Fortifying Cyber-Physical Resilience: Recommendations from the President's Council of Advisors on Science and Technology

March 13, 2024
Featuring Harry Coker Jr., Jen Easterly, Dr. Eric Horvitz, Dr. Georgianna Shea, and Phil Venables
Moderated by Rear Admiral (Ret.) Mark Montgomery
Introductory remarks by Dr. Samantha Ravich

RAVICH: Good afternoon, everyone. I'm Samantha Ravich, Chair for the Center of Cyber and Technology Innovation, housed within the Foundation for Defense of Democracies, your host for today's event.

On behalf of FDD, we're happy to welcome you here both in person and on live stream for this crucial discussion of cyber-physical resilience and the findings of the President's Council of Advisors on Science and Technology, or PCAST.

PCAST is a federal advisory committee comprised of distinguished leaders from academia, government, and the private sector, that advises the president on matters related to science, technology, and innovation.

PCAST's newest report to the president, Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World, addresses a critical and crucial complex challenge of our time, the growing vulnerability of our increasingly interconnected critical infrastructure.

Historically, there was a clear separation of digital and physical systems in our critical infrastructure but now they have become profoundly intertwined, forming the backbone of essential services in our daily lives, from energy production to agriculture and everything in between.

These systems which we call cyber-physical improve efficiency exponentially but also increase the attack surface for adversarial cyber actors, a frightening trend which I'm sure our panelists will touch upon.

And speaking of our panelists, let me introduce them to you.

Our first panelist is Harry Coker Jr., who serves as National Cyber Director in the Office of the National Cyber Director where he advises the president on the development and execution of our nation's cybersecurity strategies.

Our second panelist is Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency, where she leads efforts to understand, manage, and reduce risk to cyber and physical infrastructure.

Our third panelist is Eric Horvitz, who serves as the Chief Scientific Officer at Microsoft. Eric also served as the working group co-lead in PCAST.

Up next is Phil Venables, who is the Chief Information Security Officer of Google Cloud. Along with Eric, he also served as PCAST working group co-lead.

Last but not least is our very own Georgianna Shea, FDD's Transformative Cyber Innovation Lab chief technologist, who also served as a working group member on PCAST.

Our discussion will be moderated by retired Rear Admiral Mark Montgomery, Senior Director at FDD's Center on Cyber and Technology Innovation, and Policy and Executive Director of CSC 2.0.

Before we dive in, a few words about FDD. For more than 20 years, FDD has operated as a fiercely independent, nonpartisan research institute, exclusively focused on national security and foreign policy. As a point of pride and principle, we do not accept foreign funding. Never have, never will. For more on our work, please visit our website FDD.org and follow us on Twitter at FDD. And that's enough from me, Mark, take it away.

(AUDIO GAP)

MONTGOMERY: Great, thanks Samantha. And thanks again to everyone who made it out here or is watching online. And a special thanks to Eric, Phil, and George for your public service efforts to improve our national critical infrastructure through the PCAST report development – I think we can all agree on your tagline that we need to fortify our critical infrastructure for the digital world we face today. And a special thanks to Directors Coker and Easterly for your sustained commitment to public serve. I know we're going to have a good discussion on it, so let's get into it.

First let's lay the groundwork for everyone, Eric. Your report is focused on the challenge of securing cyber-physical systems. Can you give us a quick rundown of what that is and how your work might differ from other fantastic commissions like maybe the Cyberspace Solarium Commission?

HORVITZ: Let me just say that cyber-physical systems was an area funded by the NSF [National Science Foundation] as a kind of a narrow frontier topic, six, seven, eight, years ago. And it became clear to us, Phil, and I, that we needed to sort of really define that term as where all of our infrastructure has gone over 25 years.

So 30, 35 years ago most of our systems, our infrastructure for water, energy, electric power grid, transportation, communications, it was physical in many ways; well understood by long-termers at these agencies and utilities.

But over two decades or so with the digitalization of the world these systems have become overlaid, intermixed sometimes, re-engineered with sensors, with adaptive optimization of various kinds, with tracking, financial systems, and so on.

And of course, these kinds of changes are wondrous. They give operators new kinds of powers for controls for precision operations for tracking and even for billing in new ways, but at the same time they've introduced new complexities, they are hard to understand, many of these systems were not designed from the ground up they are you know – there's sedimentary layers over time with add-on services of various kinds.

The internet itself was overlaid on many of these systems in ways that were not necessarily worked through in detail as to what the – all the dependencies and implications would be.

So at a time now where we have complex systems that few people understand even when they're experts in their own sector, where the complex attack surface presents a playground for adversaries to experiment with in new kinds of ways, and novel ways, and where we don't – we have a poor understanding how, whether 'a targeted attack or a natural disaster, a human error – we have examples of that we studied carefully – or even just a component failure, has unexpected and surprising effects which led us to think deeply about the notion of resiliency and resilience and principles of resilience being critical in moving forward.

MONTGOMERY: Hey, thanks Eric. I'm glad you said the word resilience which I think is about to be banned due to overuse in the cyber world here particularly...

HORVITZ: Let's not – ban the word.

MONTGOMERY: ... yes. But, you know, in fairness you're right.

George, your report talks a lot about very specifically the cyber-physical resilience. Can you tell us what that is and how it might be different from the standard old cybersecurity resilience?

SHEA: Yes. So – well, cybersecurity, it's the protection of your data. It's trying to keep the bad guy out of your network, out of your systems, so that you can ensure the confidentiality, integrity, and availability.

Resilience takes it a step further and says OK, we're going to get compromised. There's going to be an issue. So how are we going to ensure that mission assurance of whatever the objective is for that system, organization, sector, that they'll be able to continue doing that. It doesn't take the approach of putting up safeguards and controls to keep the adversary out. It's accepting that there will be issues. So not just cyber but also natural disasters, supply chain issues, so ensuring that in the face of diversity [sic adversity] you can continue that objective for your organization.

MONTGOMERY: Thanks. I'm glad you mentioned that because I think what we say here sometimes is you have to assume some level of penetration, whether it's physical or cyber. Once you have that, what are you doing to take care of your system to be able to rapidly, to either mitigate the impact of penetration or to you know, respond resiliently – or respond to it and recover from it. I don't want to use the word resilience again. That'd be guilty of my own sin. All right.

Phil, there's a ton of recommendations in here. Good ones. I recognized a few. And then a few I didn't which I thought was – you always want to see a few you don't know.

VENABLES: We had to keep you happy.

MONTGOMERY: You did. So I appreciate that.

Would you say the biggest policy – you know, we have two of the most senior policymakers in this field here. What do you – as you looked at it, what did you find to be the most important or coolest recommendation? And because it could be anything I'm going to try to force you down and talk about what I had not heard before but which I've now heard you talk about minimal viable objectives.

VENABLES: Yes. So I think you know, the big thing for me in the report was really about having more ambitious performance goals. And in fact when you, you know, hopefully read the report in detail you'll see pretty much all the recommendations are about how to support us all achieving more ambitious performance goals.

And not to take anything away from the great work that ONCD [Office of the National Cyber Director] and CISA [Cybersecurity and Infrastructure Security Agency], and NIST [National Institute of Standards and Technology], and MITRE, and many organizations have done already to establish performance goals. And I think it'd be fair to say that we all had to kind of walk before we can run and the performance goals we've set are necessary but we now need to take it to the next level with more ambitious goals.

