Assessing America's 2023 Cyber Resiliency:
A Conversation with the CSC 2.0 Co-Chairs

Featuring Rep. Mike Gallagher (R-WI), Sen. Angus King (I-ME), Chris Inglis, and RADM (Ret.) Mark Montgomery
Moderated by Maggie Miller, cybersecurity reporter at Politico

RAVICH: Good morning, everyone. Thank you for coming to our event on Capitol Hill, hosted by the Foundation for the Defense of Democracies.

It is September 19, and today, we are joined by Representative Mike Gallagher and Senator Angus King, U.S. Cyberspace Solarium Commission cochairs, and the former national cyber director, Chris Inglis, to discuss the 2023 Annual Report on the Implementation of the Commission's Recommendations.

I'm Samantha Ravich, chair of FDD's Center on Cyber and Technology Innovation, and a former commissioner of the Cyberspace Solarium Commission. On behalf of FDD, we're happy to welcome you both in person and on livestream for this event, cohosted with CSC 2.0, which preserves the legacy and continues the work of the commission. We at FDD are honored to house CSC 2.0 in collaboration with my fellow commissioners of the Cyberspace Solarium Commission.

The commission's goal was, quote, "to develop a consensus on a strategic approach to defending the U.S. in cyberspace from significant cyber attacks." We met more than 50 times, often for two-hour sessions, and we analyzed, discussed and always in the most collegial fashions, argued about the main components of that goal: a strategic approach; defending cyberspace. What is a significant attack? And we reached a consensus on 116 distinct recommendations.

But recommendations are only truly effective once they become executive or legislative action, and today, I'm proud to say that we have seen significant progress on that front. While I implore you to read the assessment, I want to highlight some important figures.

Nearly 70 percent of our recommendations are either fully implemented or nearing implementation, with over 20 percent on track to implementation. This shows a steady increase from the 60 percent fully or nearing implementation from last year, and 35 percent from 2021.

Today, we have the privilege to be joined by the commission's co-chairs, Senator Angus King and Representative Mike Gallagher, former National Cyber Director Chris Inglis and Executive Director RADM (Ret) Mark Montgomery here to assess the recommendations' implementations progress. Before I hand it over to them, let me briefly introduce our panelists.

Our first panelist is Senator Angus King, who has been serving as Maine's independent United States Senator since 2013, before which he served two terms as Maine's governor. He currently serves on the Armed Services Committee, the Select Committee on Intelligence, the Committee on Energy and Natural Resources and the Committee on Veterans Affairs, giving him a depth of experience in strengthening America's national security to promote prosperity.

Angus, I recently heard you say that strategic posture is deterrence.

KING: That's right.

RAVICH: Your work on the commission was instrumental in creating that strategic posture which will help our country and its citizenry remain secure.

Our second panelist is Congressman Mike Gallagher, who has represented Wisconsin's Eighth District in the U.S. House of Representatives since 2017. Mike serves as the chairman of the House Armed Services Subcommittee on Cyber, Information Technologies and Innovation and as chairman of the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. Prior to his time in Congress, he was an active-duty United States Marine, learning the price of freedom at the granular level.

Mike, all of us who know you and all who are getting to know you through your work on Solarium, and now on China are watching in real time a leader emerge.

Our third panelist is Chris Inglis who, as many of you know, served as the inaugural national cyber director until February of this year. Chris taught at the U.S. Naval Academy and served as a fellow commissioner on the Cyberspace Solarium Commission. Prior to that, he was a career National Security Agency leader, rising to deputy director of NSA.

Our fourth panelist is Mark Montgomery, senior director of FDD's Center on Cyber and Technology Innovation and executive director of CSC 2.0. I got to know Mark as the unrelenting executive director of the Cyberspace Solarium Commission. Now I've had the pleasure of working with him at FDD as well.

Our discussion will be moderated by Maggie Miller, a cybersecurity reporter at Politico.

Thank you, Maggie, for guiding what will be an intriguing discussion.

One last thing before we dive in, a little 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 @FDD.

OK, that's enough from me. Maggie, over to you. Thank you.

(LAUGHTER)

(APPLAUSE)

MILLER: All right. Great, thank you, Samantha, for such a great introduction. And welcome to the panelists. Good morning, on this bright and early day.

So we're going to just jump right into it and start talking with the National Cybersecurity Strategy, which, since the publication of the annual assessment last year, has been put out, and the accompanying implementation plan.

So, Director Inglis, I'm going to get your response to this in a minute. But, first, Senator King, Congressman Gallagher, I want to hear from you.

You called the strategy "comprehensive," when it came out. How consistent was it with your vision on the Solarium?

And what's the impact you're seeing as a result of the strategy?

(CROSSTALK)

GALLAGHER: He said I'm senior. I don't know quite what he means by that (inaudible).

(LAUGHTER)

KING: OK. First — I think the first thing I want to say is this is something that often happens to a U.S. senator, which is to speak to a room full of people, all of whom know more about the subject than he does, but it doesn't hold you back.

(LAUGHTER)

So I'm going to make my comments, anyway.

No, I think the strategy was — was very thorough, and I'm glad you mentioned implementation. And I think we ought to recognize Kemba Walden for the work that she did in developing the implementation plan.

My experience in public policy is that implementation is as important as vision. You can have a great idea, a great plan; you can pass the bill, but it's the implementation that's really important. And — and I think that's why I'm so glad that the administration took both steps, not just to release the strategy.

So I like the strategy. My fellow members of the commission will not be surprised I still feel there needs to be greater emphasis on deterrence. Because we're just not going to be able to patch and defend our way out of this. I think our adversaries have to fear us. They have to fear that there will be consequences for a significant cyberattack on this country.

And I'm not sure we've got the clarity of declaratory policy that we ought to have in order to develop a policy of deterrence that will be effective.

So I'll leave it at that. I have some other thoughts. I do want to thank the staff. This is one of the most useful, clear reports that I've seen, and I love the way it's presented, with the color-coding. You can tell exactly what's working, what isn't working, where the gaps are, where we need to do further work. But a great piece of work. I attribute to Mark — Mike and I have often said that the smartest thing we did in the whole process was hire Mark Montgomery to be the director, who has done just a fantastic job.

So I'll leave it at that.

GALLAGHER: Well, I'll echo Senator King's comments, with one notable exception about our report on implementation, which is that the picture on the front has Angus nicely in the foreground, clear, whereas I'm obscured and blurred out in the background. I don't know what message Mark was try to send...

