISA's effort to identify those SIEs [Systemically Important Entities] completely kind of overlapping with CIRCIA [Cyber Incident Reporting for Critical Infrastructure Act], as in CIRCIA stipulates that CISA identify, you know, critical infrastructure entities, but it seemed like there's a parallel effort that doesn't overlap completely within the agency to identify those SIEs.

So I'm just kind of trying to understand whether those two efforts are kind of happening in parallel, or what?

TODT: So for everyone's awareness, CIRCIA is the critical infrastructure – Cyber Incident Reporting for Critical Infrastructure Act that's in the middle of its rulemaking. So I can't talk specifically to what's happening there.

Certainly, CISA is running the CIRCIA process in the middle of what is going on with how to identify what's critical with industry. There's been requests for comment — obviously all of the input, in addition to SIE.

So I can talk to you offline, but because we're in the middle of that rulemaking process, as well as what's happening with the SIEs from a public perspective, your favorite answer, that's all I can share right now.

MONTGOMERY: So I'll jump on that and say I think they're two slightly different numbers. The systemically important entities are what we called SICI [Systemically Important Critical Infrastructure] in the bill, but I like SIEs just fine. That was our worst acronym, SICI, in the Solarium Report.

But the SIEs are absolutely necessary. There's some number — you know, we thought about 200 — I'm guess — I'd say CISA probably thinks about 485 now, you know, entities that have to have — the government has to have an understanding of what their cybersecurity is.

They're so important to the national critical infrastructure, to our military mobility, our economic productivity, that we have to understand they're maintaining a certain level of security. We have to understand if they have needs or, you know, there's responsibilities that aren't being met, or is there a risk occurring that we need to know about? That's one group.

The CIRCIA reporting entities are ones where we need to get reports from. That's going to be a much larger group — you know, if I were to guess, 14 or 15,000, but it could be even bigger than that — you know, that need to tell us that something happened. Because there's a difference between us knowing there's something happening and there's an understanding of how secure — how stable or resilient you are in dealing with that, which is what the SIE is.

I think the SIE's the natural extension of our — of Section 9 of Executive Order 13636 that Kiersten mentioned, is itself nine years old and most companies tried to Heisman away from it. I think we're at the point now where we need that updated list of systemically important entities, and CIRCIA will have a separate list, I think.

MATISHAK: Next question?

LIVESAY: Jacob Livesay from *Inside Cybersecurity*. I'm curious about cloud and space as critical infrastructure. If Rear Admiral Montgomery's assessment that those might be omitted from the PPD 21 rewrite is correct, then I'm curious what the path to effective risk management then looks like for those sectors?

MONTGOMERY: Well, I hope I'm — by having this event and press covering it, that the NSC gets a you know, gets a little bit of encouragement and goes back to FSLC and says "think about this again," or it says "you're the Imperial Senate, I don't give a crap what you think, you know, you're gone."

But either way, the way you fix this without it is the wrong way, which is law. And Ted Lieu's written a piece of legislation, Representative Lieu, for — that very specifically says space will be a critical infrastructure. It then says — knowing it's not the right answer but knowing this will get action — says CISA's the sector risk management agency, cause eight wasn't enough, why not nine?

And — but it then says look, the administration can appoint somebody else to be the SRMA, we're cool with that. That is not the way we should pick SRMAs. The SRMA law says very clearly the way to identify sector risk management agencies is the administration — set critical infrastructure and SRMAs is that the administration should do that in a process. That process was historically, you know, a PPD — a national security decision memorandum, like a PPD 21.

So I'm — the alternative is legislation, but that's what Congress does when the Executive Branch fails to do the right thing after several go arounds, and unfortunately, I think that's going to happen if the rewrite of PPD 21 doesn't capture both of those issues.

And there could be more. You know, I — those are two that we've written on here at FDD — here — and at Auburn and a few other places. There could be an argument for others, but those are the two that strike us as most important.

MATISHAK: If I could just use the moderator's prerogative real quickly — so we talked earlier about water and how there's probably going to be legislation, we talked about the farm bill and how there's probably going to be legislation. Now you're talking about space or cloud and there's going to be legislation. That's a lot of pieces, and it sounds like we're just going to end up in a sort of bureaucratic hell of competing laws and competing requirements...

TODT: Maybe there's a bigger role for the FSLC in all of this. And you just can't quite see it…

(LAUGHTER)

MONTGOMERY: ... that's one option. The other is maybe we're a — maybe we're a country of laws. And I have no problem with Congress passing laws.