And one expression of that is to really think about what's the minimum viable delivery objectives of each part of the critical functions in our critical infrastructure and start to be able to express those goals in the form of kind of you know, X numbers of people need to have access to a service, and not be out of that service for more than say Y days.

So I give an example. We want to be able to say, no more – I'm picking an example now, no more than 50,000 people should be without clean drinking water for more than five days.

Now, again, that's an easily laudable goal but if you sit down with owners and operators of infrastructure, with utility commissioners, with local governments, and think about how can you assure that in the face of all hazards, that's an exercise that still needs to be done. And you're looking at the supply chain dependencies, the physical dependencies, the ability to operate without network connectivity, the ability to operate under the assumption of intrusion, under attack. And how do you operate in a degraded state?

Another example of that, you could pick financial services to that point of operating in degraded states, which is where the minimum viable objective comes in. You could say, we want our financial system to be able to operate, very quickly and restoring quick – services quickly but you only need to bring back payments, and the ability to maybe cash Social Security checks, and make payroll and do credit cards.

You can probably take a lot longer to bring back mortgages and M&A and IPOs and all those other things. And so I think that's the important thing, is really stressing that because then you can test the edges and the stresses of what it really takes to do this.

The other thing I would say is the big part of the report is to start thinking about how do we shift performance goals from lagging indicators like breaches, cyberattacks, incidents, into leading indicators of what organizations need to do.

So I'll give you a very quick analogy. Think about industrial high-tech manufacturing, anything like that. People measure what comes off the production line for defects but what they actually do most of the time is measure the inputs of the process, the quality of the materials, the quality of the manufacturing, the maintenance of the machines, the design for manufacturability, all of those things that if you get right, you cannot help but have good outcomes.

We need to shift all of our performance goals in that same sense in the cyber-physical resilience world. This could be things like how effective can we reproducibly build our software? Can we operate in the face of loss of network connectivity at least in minimum viable ways? Are we applying enough money for preventative maintenance to stop the build up of you know, out-of-date legacy systems? Are we investing appropriately?

And if you get all those right – and those are challenging but if you get all those right, you can't help but have the good outcomes.

And the win-win here is many of those things have massive adjacent benefits of agility, productivity, commercial benefits, as well as security and resilience. And I think all of those performance goals, when you look at the report, everything builds to enable us to actually achieve those more ambitious goals.

MONTGOMERY: If I could ask one quick follow up on that the – you said we a lot and I think the "we" there you meant was probably some aggregation of the government and private sector leadership. Where do you see the balance in that? And is that balance do you think probably different across every sector?

VENABLES: I think it is. I mean I think one of the things again in the report we talk about the need for each sector risk management agency, to really increase their skills and capabilities. And CISA as Jen will probably talk about is doing a lot and actually carrying a lot of load. And I think there's many sector risk management agencies have done amazing jobs, and there's others that have done great jobs despite the absence of resources, and they need more resources.

I also think as well you know, speaking from the private sector, the private sector has done a lot but can and should do more. And one of the things that we call out in the report is the need for executives not just to have great tone at the top but the tone at the top needs to be connected with resources in the ranks.

And when executives at companies talk as they always do about this is the most important thing for them, that's going to be translated into actual action and actual resources. Now many companies do but there's also many companies that haven't taken the tone at the top and connected it with resources in the ranks.

MONTGOMERY: I think about that with sectors you know, we know without naming names, there are sectors that are really – I can name the good ones Energy, and Financial Services, where they have this tight relationship between the government, sometimes regulatory and that they could pass this data back and forth reasonably.

There's other ones, not naming names, maybe Department of Education, where they don't have the investment in the SRMAs to do this kind of thing. So when you call for this, I think one of the things you have to call for, and I know we'll talk about it, and I think you do in the report is, resourcing for SRMAs for the level playing field.

VENABLES: Yes.

MONTGOMERY: But let me pivot away from the PCAST Leaders, and to the government leaders that are going to – that have already implemented really on their – from their own leadership but also have had the chance to reflect on this report's recommendations.

So Harry, or Director Coker, I'll turn to you now.

There's a lot in this report. What recommendations or insights have you been considering?

COKER: Well, thanks, Mark. And thanks to the PCAST team for the report.

It's often said, you know, if you have too many priorities, you don't have any, but for each of the four recommendations here, they're all important, from the setting performance goals – can you imagine doing anything without having performance goals? You got to do that.

Bolstering and coordinating research, that's just good government, being effective and efficient. And there's a realization that cybersecurity touches us all.

The third one, tearing down the silos and bolstering the cyber-physical resilience, I'll come back to that but that – that goes without saying.

You know, Mark, you and I probably grew up in uniform around the same time, where Goldwater-Nichols was there, tearing down those silos is about collaboration. We are better when we work together. And as the president says, there's nothing we can't do in America, when we work it together.

And then the fourth one, was accountability and flexibility, focused on industry and the c-suite but frankly there's room for that in the government as well, when you talk about trust at the top, and resources in the ranks, that's what needs to happen on both sides of this public-private partnership.

I am pleased to say that this is budget week in Washington. And another quote from our president is, you know, don't tell us –don't tell me what your priorities are show me your budget and I'll tell you what your priorities are.

Well, if you look at the President's Budget you will see that SRMAs [sector risk management agencies] are a priority for us. And so right back to that that third recommendation, that's – that really is the one that I've been reminiscing on certainly since the report's been out but frankly in my three months in the –position.

It's – when I look at the SRMAs, I can compare it a bit to the good old days I guess, where cybersecurity wasn't given the level of importance that it is.

Too many folks looked at cybersecurity as an inconvenience as opposed to an imperative. We are turning that corner. We're making progress. And so with our SRMAs and with our public and private sector partnerships, we're turning the corner now.

There's many, many corners and frankly we can't slow down on that so I love all four recommendations. I've been reminiscing on each of those four, but you know, the public-private partnership which has the SRMAs on the front line of that is where I've been devoting my attention and energy.

MONTGOMERY: And thanks for that answer but I'm only going to take away that we need a Goldwater-Nichols for critical infrastructure, right?

COKER: Yes.

MONTGOMERY: I think that's full-time employment for my former Commission staffers.

All right, Jen, Director Easterly, the report says these critical physical cyber systems are found throughout all 16 critical infrastructures. You can also tell us if there's still 16 after the next deputies on the PPD-21 [Presidential Policy Directive 21] replacement. That's no small task to secure. Do you think we have a level playing field – Oh this is a loaded question – do you have a level playing field across all sectors? And I see Water is here, so Kevin Morley is going to keep you accurate from AWWA [American Water Works Association], but you know, do we have the same response capabilities and problems and say agriculture as we do in water.

EASTERLY: Yes. So great to be here. And congratulations on the report.

Let me step back a second. So you know, in 2013 when Executive Order 13636, and PPD 21, and the National Infrastructure Protection Plan, were published, there was no CISA. And CISA was created in 2018 by the Congress, in some degree to help operationalize many of the elements that were in those original documents that had not yet been done.

And so we were built in 2018 to play two key roles, to serve as America's civilian cyber defense agency but also – and this is in statute, to be the National Coordinator for Critical Infrastructure Resilience and Security.