(LAUGHTER)

... with that one. It's as if I don't exist, I don't matter...

(LAUGHTER)

... which reflects the Senate's view of the House, I think.

(LAUGHTER)

No, I agree with all of that, and I should say my general view of the world is anything that has, like — that Chris Inglis had any sort of role in is usually a good thing, and it's usually smart, and I admire that product. And in addition to hiring Mark Montgomery, which was a great decision, we were lucky to have Chris Inglis as one of our commissioners, who then became the first national cyber director. And I don't think there's anyone else who could have taken on that role in its infancy. And I hope we have a fulsome discussion about the role itself and the future of the role. But Chris did a phenomenal job.

Now, I think, particularly as we think about implementation, it's up to us in Congress to continue to apply productive pressure to the executive branch. The document is one thing; the actual actions are another. There I say, in the House, at least, we do have a very good working group that's emerged.

One of the challenges we face is that jurisdiction over cyber issues is split between numerous committees. I have, sort of, the military component of it. Intel has a component of it. And then Homeland has a big component of it. And traditionally, these committees don't talk to each other; they don't work well together, but...

KING: If you look on page four of the report...

GALLAGHER: Probably another picture of Angus.

KING: No, no.

(LAUGHTER)

If you look on page four of the report, you'll see that the least implemented recommendation is to set up a special cyber committee in the Congress. We failed utterly at that because, just what Mike said, and I think — it, sort of, jumps out at you. There's a red bar right across that says "Congressional Select Committee on Cyber" didn't happen. And it is one of the real problems. I don't mean to interrupt, but...

GALLAGHER: No, please.

KING: It's — we — in order to get the first 40 or so provisions implemented in the Congress a couple of years ago, we had to get 180 clearances from committees, subcommittees, minority, majority. I mean, it was just crazy that the— and a tribute to all the work that went into getting that done. But that points out how difficult it is to make — to do this kind of policy in a situation where you have divided authority. And people are jealous of their authority. They don't want to give up at all. And, you know, this might compromise — so I — I'm sorry to jump in there.

GALLAGHER: No, I agree.

KING: But that was — that's one of the biggest failures of the work of the commission, and I'm afraid it's probably hopeless, because the committees just aren't going to abdicate their responsibility.

GALLAGHER: I'd just say that we — so, in light of that, we have a kind of a working group going on here in the House, with all the various committees that own a piece of the jurisdiction. And this was Chairman Green's vision and, you know, so it's not quite as good as having a cybersecurity committee, but it's working somewhat in the House of Representatives. And it's our job to ensure that there's implementation happening.

MILLER: And before I get to your reaction, Director Inglis, to the implementation plan, since you brought it up, Senator King and Congressman Gallagher, I know the report notes that there has been drafted legislation to create these cyber committees in the case of an emergency.

Do you ever — what would you envision that case being? You know, do you every think that there is a potential that Congress could turn around pretty quickly on this?

GALLAGHER: Well, I mean, traditionally, I mean, if you look at the creation of the House Permanent Select Committee on Intelligence, it took a crisis to create it, or a scandal.

KING: Right.

GALLAGHER: We're hoping to avoid that. I mean, our mantra throughout our two years of work was we wanted to be the 9/11 Commission without the 9/11. So we're hoping that we don't have, sort of a cyber 9/11 occur and that everyone says, "Oh, you know, we should have created a Select Committee on Cybersecurity in Congress."

So perhaps there will be something else that would spark the conversation. Because I have to — I have to admit I share Senator King's dire assessment of Congress, sort of, willingly organizing and creating a committee at this point.

I will say every period of productive congressional reform — and there's been very few in the past — has involved some reorganization and consolidation of committee authority, and I think we're at a moment now where we need such a reorganization and a re-look at how the basic committees are structured.

MILLER: And turning now to you, Director Inglis, I want to give you a chance, obviously, to respond to the lawmaker's comments on the implementation plan and the strategy. And also, now that you are outside of government, how do you think your old office is doing on the implementation of the strategy?

INGLIS: Well, I'll answer in reverse order. I think they're doing great, and I think that they're part of a much larger team that's been mobilized to actually address the needs the nation has in its dependence on cyber.

To first describe the implementation plan, you have to understand the strategy itself, and my favorite criticism of the strategy is that it was once described as everything, everywhere, all at once. Yes, it is wider than it is tall, because we have to mobilize all of the efforts, all of the capabilities, all the authorities, all the talents, to include private, public and multiple governments, and the strategy attempts to do that, and it does that in a coherent fashion where it hangs together.

As Senator King, Congressman Gallagher noted, it's really important then to have an implementation plan that instantiates that, that brings action to that — the spirit of what was called for in those various strategic principles, and the implementation plan, delivered in concert, in parallel with the strategy itself, delivered within three months, does just that: 65 actions across 18 agencies and departments. That's actually, again, wider than it is tall, and it's work underway.

There is a life force behind it in the form of the Office of the National Cyber Director that works hand-in-glove with the agencies and department, not least of which, the Office of Management and Budget, to make sure that we resource the things that we've committed to do. That's a very, very important relationship, and that life force, the Office of the National Cyber Director, reports both to the executive branch and to all the stakeholders in the executive branch and to the Congress. That's a very important join to sustain as we go forward.

So I'm very bullish on the role that the Office of the National Cyber Director can play from this day forward.

MILLER: And turning to you, Mark, want to get into a little bit of the nitty gritty of this third annual implementation — or assessment, I should say — report released today, which had looked at the progress on the 116 recommendations that the Solarium has put out around that since 2020. So how would you say that Congress and the Biden administration are doing on implementation of Solarium recommendations? And what were some of the biggest changes since last year?

MONTGOMERY: Well, I think that we've continued the kind of persistent, slow, you know, process. You know, the first year was getting about 30, 35 percent done. As Senator King used to say, you know, if you hit 350 playing for the Yankees, you'd make $30 million a year — probably $40 million a year now. So that was a good year.

But since then, each year, we got another 25 percent the next year, and then 10 percent this year. I expect that kind of slowing numbers, you know, that we can get five to 10 percent done a year over the next couple of years. So I think that kind of persistent process is good.