On the water, I think almost all of us agree that — well, I don't want to say all of us agree — but I think the administration — the NSC's coming to that conclusion. I can't speak — I haven't spoken to EPA. I suspect NCD [Office of the National Cyber Director] understands that that needs to happen, you know, who's probably the right Executive Branch agency to kind of quarterback, you know, or — you know, lead that kind of organizational push on critical infrastructures sectors, working with CISA and the SRMAs to do that.

I think one thing we haven't said, one other law that's been around but has not made it up is CISA is the national risk management agency. I do think we need to codify their role — that — as the coordinator of risk management, the person who tries to identify, you know, the single point failures, you know, do risk mitigation left of boom, left of an event, to try to reduce the impact of that event, and then also serves as the coordinator of recovery at a later date, you know, alongside FEMA, who's going to lead recovery in a —you know, in critical emergency services.

And, you know, that NRMA [National Risk Management Agency] designation is loosely in law in a few places, but it was tightly in our SRMA law and was removed. It was removed by other federal agencies not wanting CISA to have power, which is not the right — again, that leads me back to my FSLC comments, that most federal agencies' number one interest is in preserving my piece of the pie and making sure your piece — your pie doesn't somehow, you know, become part of my pie.

TODT: I'm more optimistic on the role of the agencies, but I want to say one quick thing. Mary launched with talking about most of critical infrastructure is owned and operated by the private sector. And when we look at this, we often talk — and the point about regulation. Industry and government, when they come together, they start with market incentives. What are the market incentives to do the right thing? If those market incentives and market forces don't work, then there's regulation.

And I think we just have to be very careful in how we're sequencing this because as was said in the national strategy, it was how are we putting more of the responsibility on owners and operators of critical infrastructure to do a baseline level?

The concern here always is that we are having a compliance conversation versus a risk management conversation, as Mark was talking about, and I think, you know, we cannot — we talk about sectors as if they're all owned by the government sometimes, and we have to appreciate that we've got to be working with market forces, market incentives. And this is where we can start using security and safety as a market differentiator.

We thought that was going to happen about five or six years ago, and it really hasn't happened, which is kind of fascinating, but if we can get to the place where we are looking at security and safety for industry, who have shareholders and are beholden to other people and other entities other than just the federal government, where prioritizing security and safety, building that in, and using that as a differentiator, then we can start to actually work more effectively, I think, from an industry-government partnership perspective.

And this is where the conversation this year particularly has been with the National Cybersecurity Strategy, with CISA's prioritization of secure by design, secure by default, really looking at what is the need to prioritize this for industry so that security and safety aren't regulated — aren't — don't have to be regulated but we're letting market — the market and financial resources take over in a way that will start to define the market for the future.

MATISHAK: Thanks for entertaining my question. Next question from the audience? I see a hand here in the front. I don't know where the microphone is — there.

VISNER: Thanks. Sam Visner with the Space ISAC [Information Sharing and Analysis Center] You — at the — almost at the beginning, I think you asked a question, what is it we'd want to accomplish with a rewrite of PPD 21, and Kiersten, you spoke eloquently about the Shields Up campaign, which I think is a very good thing, and now the Shields Ready follow-on, again, a good thing.

But I — it seems to me that we need to revisit a couple of changes in the environment. Mark Montgomery, you made a very, very impassioned comment that we rely on critical infrastructure in ways in 2023 that we didn't in 2013.

But I think the other issue is that there's been a significant change in the geopolitical environment, and we need to recognize that change as part of the rewrite. As we ask ourselves what we're going to accomplish in the rewrite of the — of PPD 21, we should be asking what its effect should be.

And I think its effect should be an understanding of the role that critical infrastructure plays in the defense of our country, in the context of a very changed geopolitical environment, and I haven't heard that and I don't think the — with due regard to the discussion about the FSLC, and there is clearly a — as we say, a range of views, as they say in diplomacy, on that topic.

I'm not sure if they're exactly the right people to be addressing the outcome of this discussion and the context of the overall geopolitical environment in which we're trying to protect our infrastructures. And I'll let it go at that. Thank you.

TODT: Can I make just one comment on that, because I think it's a really important point when we're looking at today.

And I think one of the biggest tangible examples of this, as we saw in February of this year, the annual threat assessment from the IC [Intelligence Community] community, say very specifically that if China thought that the United States were going to respond kinetically or respond impactfully because of Taiwan, that China would absolutely use its cyber resources and tools against the United States, specifically on infrastructure and military assets globally.