So really with – our mission is to lead the national effort to understand, manage, and reduce, risk to the cyber and physical infrastructure that Americans rely on every hour of every day for Water, for Education, for Healthcare, Transportation, Communications. So to Eric's point, cyber-physical infrastructure is really critical infrastructure given the digitization and the connectivity among all of our infrastructure.

And it really hammers the importance of having one agency serve as that National Coordinator which again is codified in statute but which hopefully when we see the replacement for PPD-21, in the new National Security Memorandum, we will actually see that in print and a policy document, which will, I think, be very important to build on, not just previous policy documents, but to build on the work of the Cyberspace Solarium Commission, that was codified in the NDAA for 2021, laying out the role of CISA, laying out the role of the sector risk management agencies.

So, you know, I really welcome the PCAST report, and we had some great discussions about it, because it is incredibly timely, to be able to really give life to some of the – some of the work that we have been doing some of the work that we will do from a critical infrastructure resilience and security perspective.

So, you know, to your question about some sectors that are better resourced, some that aren't, I think we can all agree there are certain sector risk management agencies in certain sectors that have invested more significantly in security and resilience. And frankly, it's why we prioritized over the last year and a half working with SRMA, like HHS [Department of Health and Human Services], like EPA [Environmental Protection Agency], like the education that you mentioned, working closely with them, so that we can work with those sectors to provide free services and capabilities and really increase the conductivity with our role as national coordinator and, and folks like Kevin, and the associations and the sector industry partners are key to that to helping us in a more material way, drive down risk. And it's why I love some of the metrics in the report.

But you know, at the end of the day, even in finance, where I spent four and a half years before I came to CISA, you know, we invested billions of dollars in technology, hundreds of millions of dollars in our cybersecurity budget, but we were dependent on communications and water and energy. So as good as we were, it was really the importance of managing and reducing in a measurable way that cross sector risk. So that's why the role of national coordinator and the cross-sector piece of this is so important, and why I really welcome you know, those recommendations, in particular, the performance goals, and why I love pages 28 and 29, those leading indicators, because when I was the head of resilience at Morgan Stanley, we were coming up with those types of measures. And those are incredibly helpful. I know they're exemplars, but anybody that's doing resilience in a major business, frankly, large or small, should look at those two pages and my favorite part of the report, but it's also talks about importance of collaboration, importance of the National Risk Management Center and your critical infrastructure observatory. And then this idea of CC – what I like to call CCR, because I like band names, but corporate cyber responsibility in what corporations should be doing.

So, I just think it's a terrific contribution. And I'm not going to answer your question directly.

MONTGOMERY: But with a reasonable amount of time. Yeah, but from your lips to Caitlin Durkovich's ears on the National Coordinator for you all.

I do want to say that I agree that I think this report really supports CISA's strong leadership position in everything. The only thing I'm glad you guys weren't involved is like five years ago, we weren't in Congress, we would have called it like the cyber physical security agency like CPSO, which sounds like an infection, you know, I'm not sure. I'm not sure that's what you want for your acronym.

EASTERLY: I'm not going to, start with JCPO [Joint Cyber Defense Collaborative].

MONTGOMERY: Yeah, there we go JCPO. Yeah. OK, fair. 'Or SICI [Systemically Important Critical Infrastructure], but we'll get to SICI in a minute.

EASTERLY: SICI wow.

MONTGOMERY: All right. But Harry, look we gotta come back because it's, you know, staying on the topic of sectors you know, ONCD was also given a lot of responsibility or suggested that you all should have a lot of responsibility and I think you do, and a key role to play in managing our sectors management agencies. What's your take on how the administration ONCD can best support SRMA? And how can you continue and expand on that effort?

COKER: Oh, good. Another very relevant question and glad to be here with the Director Easterly, who's leading the charge on supporting our SRMAs. And we are in partnership with CISA and SRMA's in lockstep on helping to advocate for them. The key message for SRMA from an ONCD is we do have your back? And that message is not only for SRMA, but it's for the owner and operators of the critical infrastructure. We realize that resources are required. You know, SRMA are there pretty much because of core competencies and respective sectors, we have to develop the core competencies in cybersecurity. That's a painting a broad picture there. But nevertheless, cybersecurity has to be a core competency for SRMAs.

We've advocated for resources, if you all are not aware, you should take a look at the joint ONCD-OMB [Office of Management and Budget], cybersecurity budget priorities that we do every year. Again, trying to get resources in the ranks. That has paid off, you can look at the budget trends, incremental. But nevertheless, the trend is positive. And that goes towards this year. We're also working closely with a couple of SRMA's again, in partnership with CISA on how to bulk up their capabilities and capacity at the same time, capabilities and capacity. Sitting down with a couple of those, and you'll hear about that in more detail in a period of time. But nevertheless, trying to understand what their greatest requirements are, and how we can help them understand those needs. And then again, build those capabilities and capacity. I dare say it's a bit of shared services, if you will.

We're going to bring in expertise. Again, our partners have plenty of field support for the SRMA's, but that's what we're working on. And it should be clear, not just to the SRMA's, not just to the segment, owner operators, but to the American public that we do recognize the importance of SRMA's, we have their back. And they are key to the public-private partnership that we talk about regularly. Again, we can't just talk about it, we have to demonstrate it. Look at the budget, you'll see that we are demonstrating that so we do have the back.

MONTGOMERY: I'm really glad you entered on the budget saying two people need a big shout out. I think the deal that one of your predecessors Chris Inglis made with Shalonda Young showed a lot of prescience by director – OMB Director Young. I've never met an OMB director that willingly like shared power.

COKER: Yeah.

MONTGOMERY: I mean, it's the nicest way to say it. And she did, you know, give you opportunity with the deputy NCD with the federal CISO [Chief Information Security Officer]. But more importantly, the budget and Drenan Dudley, you know, one of your deputies, I just think, you know, there's magic in that if we can get real reviews of agency budgets. That's – because what did you say - resources, you know, show me the resources.

COKER: Yeah.

MONTGOMERY: Resources are the deal, and in the end, we have to see the SRMAs properly funded.

COKER: You're right, and I'm glad you mentioned that. I'll just elaborate on that partnership with OMB. The federal CISO is dual hatted within ONCD as our lead for federal cyber. That partnership is essential. The individual we have there some might call him a unicorn. I just call him a subject matter expertise and a patriot and I know we have more in America that can help us. But Chris DeRusha is certainly a treasure and paying dividends, not just for OMB not just for ONCD, but for the nation's cybersecurity.

MONTGOMERY: All right, thanks. Yeah. Doesn't look like any of my kids' unicorns, but I'll go with you on that one.

Hey, Jen. So, I had – I said SICI, so I got to come back now. You've been an advocate for identifying the less desirable name systemically important entities. And now you look pretty prescient. I mean, I think Change I don't think any of us – if you knew what Change was, it's because you had like a terrible Medicare experience in the last couple of years before two weeks ago, but now we all know who they are. Because it turns out, they were pretty much the definition of an SIE. Where do you think we can go with this? You know, what's your – what future do you think about as the next steps for SIEs?

EASTERLY: Yeah, it's a really interesting question. Actually I was talking to Anne about this – Anne Neuberger about this yesterday. So just to step back – again, SICI, Systemically Important Critical Infrastructure. When I was on the red team for the Cyberspace Solarium Convention, that was my big contribution, do not call them SICI – I like that Sam's back there laughing.