The big things over the last 12 months are the Cyber Diplomacy Act inside the National Defense Authorization bill last year, and the confirmation — very rapid confirmation, thanks to Senator King and Senator Menendez, of Nate Fick as the cyber ambassador; a very good appropriations bill, you know, that got CISA back up to about $2.6 billion and fully funded the Office of the National Cyber Director and gave some money to the— to SRMAs, Sector Risk Management Agencies — not all. That's been inconsistent.

And then I think the executive branch has really — has done some good things over the past year. Starting the zero-trust mark [U.S. Cyber Trust Mark] program, it's a — you know, it's consistent with our certification and labeling initiative.

The SEC [Securities and Exchange Commission] rulemaking, certainly the part that has to do with governance structures inside C-suite being responsible for cybersecurity, that gets at our Sarbanes-Oxley, and frankly, we were never going to be a — Sarbanes-Oxley was — all read like cyber committees because the chance of cracking open a bill that complex, it became too hard. So having the SEC Chairman Gensler attack it through rulemaking, I think, was the right way.

So, you know, overall, a number of good things. But, you know, we need to expect that this is about a 10 percent thing each year.

What I would say is our white paper recommendations are now where we're making the most headway on workforce, on supply chain. And then even some of the papers that CSC 2.0 is doing, I'm hoping we can make some progress on things like the water sector and the maritime transportation sector.

So there's room for growth next year. I think that growth, though is as much in the white papers and the follow-on CSC 2.0 papers as it is in the original 82 as we're getting near the end of those.

GALLAGHER: Can I interject something?

MILLER: Absolutely.

GALLAGHER: (Inaudible) I just have a question for Mark. Do any of these other commissions have, like, this implementation or 2.0 thing like we do?

MONTGOMERY: I think — so you and I did an event with Eric Schmidt, the artificial intelligent — the N.S. — National Security Commission on Artificial Intelligence. They don't do what we're doing.

GALLAGHER: Yeah.

MONTGOMERY: But I do think, you know, with a generous grant from Eric Schmidt, they've — you know, they've kept the team in place, and in fact, we work pretty closely with them. But I would say...

GALLAGHER: They were very helpful.

MONTGOMERY: Yeah, because their legislative — they didn't have four legislators on their commission. I think it's a little less of a — kind of an implementation plan and more tackling the broader issue of artificial intelligence.

But definitely, this is unique. I mean, you know, the — our famous — you know, we took briefs, and the most famous commission was really Simpson-Bowles. But that track, it would be zero for 19...

(LAUGHTER)

MONTGOMERY: And as a result, our debt is no longer $6 trillion; it's $33 trillion as of a few days ago.

So, you know, this is a unique commission in that regard. I think it started with having four congressional members as leaders. Jim Langevin is not here today. Ben Sasse isn't here. But, you know, we'd be remiss to not mention that Jim Langevin...

GALLAGHER: Yeah. (inaudible)

MONTGOMERY: ... put a lot of this legislation on his shoulders for two years — two and a half years, and really carried it home.

GALLAGHER: I'm sorry for that. There's all this interesting literature about, like, commissions. Do they work? Don't they work? How do you structure them? Is it just show? And so — I'm sorry.

MILLER: No, no worries. Actually, a quick follow-up, Mark: What sort of white papers should we be looking for from CSC 2.0 the rest of the year?

MONTGOMERY: So I think that we really need to take a look at the sectors that are weak. Like, we constantly say, you know, across the 16 critical infrastructure sectors, there's a winner like energy, and losers, 15 — I wouldn't say 15 others, but you know, even on a bell curve, there's a lot of Cs and Ds in there.

We've hit water. We've hit maritime transportation security. I think we'll hit healthcare, food and agriculture, aviation. And then there's an important one we're working on — whether or not we need a Cyber Force. I know that'll be well-received by all the commissioners as we bring that through, and you know, a couple others like that. But that's where we're headed right now.

MILLER: Well, we'll be watching closely on the Cyber Force issue in particular.

And actually, I want to turn to Senator King now. Something Mark just mentioned, the Cyber Diplomacy Act, was one of your top priorities a year ago. And while the Bureau of Cyberspace and Digital Policy had begun its work last year, you had said codification was important, and you were able to get that done in last year's NDAA. And since then also, as Mark mentioned, Nathaniel Fick has been confirmed as the ambassador. So what are your thoughts on how the bureau is doing so far? And also, they're currently working on an International Cyber Strategy. What all do you think should be addressed in there?

KING: Well first, I have to describe Nate Fick's confirmation hearing, because I introduced him and I sat in front of the at the witness table, and I looked up at the chair and said, "I want to introduce Nate Fick, who's nominated for this position and articulate his qualifications. He's from Maine."

(LAUGHTER)

And I folded my papers up and started to stand up and walk away. And it worked.

But no, having that position, I think, is more important than ever. There's an old saying: We wrought better than we thought, and I think we all realized there was an important international aspect to this question, but today it's even more clear than it was three or four years ago. And so having the position, having it codified so that it's not — I give the administration credit. They appointed him and started the process before the law was passed, but it was in a kind of — it had no long-term currency. It wasn't established in law. Having established it in law, I think, is very important, but also having somebody of Nate's capabilities in the office.

But the conclusion is this is an entirely international issue, and we can do everything right here, but if there are breaches in other countries, if there are weaknesses in other places and that's clearly a vulnerability. But also, we need to be working on setting international standards so that there's some clarity for countries around the world about what the rules of the game are. And that's where America was lacking prior to the establishment of this position. We weren't playing in the multitude of conferences and meetings and exchanges with other countries, and now we're clearly in that position, and Nate is a guy that can really, I think can make a significant contribution. So that's one that I'm really feeling good about.

I — and you mentioned the National Defense Authorization Act. Congress is like a train station, and there are very few trains that go through. But when a train is going through, you better put everything on it that you possibly can. So that's why we created the position of a national cyber director in the National Defense Authorization Act, because that was the train that was going through the station, and we were pretty sure it was going to get to its destination. So I'm very pleased. I think that was a big win last year.

MILLER: And do you have any thoughts on this upcoming International Cyber Strategy that I know they're working on? And if anyone else on the panel has thoughts on that as well.

KING: I'll let — Chris, why don't you — Chris?

INGLIS: Yeah, let me just while I'm thinking about those thoughts, just say first, a complement to Nate. There are some people that you meet that are great at the podium and less so, perhaps, close in as they compete for a kind of oxygen and space in the room.