So for the first time, we saw the IC community lean pretty far in on the fact that — and Mark, you made this point about — earlier about what our critical — how our open critical infrastructure is potentially compromised and where does that resilience bake in?

And I think we always want to be careful that what we're building, to the point about a 10 year policy, is agile for the future threats and is not solely restricted by today, but I think it would be not, you know, at all informed to think that the environment — the threat environment today is not indicative of where it's going.

And so the protection of infrastructure and the resilience has never been more important, given the global environment. I think it's a — an important point.

MATISHAK: One last question from the audience? We have — oh.

GARZONI: Hi. I'm the deputy CISO for a healthcare organization, and I did have one comment, I guess, and then one question.

First — so as far as SRMAs, most private sector partners don't want to talk to their SRMA cause it's their job to fine you, right? So there is some obviously consternation there.

But the question I have around that would be the SEC's [Securities and Exchange Commission] — so the SEC reporting requirements, how does that — how is that affecting conversations for rewriting PPD 41 [sic, 21]? And I ask because there is a — there was — well, thoughts from the White House on cybersecurity-regulatory harmony. And then it seems like SEC just threw a grenade in that process.

So is the SEC requirement sort of helping the conversation or harming the conversation?

MONTGOMERY: So I'll jump on that. And first, I like the SEC regulations. They were, as you may recall, a carry-on of our Sarbanes-Oxley recommendations, Charlie . The — so what I would say is it's two things.

One, I get it — one week after CIRCIA passes, coming out with proposed rulemaking that has a slightly different incident reporting requirement, was slightly tone deaf. And then not fixing it along the way is just, you know, rank stubbornness. They probably should have — we should have — we had a chance for some harmonization there.

I think long-term, we need to give that to ONCD, Office of National Cyber Director, to work with CISA and get the harmonization of the 20-plus incident reporting requirements across the federal government in law done.

The second part of that law though was important, a rulemaking was important, and that says C-suites and boards are responsible and accountable for the cybersecurity performance of their company, similar to, you know, Sarbanes-Oxley made them responsible for the financial accounting and the ethical performance of the company after Enron.

And so I — it's a mixed bag. I love what Chairman Gensler did with the responsibility and accountability and putting it there. And I think most CISOs appreciate that cause that's got to open the door to the COO, CFO, and CEOs' office just a little more frequently for the CISOs.

I get it, the rulemaking was a tiny bit tone deaf, although they are right to say we had these specific requirements. They probably could have harmonized it better with CIRCIA. In fairness, CIRCIA was being done by Congress. SEC has rulemaking. They probably were legally not allowed to coordinate. That would have, I think, crossed a few article — you know, Article One, Article Two barriers. But it did come off the wrong way.

Overall though, good rulemaking.

TODT: I felt the governance piece, I think, is critical. I just really want to — the corporate cyber responsibility piece has never been more important than today. This cyber risk is a business risk, when we think about fiduciary responsibility, the digitization of corporate assets is the digitization of corporate risk. We have to be prioritizing this for senior executives, for boards of directors, to have that responsibility.

When Joe Sullivan was getting his sentencing in May of this year, the former CISO of Uber, the judge, Judge Orrick, looked at him and they said "you committed a serious crime but I'm wondering why your CEO isn't sitting next to you," because this isn't just an IT issue, and that is the future of business risk.

MATISHAK: Mary, do you want to...

BROOKS: Just a comment on looking at the authorities for that. Obviously, the SEC focused on investor — you know, investor insight into the companies that they're going into, CIRCIA-focused on more national security, kind of internal reporting.

So, I mean, one is just infusing the public — you know, kind of the public eye with so much more information about kind of cybersecurity threats and kind of giving us a sense of, you know, how widespread this issue is and maybe, you know, what sectors are being more targeted.

CIRCIA, because it's, you know, so private, I think we're just going to hear less kind of from the outside on that.

MATISHAK: Well, I think we're actually out of time. I wanted to have some closing thoughts but I — we ran a little bit over. I apologize. So I just want to say we'll all be watching this space closely, I think, and if predictions here at the end, if they're going to bear fruit or not, and if the country's moving in the right direction on critical infrastructure security.

And I want to thank you all for attending, thank everyone in the audience and everyone who's viewing online. And thank you all for coming today.

(APPLAUSE)

END