So, we came up with a better name SIE, Systemically Important Entities. And we've been working on that for the past few years. Now, these are organizations, that the disruption or the malfunction of which could be extremely damaging to national security, to economic security to public health and safety. And as I think the commission envision, there are not thousands of these entities, right. So, the list that we have, that we have been working on for several years now is less than 500. That list is shared with the sector risk management agencies, because of course, we need their expertise, to be able to validate those lists and then past that, needs to be shared with – with industry.

But when the Change Healthcare incident happen, I actually went back and looked at that list. And you saw the parent company, you know, obviously, one of the biggest – biggest companies would be something that we would think about as systemically important entity. But Change was not part of that. And I think it really implicates a really important thing that we need to do coming out of the new National Security Memorandum, which is, and we've done some of this work, we've actually taken each of the national critical functions, so 55 of them, and we've decomposed them. So, provide health care, for example, is decomposed into 134 sub functions, one of which is to provide payments for healthcare, and you would think Change would – would fit into that.

But you can see how it can go from less than 500 to several thousand, when you actually do the decomposition and then look at specific companies within that. Now, that doesn't mean, we're not going to do it. I think it's one of the really important things, we have to sit down with the sector and with HHS, and really look at what we can do to better highlight those companies that are much more critical than we actually were expecting.

So that work is continuing, I think we will be doubling down on that work with the new sort of authorities that we'll get coming out of the NSM (National Security Memorandum). But it's it just illuminates the fact that we have to have an understanding of global supply chains, and where impacts can be felt most seriously to the American people.

MONTGOMERY: I appreciate that. And I have to imagine someone senior at CISA said you're not going over 500 and then that's why we've ended up less than 500. Because if you let the government decide something like this, you can be at 14,000 in a heartbeat.

EASTERLY: Yeah, but as, you know, that wouldn't ...

MONTGOMERY: Yeah ...

(CROSSTALK)

EASTERLY: If everything is a priority nothing's a priority. Yeah.

MONTGOMERY: No, I appreciate that. Thanks. The – Phil, I have to ask one of the most innovative ideas and one I've certainly not seen in other Commission's is the idea of the national critical infrastructure observatory. Can you walk us through this recommendation?

VENABLES: Yeah. So, it was interesting. So, you know, you know, first of all, a big shout out to is in the report, a large number of people that we interviewed over the period of a year, that contributed many of the ideas that we encoded in the report. And one of the things that we had an intuition of initially, but was confirmed in talking to dozens of people in various different settings was this notion that our adversaries have a better map or understanding of our critical infrastructure than we collectively do ourselves. And that's a worrying place to be. Because you know, to what Jen and Mark were just talking about, that gets us in positions where we just don't understand what our hidden dependencies are, where you get these, these identified critical areas that may be in a third, fourth or fifth party dependency dependent on some foundational thing that could have this kind of big knock on effect.

And so, we came up with this idea that says, wouldn't it be great to have what you might call a national critical infrastructure observatory, and I like to think of this as almost it's like a, like a digital twin of the United States critical infrastructure that we can have a big system that is constantly updated, that represents a model of our infrastructure that we can ask questions of, we can say, what's the biggest concentration risks? What are these dependencies between sectors where you've got something like something critical, that is, in fact, dependent on something that is not identified as critical? And what does that dependency mean? We can then ask, in the case of emerging vulnerabilities, so some of you know, a few years ago, there was a big vulnerability called Log4J. Everybody introspected on that everybody analyzed that. But a lot of the reaction to that was a lot of requests for information of companies to say, are you in good shape? Are you in good shape, you're in good shape? And so, we didn't have that kind of ability to kind of manage that.

And then ultimately, if we had this observatory, we could then potentially, and I don't want to kind of jump on the – and turn this into an AI conversation. But we could use AI against that to say, what are the multistage, multi-step attacks that could be formulated, that we can identify, get ahead of, before our adversaries apply the same techniques to look for the things that we've not spied. And there's huge potential here.

But to be clear, because a number of you will be thinking in your head, wow, having this big collection of information could actually be pretty dangerous. And so, we have to protect – we would have to protect it, potentially, in some respects, could need to be classified depending on how we use it, and what's in it. Or it could, for example, use some of the innovations in privacy preserving computation or multi-party computation to achieve the effectiveness without ever aggregating together. But fundamentally, we need this to identify those dependencies, those concentration risks, and look for those 80-20s those leverage points, that could be a weakness, but the leverage points that could be a big means of upgrading infrastructure, by finding out what those leverage points are.

MONTGOMERY: Go ahead.

HORVITZ: Just to add to that, for me, thinking deeply about having a critical infrastructure observatory was motivated, not just to the side by artificial intelligence technologies, the idea – we're seeing capabilities now systems that can take in a large corpus of information. And given a directive can reason in very creative ways across sectors and across dependencies that would really be beyond the typical analyst or adversary. So, we want to basically get ahead of that right now with our own fund of knowledge.

And it's was pretty clear, as Phil mentioned, from our engagements with – with multiple agencies that our adversaries most likely have a much better map, cross-sector or cross sectoral map of the United States critical infrastructure that we do.

EASTERLY: Just – I should jump in, and we had this great discussion. This is a lot of what we've been building in the National Risk Management Center. And so definitely like the idea of kind of a common operating pictures, I would call it in the military, of that critical infrastructure, the connectivity that dependencies. Because we live in a country where there's a lot of good privacy and I don't think we'd have necessarily that same picture that some of our adversaries or Phil would call them adversaries - would have.

However, I think, as we are able to operationalize what will be in the National Security Memorandum, I think we will get to a picture that we can then build out so we can more clearly illuminate those dependencies and vulnerabilities.

MONTGOMERY: You know, I think is veteran you Harry and I would recall, like JWAC when I think of this Joint Warfare, Analysis Center at Dahlgren, and you know, that examined our enemies in great detail, but maybe a JWAC turned on ourselves in a way.

VENABLES: I don't know if any of you were Air Force, but I would like to think of that this is the OODA [Observe, Orient, Decide, and Act] loop. So, our ultimate measure of success is speed. If our OODA loop can be faster than our attackers OODA loop informed by observe – you know, that observability then we win.

(CROSSTALK)

MONTGOMERY: OODA loop was forced on all of us, but yeah I've got you. Thanks. Hey, Eric, I'll stick with you. Your report talks about how the dependencies of digital systems have on one another. And in part, that's the cause of the issues we're seeing now. So, what's the best way to mitigate kind of the cascading effects, you might see as a result of these dependencies?

HORVITZ: So, we have a bunch of experience now over decades in the software engineering world with what's called verification, which includes static analysis of all dependencies in a software package or dynamic analysis, you run the thing and see what dependencies might be that go beyond your ability to see when things are at rest. And it would be way over the shot – over the top moon – moonshot to imagine where we asked for that of cyber physical systems in the real world.

So, one notion is stepping back a bit. And I like to think about this as looking at the leading indicators we have as exemplars, as Jen mentioned in the report, as North Stars, really about managing dependencies. If you look at each one of those things, they're about – well, how do we really deliberate and reflect and have measures that give us a sense for – for example, the modularity of our systems, that would give us a sense for how connected they are in a way that we understand. We would have an indicator called Bounded Modularity, we even got a little technical in defining. Well, that's in a large cyber-physical system. That's the computation of for all single faults that you recognize, what's the average distance it travels, across cascading through multiple systems? Give us a measure of the bounded modularity of this system to give a sense for the – its health.