Nate is just the opposite. He is terrific at both of those. He's very collaborative; sees the diplomacy with — within cyberspace as an instrument of power, not the principal instrument of power, and therefore, collaborates extremely well across the other instruments of power, not least of which in the private sector.

And I think to Senator King's point, this is a truly international issue. If you're an individual making use of services in cyberspace, you're reaching across national boundaries. If you're a company doing business in cyberspace, you work across national boundaries. You hope that the people who are actually directing policy and diplomacy think in those same terms. Nate does. The State Department does. He's a godsend.

GALLAGHER: I agree. Someone once remarked of Nate Fick that he's — he has the distinction of being better-looking than the guy who played him on TV.

(LAUGHTER)

It's true. A great Marine. So Nate's been fantastic. I — you know what? A sort of — a sort of thought. We had, remarkably, with Nate, Chris, with Jen Easterly who was, you know, did some red-teaming for us on the Solarium Commission. All these incredibly talented and collaborative people which, you know, it's obviously very rare in government.

And just to sort of, you know, provide the support necessary to those talented players, iterate based on some experiences we had with the creation of the national cyber director, I think we'd be in a very good position.

So it's incumbent upon Congress to make sure that folks like Nate, you know, future national cyber directors and Jen Easterly have the resources and support they need in order to advance the objectives that we all agree upon.

MONTGOMERY: So on the International Cyber Strategy, I I'd be excited if they have it done by December like Congress asked. I think it'll probably be late.

GALLAGHER: Yeah.

MONTGOMERY: But I'm — I am excited to see it really emphasize building partner capacity-building. The CSC did a paper on this a few months ago, and you know, it's our strong belief that we need to get, particularly the nonmilitary aspects of cyber capacity-building of our international partners organized, make sure that we've examined it, removed any redundancies, but also addressed any gaps, and then give it — give State Department the funding line they need to lead this, and then make sure we're helping them. And we should definitely prioritize those countries whose national critical infrastructure is critical to our military and our economic security. In other words, the countries through which we may have to move through and over our U.S. forces and the countries upon whom we're really dependent for supply chain parts during a crisis or a contingency.

GALLAGHER: Yeah.

MONTGOMERY: And then, you know, get those out there and build the cyber resilience of those partners.

GALLAGHER: Can I just make a quick point on that. Like, if you're considering the most stressing national security scenario, let's say a Chinese invasion of Taiwan, my view is that the only short war for Taiwan would be a quick Chinese victory, and therefore, you have to assume that we are going to need to surge men and materiel forward to the Indo-Pacific theater, which is not an easy thing to do in any circumstance, but that surging would be contested in cyberspace, and our airports of debarkation, our seaports of debarkation are incredibly vulnerable to cyberattacks. Some of that's on domestic U.S. soil, but some's just in our own neighborhood in places that we've neglected.

And putting on my hat as chairman of the Select Committee on China, to see the amount of investment — diplomatic, economic, military — that China is putting in our own hemisphere is incredibly troubling, and it's just something we've neglected for far too long.

Sorry if that was a tangent.

MILLER: No, actually, that tees us up perfectly for the next question, Congressman, which we're going to stay with you. Of course, you are also the chair of the House Armed Services Cyber Subcommittee, in charge of the cyber elements in the House of the NDAA. It's approved on a bipartisan basis; dozens of provisions to strengthen U.S. and partners' cyber resilience. And so looking at that from that position, and also from your position, as you mentioned, as chair of the Select Committee on China, how are you hoping that the NDAA will shake out once it gets through conference on cyber issues? And —how are you using both of those leadership positions to push forward provisions on cyber?

GALLAGHER: Well, if you look at — our first report was called "Ten For Taiwan", which is focused on things we could do in the 118th Congress to enhance near-term deterrence across the Taiwan Strait. Of our 10 recommendations, seven, I think at last count, got into NDAA. I should recognize the great work of James Mismash over there, my MLA and defense guru, with an assist from Bridget, of course, my Marine fellow. By the way, a former Gallagher fellow, Ali King in the back there.

So just remember, you may escape the office, but you'll always work for me still, as Mark has found out.

KING: We call it "staff for life".

GALLAGHER: Yeah, it's — exactly.

(LAUGHTER)

Probably the most important one for this discussion of the seven in NDAA is a provision to turbocharge our cyber collaboration with Taiwan, building off some of the best practices we've learned in other parts of the world, and having a conversation with them about how they can improve the resiliency of their grid, their critical infrastructure. One comment that the now-vice president and likely future president made to me when I was in Taiwan that stuck with me as we had this conversation about, how do we turn Taiwan into a porcupine, is that OK, you can't swallow a porcupine, but you can starve it.

And I left my last visit to Taiwan thinking that we need to be — we, i.e. those of us who come at this with a military — conventional military lens, need to be paying far more attention to a different scenario, a blockade scenario or a scenario in which China tries to weaponize or a scenario in which they expand the cyber war that I would suggest has already begun for Taiwan. So that's the provision I'm most closely tracking.

Another thing that I think is going to be important is a report we have evaluating the need for or the precise nature of a Cyber Force — we're going to have that debate in the CITI Subcommittee — as well as a report on the — how can we can improve occupational resiliency in the Cyber Mission Force.

And that brings to mind a related issue that we've — sort of haven't legislated in the NDAA but it's conversations that we've had with the Pentagon — it's are we making the best use of things like Cyber Excepted Service, are we making use of the creative authorities we've given to the Pentagon so they can hire some of the best and the brightest from the private sector who wouldn't traditionally be interested in a job in the five-sided building? So that's what comes to mind right now, but I know Chris has something.

MILLER: Yeah, of course. Director?

INGLIS: I was just going to add to that that I think we can take some lessons from our Ukrainian experience. The Ukrainians have acquitted themselves quite well, not just on the physical battlefield but in cyberspace, against what most of us would have said were very long odds.

And in cyberspace, I think what they've shown is technology matters but expertise matters more and coalitions matter still more, that coalition that they've built matters most of all, where the Russians now find themselves having to beat more of us, if not all of us, to beat the one thing that they want to beat. That's a lesson for us, in terms of our materiel disadvantages as we attempt to defend something that's kind of on the backside of the planet, expertise and coalitions will matter more, right, than that physical reality or the technology that's in play.

MONTGOMERY: If I could add a few — I think this year's NDAA's another thick, good cybersecurity-laced NDAA. Both the House and Senate versions, they have a total of about 47, 48 in there. There's 25 provisions that we're tracking having a tie back to our initial reports.

I mean, some of the most important ones come from the Senate are a nuclear command-and-control, continuing to make sure that our NC3 system has the proper cybersecurity. Senator King was emphasizing that repeatedly the last few years as an important part of our strategic deterrence, is actually having a secure system for controlling our nuclear weapons.

Another one, there's a Continuity of the Economy pilot program in the Senate version that I think will be critical for moving that along, you know, studying how secure are we once we leave the bases? You know, can we transition our supplies, our equipment, our personnel from the bases to the aviation points of departure and sea points of departure that Representative Gallagher mentioned?

And a final one I'd mention is there's a lot there on Cyber Command readiness. You know, how do we get the metrics right? We are always interested in metrics. And I was glad to see both the House and Senate versions — those staffers are continuing to push the issues into the NDAA.

MILLER: And Senator King, do you have thoughts on the Senate side on the NDAA?

KING: Well, I want to change the subject slightly. And we talked about Continuity of the Economy. I'm still worried about the private sector in not only in a security sense of the compromise of a smaller facility that is a sub to a larger defense contractor, and they get in in that way.

There can't be any holes in this system supply chain, but I'm also — I just —I don't know whether — I don't know quite how to say this but I'm worried that, in many places in the private sector, they're just still not taking this as seriously as they should be.

And I don't know what it's going to take because smaller — a lot of smaller entities are grappling with these ransomware attacks and those kinds of things, but I think the energy sector is taking it very seriously, probably the best of any of the private sector entities.

The healthcare sector, I'm very worried about. Water — there are 70,000 water systems in America. Now, that's good news in a sense that it means you can't compromise them all at once. It's bad news in the sense that very few of them have the capability to have a serious cyber protection, you know, they don't have a — they don't have a person on staff. They're four or five people that run the system.

So I just think there's a —still an enormous amount of vulnerability out there in the private sector and I don't — you know, we just keep talking about it but I'm glad that the SEC took the step that they did. I think corporate executives are going to have to view this as a — just as if they view financial risks and weather risks and those kinds of things. This has to be, I believe, one of the highest priorities.

And in a case of a major cyber conflict, there's going to be no distinction between private and government. I mean, it's all — we're all in it one way or the other, and a compromise at a major industry is going to compromise the country.

So I just — I want to get that in. I think that's where there's still plenty of work to be done.

MILLER: And to quickly follow up with you, Senator King, I know Congressman Gallagher mentioned Cyber Force and the support to Taiwan. Do you think those are both issues that the Senate can agree on and that will get through conference on your side?

KING: Yes.

MILLER: OK.

KING: How's that for the shortest answer you've ever heard from a Senator?

(LAUGHTER)

MILLER: That's great.

GALLAGHER: We're probably both conferees. I don't know, so.

KING: Yeah.

GALLAGHER: We'll jam it through.

(CROSSTALK)

KING: With our immense power.

GALLAGHER: Yeah, that's right.

MILLER: On cyber, you're the leaders.

And I want to turn to you, Director Inglis. The commission focused on operationalizing public-private collaboration, of course that's a big focus of the Defense Department's Cyber Strategy they just released. And in your time in office and since, what do you think have been some of the big gains, what are the remaining hurdles in this space?

And then after Director Inglis, very quickly perhaps Congressman Gallagher, Senator King, you can comment on views from Capitol Hill on whether Sector Risk Management Agencies and others are making the right investments to advance this public-private collaboration?

But we'll start with you, Director Inglis.

INGLIS: Yeah, it's a great question. I think that the Solarium Commission took care to use the word "collaboration" as opposed to "division of effort" or perhaps just kind of same way, same day terms, because collaboration is materially different than what we've been doing.

You know, for a very long time, various parties in this space, cyberspace, have been defending in their own silos as if they could defend their patch with the limited expertise, limited insights, limited powers, authorities that they might have.

That's simply not true. We're not trying to solve the same — or a similar problem in those various stovepipes, we're trying to solve this same problem that ruthlessly cuts across those stovepipes. So first and foremost, I think we finally understand what collaboration is — combining our resources so that we can observe, understand, discover things together that no one of us could discover alone, and then together, solve those.

To that extent, things like the JCDC, the Joint Cyber Defense Collaborative, which is built on a Cyberspace Solarium provision, essentially is a place where it's not policy experts that show up, it's subject matter experts that show up so that they can compare their shards, their shreds, their hunches in cyberspace to say "does the half of the thing that I'm looking at line up with the half of the thing you're looking at, so that we might then together discover something and do something that no one of us could have done alone." I think that's the material advance that we've made, and that exists in the Sector Risk Management Agencies as well.

The Department of Defense is doing that. It's something they call the Cyber Collaboration Center. The Department of Energy proposes to do that in something called the Energy Threat Analysis Center. This can work broadly across the system, and there can be something that then synthesizes, pulls all that together so that we benefit collectively from what we discover in the collaboration across that broad front.

MILLER: And, Congressman Gallagher, Senator King, thoughts on sector risk management agencies, very quickly?

GALLAGHER: Well, I think it's fair to say — I mean, there's been inconsistency across the sector risk management agencies. My understanding — I mean, CISA's, what, the sector risk management agency for eight out of the 16 critical sectors?

But each of them have different needs. So even, I think it's fair — even CISA's performance has been inconsistent across the different sectors.

So that's an area where I think we have more work that needs to be done. I guess, given CISA's outsized role, it gets to something we tried to do in our initial report, which is to elevate and empower CISA. I mean, that was one of the bigger themes that came out of our initial report was how do you make CISA sexy, for lack of a better term. And I think Easterly's done a great job, but I think there's more work that needs to be done on elevating and empowering CISA going forward.

KING: I think one of the failures that we've had is the — our — we haven't gotten the Joint Collaborative Environment established, which is something that we've been working on, and we get close and it doesn't quite happen in the Congress. CISA has developed — is working in that direction, anyway. I do — I think — we're talking all about policy here, but we ought to be also talking about people. We talked about Chris's role in getting — establishing the national cyber director. Jen Easterly — Chris Krebs before and Jen Easterly at CISA, I think, has done an extraordinary job.