Again, a North Star calculation, but pulling back on that I like to go back to what's the minimum viable operational objective of a system, start there, start with key potential failures and look for just two steps out, one to two steps out from the key failure. What happens if the internet is out? What happens if there's a ransomware attack on the billing system? So that leads to a scarcity of fuel and northeast sector and the Northeast – Northeast sector of the United States just because our billing system is out? Should a fumbling up a file in an FAA [Federal Aviation Administration] computer lead to several thousand flights being delayed for hours? Could that have been seen proactively? What kinds of reflection and deliberation are needed just to go a couple of steps deeper?

Now, there's this fancy term people may have heard called digital twin, building a digital twin of a system, a high-fidelity representation of the cyber and physical aspects of the system that's focus of attention, that's hard to build in general and hard to do modeling and simulation on. That would be wonderful for managing dependencies and identifying them and addressing them.

But you can step back from that and begin looking at simpler models, asking for more reflection, asking for some study of key faults and single dependencies on them, for example, as a starting point, I think deliberation and focus on two depth cascade would go a long way across our cyber physical infrastructure in United States right now.

MONTGOMERY: Thanks. And I'm glad you used actual examples in your simulated examples of casualties we've had - Harry, I mean we've heard - there's got to be some barriers to all this PCAST talk, not just resources, which we've dealt with.

You've really talked passionately in your first three months and previously about the cyber workforce, how is the need to fill cybersecurity jobs going to affect the kind of critical services that underpin this physical cyber portion of our lives?

COKER: Oh, workforce, I'm glad I get a chance to talk about that - I never pass on that opportunity. And frankly, it doesn't matter where I'm working, people make things happen. Relationships make us or break us. We talk about relationships between people in mission, in and out of uniform, but with regards to cyber workforce, you can – I'll use a conservative number, 500,000 open cyber positions in the United States, conservative number.

So, whatever we've been doing to date has been insufficient, it's been lacking. So, we need to make real progress on that front. And I think we've gotten lost in =past government assignments when we've talked about cybersecurity jobs, we've talked about competing against, you know, Microsoft and Google.

They're a part of national security, all right. We need to complement not compete. We lose sight of making sufficient gains when we talk about competing against entities that are also protecting critical infrastructure, so that's one, let's not get caught up in that. You know, make your environment right and people will come and stay.

But to close that gap, a couple of things we're doing. And you know, my first trip in this position was to a community college - Baltimore County, it's a two-year school. We went there to communicate, not just to those students, staff and faculty, but to America that - that four-year degrees are not required to make contributions in cybersecurity. You don't need it.

We thought we needed to change the rule, turns out, for federal contracts, you didn't need to have a four-year degree, but that was the general thinking. So, we were misinformed about that, so we've been working to get that word out. Four-year degrees are not required for cybersecurity federal contracts.

Where we want to go is skills-based hiring. You know, degrees are nice, but it's really the knowledge that we have to have. You know, I actually have a Computer Science Master's degree from NPS [Naval Postgraduate School] in Monterey, decades and decades and decades ago. It looks kind of nice on my wall, but...

MONTGOMERY (?): Was Grace Hopper one of your professors (inaudible)...

COKER: Yes, yes...

MONTGOMERY (?): ... with how far we're going, here, all right.

COKER: ... yes. So, I have the degree, but it's the skills that matter most. And you don't need that Masters, Bachelors or in some cases, you may not need a two-year degree, it – it's what – what we know.

So, we need – we need employers to understand that, believe in it and then we need the system to work to – to change that.

Another obstacle on this is that there's a belief amongst a lot of us that an individual has to be esteemed in stem to make contributions to cybersecurity, wrong - wrong. We need creative, agile, persistent patriots to work in national security and cybersecurity.

So, those are just some of the obstacles. We are taking those on. Again, next week, going down to Fayetteville Technical College in Fayetteville, North Carolina to again, convey to the folks there that four-year degrees aren't required, but also Fayetteville has a lot of military there - military dependence, and we want to convey in particular to the military spouses, that you can make a contribution to national security. Oftentimes, these families are moving around the country – you know, there's opportunities to be mobile and contribute to a cybersecurity career. We need to get that word out. We're going to continue to pound the pavement on that front.

MONTGOMERY: Thanks, Harry. Well, I'll let my daughter who's doing her art degree know that NCD's hiring. All right, good.

All right, George, you've been an advocate of cyber-informed engineering and the reports suggest that work in this area is useful. For the uneducated, what's CIE mean and how can it be helpful in this?

SHEA: So, Cyber Informed Engineering is really the secure by design. It's 'taking the engineer who's developing a system and educating them on the impacts of cyberattacks so they can understand what the requirements should be and then alter their design.

MONTGOMERY: That's it?

SHEA: That's it. It's - it's super easy and it's – it's kind of common sense...

MONTGOMERY: Got to look my next question up, you're going too fast.

All right - all right...

VENABLES: A suggestion one of my - you know, additional favorite recommendations is what one of the ones George came up with, which is the notion of - we talk about the cybersecurity workforce, but I don't think we talk enough about how to embed cyber-physical, like, capability inside other engineering professions.

And I think it would be just transformational - you know, clearly transformation if we had more cybersecurity workers and all those great things, which I think is foundational, but wouldn't it be even more amazing if every one of our professional engineers - you know, every ABET [Accreditation Board for Engineering and Technology, Inc.] accredited-engineering program, whether it's mechanical, electrical, computer, civil engineering, chemical engineering, had a core part of what they do to think about cyber-physical resilience, so when that civil engineering is signing off on that water utility design or that chemical engineer is signing off on the design of that chemical (inaudible), they're thinking about the cyber-physical part of that - that'd just be amazing.

(CROSSTALK)

HORVITZ: I - and I should say that many of the concepts that we talk about in this document are not foreign in engineering in general - fail safe design, fail over. There are notions of flexibility and resilience in a system and tolerances. The idea of backing off to a different operating mode when necessary - so these - but the - it's scattered right now, and it's not necessarily core curriculum.

EASTERLY: I just want to jump on this...

MONTGOMERY: Yes.

EASTERLY: ... this concept. You know, it's incredibly important that we prepare for and expect disruption. Whether that's a cyberattack, a technology outage, a weather event, an infectious disease, a terrorist attack, we do need to plan for it. We need to prepare for it. We need to exercise against it. We need to be able to respond and recover, which is why ensuring that we're actually looking at the infrastructure that owners and operators use to provide services to the American people are in fact, measurably resilient.

And that's why I love those indicators, but you know, at the end of the day, you - the point that George brings up on the secure-by-design, I mean let's – let's just be realistic, we have a multibillion dollar cybersecurity industry because software manufacturers, technology manufacturers really never had to prioritize security.

Even some of those software developers, how many of them are being taught secure coding, memory safe coding. I think in one out of 20 computer science programs, they have to take a security course.

So, this needs to be an effort that starts in education but the big technology manufacturers need to design, develop and deliver products that measurably decrease the number of exploitable flaws and defects, frankly and prioritize security over speed to market and features and driving down cost, because that's frankly why we are in this reactive mode trying to ensure that we can keep infrastructure safe.

So, I think that is one of the most important parts of this report, and it really resonated with us at CISA, because we've spent the last year really trying to create greater awareness about all of the things that need to be done from a technology manufacture perspective to drive down the number of exploitable flaws that are causing all these cyberattacks.