I want to thank and compliment Anne Neuberger at the National Security Council for the work on the labeling initiative, which is also one of our recommendations. And they had a very thoughtful process and have come out with — basically, it's a labeling system for consumer electronics. I mean, now we've got, you know, the Internet of Things. And we need to talk about the cybersecurity of your router or probably even your microwave or your car, and so that we move toward a voluntary labeling situation, like UL on electronic devices, I think is big progress.

So I want to thank those individuals and of course Chris for establishing the office and Kemba for continuing his work.

But you can't separate policy from people, and we've had some really good people that have been involved in these issues. But again, I think the joint collaborative environment is something that has been — is lacking. We've got to build a situation where the private sector and the government can work together harmoniously, seamlessly, in real time. And that doesn't come naturally to either of those entities.

You know, it just — it has to be — I think we have to set up a structure before the crisis so that trust is established which can then lead to positive outcomes during some kind of crisis or confrontation. It doesn't work — I used to say to my friends at the Maine legislature, "The relationship has to come before the ask." And I think setting up a structure that will enable a kind of ongoing communication between private-sector entities and CISA or whatever agency is involved, whether it's a sector risk management agency, you've got to do that first, rather than when the world is falling down around you.

So that's, I think, something that I'm hoping we're going to be able to continue to pursue actively.

MILLER: Yeah, Director?

INGLIS: So, Maggie, I know you want to go to questions from the audience, but can I just follow on that to say that I couldn't agree more that form will follow function and the mechanisms will follow the life forces. And you can see no better example of that than what you saw in Solarium, where Republicans and Democrats combined their efforts to come up with something that was a consensus report.

The only tension I recall in that room across those two years was when the Green Bay Packers got into the finals, and it was suddenly, kind of, apparent that not everybody was a fan of the Green Bay Packers.

(LAUGHTER)

I don't know who it might be, but...

(LAUGHTER)

... but all the same.

GALLAGHER: Those people were summarily dismissed.

(LAUGHTER)

INGLIS: But I think that having, kind of, put down ideology and put the nation's, kind of, you know, fortunes first, in the Solarium Commission and then what then follows, we will figure out how to get the mechanisms and the structure and the JCE, the collaborative environment, which is really a response to how do we actually equip that life force, how do we actually sustain that life force? I think we'll get that right.

MILLER: And I could — I literally have a list of questions that I could sit here and ask all four of you all day, but that would be rather selfish. So we are going to...

(CROSSTALK)

GALLAGHER: Mark's gotten off easy.

(LAUGHTER)

I think Mark needs a hard question.

MILLER: I think he has.

So we're going to turn to...

GALLAGHER: Give Mark a hard question.

(LAUGHTER)

MILLER: Well, if anyone in the audience has a question for Mark that's more difficult, we're going to turn to an audience Q&A, take a few questions, for the next few minutes.

So if anyone has a question?

Absolutely, here in the — yes?

RITCHIE FRIERSON: Thank you. My name is Kelsey Ritchie Frierson. I'm a technology fellow in Senator Thune's office with a background in A.I. and cyber. So really appreciative of the event today and of the report.

My question, kind of, combines the A.I. and cyber piece of this. I know you mentioned the NSCAI. How does, kind of, emerging technology, especially, kind of, in this boom of A.I., impact the way that you're thinking about, kind of, the implementation of the cyber strategy?

And how does it change the way that we need to be thinking about the cyber domain in general?

GALLAGHER: Well, first of all, Senator Thune, a Packers fan, let the record show. True story.

(LAUGHTER)

MONTGOMERY: I'll take a first whack and just say one of the things that A.I. is doing is forcing even more — you know, we noticed — we were pretty dumbstruck by the slow process of updating documents, of getting regulation — getting provisions and legislation right in cybersecurity. Now you add in artificial intelligence, and you're going to need a lot more agility than we're used to in both the executive and legislative branches.

And you're going to actually have to — one of the things we've avoided — Chris said it gently, I think — is that, you know, we've had 23 years of following a pretty poor, you know, voluntary partnership program, and we've allowed that to persist. I think artificial intelligence is going to remove our ability to be slow, and it's going to require agility, and it's going to remove our ability to not make sharp decisions.

I mean, we really do have to make decisions, and we really do have to do it in a speedy way. And I think — you know, I'm not saying it's going to help us in that regard; it's going to force us in that regard. So that's one area. And I do think artificial intelligence — you know, when people say, "Is it good or bad for cybersecurity?" My answer is both. You know, it's just one of these things that we're going to have to take advantage of the opportunities and manage the risk. But we're going to have to do it in a much more rapid fashion.

INGLIS: I'd just add two things to that. I agree, I would just say that, from the dawn of the Internet, there were, kind of, two driving factors that essentially characterized the technology — innovation and market efficiency. For too long, safety has not been that, kind of, third leg under the stool. We need to make sure that safety, or reliability — pick your term — but we need to make sure that's the third leg under the stool. That needs to be a cultural norm, and it needs to be an expectation when you develop and deploy technology. That's the game.

Two, this technology is moving so fast that we can't actually get our arms around, stop, kind of, you know, focus on a given technology. We need to prepare the human being to actually be resilient and robust, kind of, in the face of that technology.

For those of you as old as me, you might remember a Bose speaker commercial where this person's sitting in front and the speaker is blowing their hair, kind of, to the far quarter. That's where we are in terms of technology. What's next is quantum computing. What's next is, kind of, gene splicing at home — I'm just making that up. But the technology is moving so fast we have to make sure that we double down on actually the resilience of the human being and place them at the center of the frame.

KING: I want to touch on that because — and broaden the discussion. We're in a — we're in a competition with China particularly but also with Russia and with other regimes around the world about whose system is better, democracy or some kind of authoritarianism?

And Xi Jinping believes, and has discussed this explicitly, that democracy can't work in the 21st century because of the speed of decision-making that's necessary. And so we have to be responsive to that, we have to show that our system can work and be responsive and not take years and years and years and years because the reality of our current life, both in technology and generally, is speed.

And speed is not a — is not a word that you generally use in applicability to the U.S. Congress. Our system was designed to be cumbersome and slow, and the framers exceeded — succeeded beyond their wildest imaginations.

And — but we have to be thinking about that, not to trample the checks and balances and all those things, but I really think we need to understand that there's an underlying competition going on in the world today between visions of how you govern.

And we have, I think, the best system but we have to realize that speed and agility, which aren't qualities normally associated with our governmental system, are values and imperatives as we move into an age of accelerating change. That's my sort of constitutional speech this morning.

GALLAGHER: I'll just quickly say — and by the way, we're wearing our — we got the Constitution tie, I've got the Declaration of Independence tie, that's part of our uniform that Angus and I wear together. The — if you read our initial report, you see the tension between the demands of speed and perhaps — let's say the demands of safety, right? It — or the desire to incentivize or force the private sector to step up and prioritize cybersecurity while not saddling them with counter-productive, onerous regulations from the federal government.

That was really a tension that persisted throughout our work and it's sort of a tension that's impossible to resolve perfectly. I think that tension is even greater as Congress turns to this question of how to deal with A.I., right? How — because we can't pause — we just can't pause for six months because that hands a victory to the Chinese Communist Party.

And the only thing I know is that if they command the heights of A.I. technology, they will use this technology for evil purposes. So we have to simultaneously keep innovating within the free world while also trying to slow them down.

There's some obvious steps there, in my opinion. We have massive loopholes in our export controls related to advanced semiconductors that are necessary for A.I. that should be shored up. We should not allow private investors in America to invest in Chinese A.I. companies — I'm speaking just for Mike Gallagher, not for the Solarium Commission.

And then on the positive front, I do think DOD's ethical sort of framework for the use of A.I. is pretty good, and it's a framework we could build upon and expand across the federal government. And then if we were really smart, we would start to build out in the concentric circles that are our alliances and get our allies on the same page with us, in terms of striking that balance, starting with AUKUS, expanding it to Five Eyes, and then to certain NATO countries or technologically advanced countries.

(CROSSTALK)

MONTGOMERY: ... go ahead, Chris, and then I'll go.

INGLIS: I think the really good thing about what Congressman Gallagher right — just said about that tension in American society is that it's always been a feature, right? We don't have the word "or" in the preamble of the Constitution. We intend to do all of these things.

That sometimes means we have to work harder to deliver those, but we can deliver innovation, market efficiency, and safety. We've done that in other systems of interest. We just have to make sure that, to Senator King's point, that agility is one of those things that actually is a common property across those three dimensions.

MONTGOMERY: You know, I think as we address artificial intelligence, there's two things that we looked at in the commission that have not gotten done, that have to get done. The first is understanding how we secure data properly so that it can't be misused in artificial intelligence gathering. And the second is the security of our cloud service providers. That's — that — to me, that's critical.

You know, one of the big, obvious flaws in Presidential Policy Directive 21 is it doesn't — it doesn't designate cloud — it — they didn't exist at the time. The big flaw is it's 10 and a half years old and it doesn't recognize there are cloud service providers.

The cloud service providers are — at least the cloud computing industry needs to be a critical infrastructure, it needs to have a Sector Risk Management Agency, and we need to figure out some baseline standard for cybersecurity in there or we're really going to be exploited heavily by artificial intelligence.

So those two things need to happen, securing data and securing the cloud.

MILLER: Any other questions? Yes?

VASQUEZ: Hi. My name is Christian — I'm Christian Vasquez, I'm a reporter from CyberScoop. Thank you for doing this. I have two questions. I — so...

KING: We're having trouble hearing you.

VASQUEZ: Oh, OK — yeah. So on SRMA, I'm thinking about funding and resources. Which areas or which agencies are you most concerned about? I mean, there's been — historically, TSA, EPA haven't had much funding. TSA after Colonial, you know, was like a skeleton crew I think. One report had EPA similar kind of thing was going on. I'm kind of curious which agencies don't you think currently have enough? What is enough? And where does CISA fit in?

And on new tech, where are the, you know, regulations for distributed energy resources, which is going to be a huge thing in energy supply — space, like you just mentioned, cloud service providers? I'm just kind of curious, as we're kind of going through these rapid, you know, accelerations in these different areas of tech, where does regulation fit in?

Thank you.

GALLAGHER: The first question was, like, human resources, which agencies don't have enough?

(CROSSTALK)

MILLER: Which — yes, which SRMAs don't have enough resources? How can we increase that? Yeah.

KING: The two agencies that I'm most worried about are HHS and EPA. HHS because of its relationship — and CMS, the healthcare sector generally, and then EPA water sector, as I mentioned. Those are two areas that I think are particularly vulnerable and that they need more resources and more focus, frankly.

MONTGOMERY: And if you want bad news in threes, I agree totally with those two. And I'll throw in food and agriculture, which is the Department of — the Department of Agriculture needs — is going to need a lot more investment as an SRMA.

I think those three — and those are kind of our health — you know, those are your health and public safety, your — you know, your, you know, key — along with energy, key to — you know, to survive — personal survivability.

So we really need to tackle all three of those.

GALLAGHER: I just had a hospital shut down in my district because of a cyber issue. I mean, it's just offline for — I mean — it's catastrophic consequences at the local level.

Go ahead, sorry?

INGLIS: No, I think your second question was about regulation writ large. You know, that's the word "Voldemort" in the room finally. So I think the new and novel part of the strategy, the National Cybersecurity Strategy, was it introduced the prospect of regulation.

I think that that's been something that we have used in other kind of systems of interest, whether that's transportation systems, drug, therapeutics, and it's time that we actually consider the possibility that there's — there are things that are so important, in terms of our dependence on cyberspace for health and critical and life safety issues, that we need to, on occasion, specify that.

However, it needs to work the way — this way. You know, we need to make sure that market forces have had their full opportunity to kind of play through and deliver the goods, and when they fall short and we need to actually extend what market forces have done, we do so, but we do it with the lightest possible touch and no lighter and we harmonize the result so all of the would-be regulators are not actually kind of smothering the baby in its crib with blanket after blanket after blanket. That's hard to do, but we've done it before, and we must do it again.

MILLER: Yes, another question over here?

SAKELLARIADIS: Yeah. Hi. I'm John Sakellariadis at Politico, so a little bit of an inside job, I'm sorry. I wanted to ask the middle three panelists whether you've been in conversation with Harry Coker about his pending confirmation process, and then what your hopes, and perhaps concerns might be, in particular on the timeline of his confirmation.

(CROSSTALK)

KING: Mike and I are meeting with him this afternoon.

GALLAGHER: Yeah. I — I'm not in the confirmation business, so I'm taking a pass on that, as to that — the question, but very much looking forward to the process.