VENABLES: And I think that - that's really important because I think it's 'back to those dependencies. I'm not just viewing dependencies as a point of concern, but as a point of opportunity.

And exactly as I've heard you talk about before, that under each critical infrastructure industry, there's a set of software providers, tech providers, infrastructure providers, that are the real heart of the dependency because again, across each utility sector, even say financial services, which is renown to be sophisticated in technology, underpinning thousands of regional banks are a small number of banking IT service providers.

You know, they can be considered a point of risk, but they can also be considered a point of opportunity just like the large tech companies, because if we get those things right, the ripple effect is going to be massive. And I - I completely - you know, agree with the notion that everybody has a responsibility to drive this secure-by-design and secure-by-default.

In fact, one of the - one of the interesting graphics in the report when you read it, we have this kind of - you can't do a report without a four quadrant diagram, but we kind of plot this - this notion of companies that - you know, have a potential high impact and companies have high capabilities, so companies that have high impact, if it goes wrong and they have high capability much should be expected of them.

And I think that's in the category of the big tech companies and others. There's also one of the quadrants which is - you know, if something goes wrong with this company, it's a massive societal impact, and they have no capability or no resources, then that's what we can in the report, the bad place. And that place - that quadrant should be empty, sadly it's not empty today. And we either need to make the impact low or raise the capabilities, but we have to focus on that quadrant especially.

MONTGOMERY: And I think that's what the ransomware criminals call my target set, right?

VENABLES: Yes, yes, that's right...

MONTGOMERY: (Inaudible).

COKER: Mark, if I could...

MONTGOMERY: Yes, please, Harry.

COKER: This treat is in alignment with one of the two big shifts called out in the National Cybersecurity Strategy, shifting what some people call the burden of defending cyberspace, I call it the responsibility of defending cyberspace from those who are least capable to those who are most capable.

These companies you've been talking about, it is 'unfair to expect a child or a person who's not familiar with cybersecurity to have to protect themselves totally. That's where the federal government, big tech industry need to take up their responsibility to help defend critical infrastructure.

And I'm from small town Kansas, and the - the local water system, the local school system, they're going up against nation states and - and not fair. That's - I can bring it back to the SRMAs, to our partners, all of our partners here, but again, it's taking the responsibility to those who are most capable to defend the ecosystem.

MONTGOMERY: Thanks. Well, Jen, you guys actually have a bunch of – under - efforts underway to kind of, like, direct his policy – a National Infrastructure Protection Plan, National Critical Infrastructure Response Plan. I think they align closely with the PCAST efforts. Obviously, I haven't read - read final drafts or anything.

Can you talk us through the importance of these documents, when we might see them, and - and how you think they align with the PCAST Report?

EASTERLY: Well, I'm really hoping we see the replacement for PPD 21 in the near term. I think it's a really important document. It's been over 11 years since PPD 21 was published, and I suspect, like all documents out of the White House, there'll be some very aggressive and unreasonable timelines that appear in that document.

So, we've already kind of gotten a head start on some of the ones that we are going to need to implement, but that will involve some of the sector risk assessments. It'll involve what ultimately will be very important cross sector risk assessments. It will involve a rewrite of the National Infrastructure Protection Plan, a revalidation of the systemically important entities.

And then, in addition to that, I think it's important to recognize some enabling work that we've been doing, the Cybersecurity Performance Goals, which the White House asked us to do as part of NSM and NSM published in 2021 are very consonant with what it's being asked for in the PCAST Report. We published cross sector performance goals, we've done two iterations. In a couple of months, we'll publish sector specific ones for finance and information technology and energy.

And I think those are really important because they are measurable. We all know the NIST cybersecurity framework is a gold standard, but frankly, it is very difficult to align yourself with the NIST Cybersecurity Framework if you're a - a under-resourced water facility or a small school or a rural hospital.

And so, the idea behind these cybersecurity performance goals where - it's an extract, we've worked on it with NIST. So it's 38 things that must be done, characterized by cost, complexity and impact that entities can do to reduce risk, in a measurable way.

And so, I'm excited about getting more of those out there. I am a big proponent of minimal standards for critical infrastructure. I think that's incredibly important.

And then the other thing that we are trying to do, we recently published something called the Physical Security Performance Goals. We did that for faith-based institutions. And what we ultimately want to do is create infrastructure security performance goals, which reflects measures that need to be taken from a cybersecurity perspective and measures that need to be taken from a physical security perspective.

So, I'm excited about all of that coming together, and again, I think the recommendations will only reinforce a lot of the good work that we're going to be having to do, and - and as you mentioned, you know, the last thing that came out of the National Cybersecurity Strategy was an update to the National Cyber Incident Response Plan, which we should get out later this year.

MONTGOMERY: That's on - if I could translate government, it sounds like - pretty soon - as soon as we can get that PPD 21 rewrite done, we'll see a lot of other stuff. And I hope part of it too is the sector-specific plans because I think those get down to the more germane things that - that industries can go at.

Alright, Harry, I think you almost answered this already, but I'll just give you another chance to talk about the private sector for a moment. The – you know, a lot of this stuff's been about government so far, but clearly Chairman Gensler at the SEC has kind of made pretty clear that the, you know, boards and CEOs, C-Suite are also accountable for cybersecurity.

But more broadly, what would you say to industry as they look at a report like this and maybe not here the software industry but the critical infrastructure in – you know, this big 85 percent of owners and operators of our critical infrastructure, when they read this report?

COKER: Well, takeaways from me from former industry perspective is the import of – of the partnership, the import of critical infrastructure, the need for the government to work with the private sector. Neither of those partners are going to get it done by itself.

Again, every one of those recommendations has something for all of us. Priorities need to be consistent but we have to resource the priorities. And Phil said it and I said it a couple of times already, it's in the report – you know, the talk from the top needs to transition to resources across the board.

Another thing that has concerned me but I think in the report – if – when one reads it, you can see that there's no time for complacency. I've 'had concerns over the years about whether cybersecurity was going to be resourced. Congress gets it. Congress stood up CISA not that long ago, stood up ONCD even – fewer years ago.

Again, the budget shows the priorities. We are applying the resources. It – it's an effort that we have to win. So there's no room for complacency. And, you know, I can look at the portrait y'all have on that wall back there – had a quote by Winston Churchill – "never, never, never give in."

We've painted some realistic pictures – I almost said scary pictures – they're realistic. When Jen and I and Director of FBI and the then Director of NSA and U.S. Cyber Command testified a month ago about the unacceptable risk that America's critical infrastructures have been placed under by the PRC (People's Republic of China), America needs to know that, industry needs to know that.

So awareness is a good step, doing something about it. Resilience is the other step that industry needs to take with the – public sector. So we need to be ready, we need to react, we need to respond, and we have to recover because there will be – there are nonstop attacks against our critical infrastructure.

So it's 'real. Don't expect it to stop any time soon. Be ready and respond and recover.

MONTGOMERY: You remind me of two things when you say that. One, the – much like we did before Ukraine, the administration has done a good job – I think the Volt Typhoon releases of information is very timely, to say look, you probably suspect this, you can tell we're – caring –about it, but here's some specifics – these sectors – you know, Colonel Mustard with a cane in the library...

(LAUGHTER)

... you know, these sectors, this country, this risk. And I think it's very important that the four of you were up there, you know, giving that message.

COKER: I agree with Mark. And it was important when America released that information on the eve of Russia's invasion of Ukraine. I was retired at the time, at home, not setting an alarm clock, sitting around in slippers and a robe all day. But I read that...

(LAUGHTER)

... what used to be intelligence – being in the newspaper, I'll 'call it information – but previous experience has told me that the – that information came from some exquisite collection. But the United States made the right choice to make America and the rest of the world aware of Russia's intent. We need to do that on a regular basis with cyber threat intelligence as well and share it with our partners.

As America correctly concluded with that intelligence that became information, it's typically the sources and methods that need to be protected, not always the information. We got it right then. We need to get it right every minute of every day when it comes to cyber threat intelligence.

VENABLES: One of the things that I think's interesting and what we tried to get across in the report was a little bit of optimism as well. So...

COKER: Sorry, I'm not your guy.

(LAUGHTER)

... so it's interesting. I mean, the situation we're in is clearly very serious, there is more ambitious things to do, but there are glimmers of hope every day, there are large organizations defending themselves every day, there are intelligence successes. We are making attackers work harder and harder all of the time.

And there's a reason we kind of threw that William Gibson quote in there in the report, "the future's already here, it's just unevenly distributed" – a big part of the recommendations is how do we get these bright spots of great work, you know, examples of secure by design and secure by default, and how do we get them in more places more consistently with more rigor and no falling back to the prior state, and doing that sort of just becomes the default mode of operation for organizations, large and small, across society.

And – I think we have the bright spots to do this. So – and the optimistic thing is we know we can do it, we just need to do it in more places.

SHEA: Well, I just want to quickly throw in one very positive thing I saw recently, the NIST Cybersecurity Framework 2.0 that came out. It was released February 26th. I think our report was the 27th. They have a new sub-category in there, infrastructure resilience.

And so if you dig into that, it – that's – actually says that you are meeting your resilience requirements. Oh, so great, what are the resilience requirements? Now, organizations start to ask themselves those questions and look at a report, come up with their minimal viable objectives, and engineer them the way they need to.

MONTGOMERY: Yep. Georgia, I'm glad you mentioned this. That was the other one from – that I thought of when Harry was talking, which is we've said NIST a lot. If you read any executive order that's come out in the last four years, it's tasked NIST with, like, two or three things. I think the A.I. one tasked it with, like, recreating itself.

(LAUGHTER)

There's laws that tell NIST to do things. I have to tell you, when you look at NIST's budget, it doesn't look like it's doubled, right? It hasn't gotten the treatment that CISA's gotten over the last five years, in – you know, in terms of rightfully growing it more than 100 percent. NIST has grown, you know, 18, 20, 25 percent.

I – I'd – for the members of the Fourth Estate, I'd take a hard look at this budget, see how NIST did. If they did well in Cybersecurity Division, then, you know, our resources are matching our rhetoric. If they didn't, we're going to have trouble because we assigned NIST over the last year or two years a lot of work, and I sometimes question how many engineers – and I certainly read the reports of the physical construction of the buildings and it makes me feel, if they're not fixing that, they may not have enough people up there. So 'let's make sure we're taking a look at that.

All right, enough from us. I do want to go to Q&A in the audience. We have people with mics. So put your hand up and Erin will come around.

Go ahead. You yell it out and I'll repeat it.

(INAUDIBLE)

MONTGOMERY: You got it? Oh, we got it fixed. She's faster than me.

WEILER: John Weiler, I.T. Acquisition Advisory Council. Phenomenal content here; report's great, and I really want to build out some of the thoughts on these measures of effectiveness, because I've been working on things like that with zero trust and SCRM [Supply Chain Risk Management], measure what matters. What is the role for these in – these commercial-supported standards bodies in government? Because I believe public-private partnerships could be a role in capturing some of those metrics in the technology domain, you know, the things like function point analysis. And we're not applying the work that is supported by Fortune 500, Silicon Valley through these independent standards bodies, these think tanks, these 501(c)(6)/(c)(3). Because I think what you've said here and in this report has to move forward, and I believe there is work being done supported by Fortune 500 and Silicon Valley that's not seeing light.

VENABLES: Well, you know, I think it's interesting – so I think it comes back to this thing that we – and this is why we need everybody's help on this, is that we just have to be more ambitious. There is many working groups on standards and cyber metrics that come up with great ideas, and we've got some of these in the report. And then everybody says, "Oh, it's going to be too hard. Nobody can do that," and then we never do it. And we've now actually just got to bite the bullet and do these things.

The classic example I always use – there's one thing in the report about this notion of software reproducibility. So what percentage of an organization's software can you have under control and reliably rebuild? And the – I get pushback on that quite a bit, which they say, "Well, you know, boards and executives shouldn't pay attention to that metric. It's kind of in the weeds." And I go, "Hang on a minute. Imagine if you're a chief financial officer sitting in front of the board, and the board says, 'Have we got all of our finances under control? And is there a single general ledger and a cash flow statement?' And the chief financial officer goes, 'Well, not really. It's kind of in spreadsheets here and there, and we have a few different places where we keep all of this.' You know, there'd be a big emergency action to bring it all under control."

It's not – this is a difficult problem so I'm not kind of castigating the chief information officers out in the world, but we have to set as an ambitious goal that organization should have their software under control, reliably reproducible not just for security, but for resilience. And again, the great thing about it for boards and CEOs – the organizations that do that have massive productivity increases and agility increases, so you get security resilience allied to business objectives. You know, what's not to like?

PITCHER: Steve Pitcher, Joint Staff J6. I'm the senior cyber survivability analyst for the department, and it really is refreshing to hear all of what you've said here today about, you know, the performance goals and you know, resilience at – I know that Mark doesn't want to hear much more about resilience, but...

(LAUGHTER)

... but it is critical. And one of the things – reason I'm the senior cyber survivability analyst is we've got to stop saying just cybersecurity. We either have to say cybersecurity and immediately say cyber resilience, or we need to change our vocabulary so that people understand that we are going to – you know, the adversary's going to get in and we've got to find a way to be resilient enough to ensure that the mission is accomplished.

And so I'm looking for help from everybody to change our mindset from cybersecurity compliance, because that's the only thing people think of when you say cybersecurity. And if we're going to design – you know, have secure by design, resilience by design, we're going to have to define those threshold performance requirements for a minimum viable capability in our contracting doc, because it's got to be contractually binding, you know, mission-focused, threat-informed and system-specific. We've got to get away from, here's the 38 standards, OK, or the 72 zero 92 zero-trust standards by 2027 to get to, what are their – what are we trying to achieve? What are those leading indicators that we need to put in there? And we need your help, and can we get you to help say "cyber survivability"?

MONTGOMERY: Well, well thanks. I'm glad. It would've been totally inappropriate for someone from DOD to ask for resources from the other agencies, but...

(LAUGHTER)

Rhetorical and policy support, I'll go along with.

Anybody want to say anything on this, or on? I think it would – let's go to the next. Scott?

SANDERS: I had a question for Director Easterly on one of the 16 areas, food and agriculture, that goes back to something Director Coker was talking about. He knows I own a farm, and so...

UNKNOWN: And a distillery.

(LAUGHTER)

SANDERS: ... and all those little pieces in there, all those hundreds of thousands of farms across the United States cannot protect themselves. It's just way too hard. So how do we do that? How do we, as one of the 16 sector – and food is different from agriculture, but there's a lot in there. And one little family farm is not critical infrastructure for the U.S. However, all of them collectively are. So how do we approach – I mean, it's different than oil and gas. It's different than banking. So I just wanted to get your thoughts and inputs on that, please.

EASTERLY: Yeah. So first off, we do a national cyber exercise called Cyber Storm that we do every two years. This year is in April, and the focus is on food and agriculture, a major cyber attack. So you're welcome to participate from your farm and...

(LAUGHTER)

... call in advice. So the...

UNKNOWN: assistance.

EASTERLY: Yeah, well, exactly.

So the way that we're thinking about this is as national coordinator, we are able to provide a lot of services, as well as expertise, training, assist in exercises. I'm proud to say that while there is a big concern about cyber workforce, we've actually hired 1,700 people over the last two-plus years, so we are doing really good getting expertise in, to include ICS expertise, notwithstanding certain government reports that have come out.

All that said, what we plan to do is we have an – a liaison within our sector, somebody who comes from the food and ag world, who is working with FDA and the Department of Agriculture in their SRMA role. And when this NSM comes out, I think we will see greater focus on working with the SRMAs on how we can lay out what those risk standards are, what that cyber – or what that sector risk assessment document looks like so that we can then use that on managing cross-sector risk, because of course, food and ag is heavily dependent on water and power. So that's something that we've actually put – I don't know if you saw the NSM that came out from the White House specifically on food and agriculture, but there's been a lot of work that – put into it, but much more work to come.

SANDERS: OK, thank you very much. Appreciate it.

EASTERLY: You bet.

COLE: Hi. Tony Cole, from Digital Directors Network. I was really glad to hear you talk about tone at the top, you know, in the report, as well as, you know, mentioning the SEC new rules around cybersecurity reporting for publicly traded companies. And I just would love to hear your thoughts around what else we can do, because even though that policy is relatively new at the SEC, you know, most of the new reports that have gone out, the AKs and the other filings, you can see some of these companies are in violation, you know, of those new SEC rules.

So what are your thoughts about bringing the rest of industry along that aren't publicly traded companies to get boards actively engaged in thinking about cybersecurity and building a tone at the top versus specifically just publicly traded companies that fall under those – that regulatory framework of the SEC?

EASTERLY: ... let me hit this one.

So a couple things. I think whether you're the CEO or a board member of a public company or a private company, if you are critical infrastructure – and of course, not all critical infrastructure entities are public companies – CEOs and boards have to own cyber risk as a business risk and as a matter of good governance. You cannot delegate the ownership of cyber risk to your CISO or your CIO and then fire them when something goes wrong. And we have made this point – and I was glad to see it illuminated in the – in the report itself.

But on the SEC rule – so just to be clear, the – that is specifically on shareholders, right, that – and I do think it will have a positive impact ultimately. But I want to say two things.

One consideration – I want to ensure that public companies do – it does not affect public companies collaborating with the U.S. government because they're fearful that they will get sued if they share information, because we've made a lot of progress over the last two and a half years in building connectivity between the U.S. government and the private sector that has really helped us to understand the threat environment and reduce risk. And so I would want to ensure that public companies don't backtrack on that.

Two, the thing that I think will get to your point is the Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA, another crazy government acronym. That NPRM will come out shortly, Notice of Public Rule Making. We will see the rule go into effect next year, and that will help us understand more about what is going on, and people will report to us not to shame them, not to stab the wounded, but rather so we can understand and help them and then use that information to be able to help others before they get hacked.

So at the end of the day, I think that will make a big difference, as well as giving us a better understanding of what's happening in the critical infrastructure ecosystem that we just don't have today.

MONTGOMERY: All right. Thanks. And I will say one thing on – the one thing Gensler left off – he had a great bill. I mean, I'm very happy with the rulemaking – was – the one last thing that was in there that got scourged out was having a cybersecurity professional on your board, not because it would have been a full-time employment act for the five of us up here...

(LAUGHTER)

... but – six of us up here – but I think that would have been helpful.

Erin, one more question, I think.

SAFRAN: Hi. Roselle Safran, the founder of KeyCaliber, a cybersecurity startup. So this question is, I guess, better directed to the – the government folks, to Director Coker and Director Easterly.

So we have a Department of Commerce, a Department of Agriculture, Department of Education, departments that cover all the big elements of our society, but we don't have a Department of Information Technology. Is there any thought of having something like that, which would encompass cybersecurity, would – which would encompass A.I. and everything else that goes along with that?

EASTERLY: Sure. I mean, I think Eric said it will at the outset – at the end of the day, our critical infrastructure is now underpinned by a technology foundation. Everything that we rely upon every day for water, healthcare, transportation, communication is a technology platform.

And so I don't think we can treat it as OK, we need a department to only help with the information technology areas. I think we have to be able to manage the cross-sector risk from both a technology perspective and a physical perspective across all critical infrastructure entities.

Now, of course we are the Sector Risk Management Agency for the Information Technology sector, and we work closely with them – and they of course include the cloud service providers, just to make you happy, Mark – but at the end of the day, I think, you – you know, IT is everything now, and that's why resilience as opposed to just security – and I totally agree with you. When I went to Morgan Stanley, I started out as the head of cybersecurity operations, and ultimately I ended as the head of resilience because it recognized that it's not just cyber. You have to be able to prepare for, respond to, and recover the full range of threats to any critical infrastructure entity.

MONTGOMERY: All right, I thank you very much. I have to wrap it here, but I do want to allow the two chairmen, if you want to – final words – only that this was a great report that ONCD sponsored and that two of you gave your time to lead. Any final thoughts?

VENABLES: Yeah, like, I would just, you know, again give a shoutout to not just the members of the working group and the wider PCAST but literally hundreds of people we spoke to over a year that were – you know, that were gracious in their time and they worked with us through the report. And I think, you know, we're just – very, very grateful to everybody, not just the people listed in the report. There were many more that we couldn't even list that there was lots of conversations with.

The final thing I will say is just what I said before, which is, you know, we tried to, you know, set a tone that we need to do more but also wanted to preserve this kind of optimistic note that we actually know how to do this, we've just got to do it.

And, you know, there's a lot of ambitious goals we need to do, but there's not necessarily new things we have to invent, we just have to drive this. And again, the future's already here, it's just unevenly distributed.

HORVITZ: And I'll just add to that by saying thank you again to everybody who provided us with, quite a few insights, and that includes Jen and your team. And I was hoping that we'd end on your comments because I thought there were – it's a perfect summary of where we need to go and where we are right now.

One goal that I've had in this report was to make sure it was impedance matched, to use a geeky term, with reality, so it – we didn't end up being impedance mismatched, sitting on a dusty shelf somewhere, but actually could start having effect and could amplify great work going on already right now.

And maybe some of it's here, but there is kind of a – several North Stars that have the gradients along with them that we can now –track and move forward into the future.

MONTGOMERY: Well, thank you very much for raising the discourse with impedance. I want to...

(LAUGHTER)

... I want to thank the team here at FDD, Erin Blumenthal and her team for putting this on. I want to thank the three commission members who are here for coming. And most importantly, I want to thank Director Coker and Director Easterly for your leadership of our national critical infrastructure.

(APPLAUSE)

END