KING: I would never take a job that requires confirmation.

(LAUGHTER)

KING: Although I guess I have to do that every six years.

MONTGOMERY: That's validation.

GALLAGHER: Yeah. Yeah.

MILLER: And I'm going to quickly follow up and say, you know, Senator King, what do you think in terms of pace for getting him through the Senate, his nomination?

KING: Who knows?

GALLAGHER: Yeah. What was the Inglis standard?

KING: As long as he's not — doesn't — as the title doesn't involve general, we may be able to do it.

No, I we are moving some nominations. The budget bill is in a — in limbo right now, so I just absolutely can't give you a time. I'm sorry.

MILLER: That's OK. Any other questions? Yes?

CONFRANCESCO: Hello. I'm John Cofrancesco. I'm the founder of the Applied AI Company. I'm curious to what provisions have been made and should we be making in light of a cyber 9/11. I think it's pretty likely that we're going to have something kick off in Taiwan. The majority of our critical infrastructure, it remains unprotected. for example, if you were to turn off a couple substations, we don't have supply in this country to replace the components in those facilities, so you'll leave large measures of the country without power for months.

GALLAGHER: Let me just — quick on that with — so taking off the Solarium hat, putting on China Committee hat, we just we were just in New York, and we did a wargame with, you know, major asset managers and financial executives to examine sort of the non-kinetic aspects of a Taiwan scenario, and the results were troubling. We — this is a 2028 scenario, but then we popped in the DeLorean and we went back in time to 2023 to see, what choices can we make now to expand the range of options a president would have, non-kinetic options, in 2028 to defuse the crisis?

To me, it hammered home the point that at least in key areas, we are going to have to strategically or selectively decouple, otherwise you're going to find yourself allowing the CCP to weaponize key supply chains or, to your point, sort of attacking various vulnerabilities we have. And I do think energy policy is a big part of this. Improving the resiliency of our grid here domestically is a key priority.

And you assume — final point I'll make — sorry to go on. You assume there are people in Treasury and Commerce that are doing this, right, that are going through the financial and economic escalation in the way we sort of rigorously do that and have a well-thought-out, multi-decade theory of the case on the conventional and strategic — certainly, on the strategic side, but it's not happening unless you've been part of something that I'm unaware of.

And they need to be doing it with the military people. We need to have that, you know, our theory of the case in place prior to the crisis happening so we're not making it up on the fly.

KING: And to your point, we should be learning from Ukraine. The Russian attack on the Ukrainian electrical system has been substations. That's what they're — that's what they're — and transformers. That's what they're taking out, and they're hard to replace and there's a shortage of them, and we couldn't replace them in this country if there were — and we've learned in some cases that you can take them out with a rifle with a scope sight.

So this is a — again, a serious vulnerability. As I said before, I think the energy sector's ahead of it, but in this case, it's sort of a combination of cyber and physical risk, and you know, the system, you know, is just — very vulnerable. Bridges, fiber lines — all of those things, we need to be...

I remember after September 11th, I assigned the State Police in Maine to assess where the risks were, and I think it's time to keep doing that. If you were a terrorist, where would you go? If you were an adversary on a cyber mission, where would you attack?

And that's why I'm a big believer in red teaming. We should be red teaming the whole country on these issues.

MONTGOMERY: Yeah, so two — we had two thoughts on this in the commission. One was that we needed to have a fund for recovery, a national cybersecurity recovery fund. That one we got through in the Bipartisan Infrastructure Act, a lot of it, and there was money put aside against it, appropriated against it.

But we also recommended a national critical infrastructure resilience fund to identify — you know, and a process to identify single points of failure ahead of time. Electrical power grids was a big area here. Some industries — and the electrical power is one that does do some investment in buying excess capacity, transformers and things, but not enough.

But many other areas have nothing. And you can think back to position, navigation and timing, where we actually gave up our backup system. The DOD said they didn't need it anymore. We retired it. And the rest of critical infrastructure was like, "Hey that was our backup, and it's gone."

So we absolutely have to do that preventative mitigation work, and then do some investments. The government's going to have to help pay for some of that procurement, which is not going to go over well with everybody. But that's got — you've got to have that beforehand. And we do have the recovery fund for after. So we're about 50 percent of the way there, but that's not good enough.

INGLIS: I'd just add to all that, agree, but all of those are appropriate responses to a cyber 9/11 that is already happening. It's happening as we speak. It's just diffused in time and space. We haven't seen it for what it is. There's too much proactive ambivalence — fancy term that says there a whole lot of folks that say "There's smoke in the room, but I hope to God somebody puts that fire out," not realizing they're a part of the solution.

All of us need to mobilize our time, our talent, our authorities, individuals; organizations; sectors, plural; governments, plural.

And I think there are three things that are particularly frail at the moment. We're addressing these. But the three things are the materiel, the hardware, the software, the systems; the collaboration that essentially is what delivers those in useful form, critical functions. So we need to make it such that we have coalitions that collaborate in the defense of those systems the way the Ukrainians have shown us that you can, in confidence. That's the third thing that's particularly frail.

Think back to the Colonial pipeline event, when there was plenty of petroleum in those pipelines up and down the Eastern Seaboard, with people believing that cyber held that at risk in some absolute way, panicked and essentially then rushed the gates in a way that we could not, at that moment in time, properly allocate those supplies so that we could just weather that storm. We need to get to a place where we're confident that we can weather the storm. Because we've got robustness built in. We're actually on the front balls of our feet defending that space. We do that collaboratively, they're going to have to beat all of us to beat any one of us. We need to get to that place.

MILLER: And as we begin to wrap up, I'm going to ask you to give a very quick, rapid-fire — start at the end of the line with Mark — response. As we start a new year, what is the one outstanding recommendation you want to move forward? And, yeah, try to keep it under 10 seconds. We're running out of time.

Mark?

MONTGOMERY: So mine's going to be get PPD 21 rewritten...

MILLER: Um-hmm.

MONTGOMERY: ... and, you know — and in a mature way that adds critical infrastructure such as cloud computing and space support infrastructure. And I will make sure, for next year's front piece, instead of blurring Representative Gallagher, we'll give him the Trotsky treatment and just wipe him out of the photo.

(LAUGHTER)

MILLER: Senator King?

GALLAGHER: Fair enough.

KING: Joint collaborative environment.

MILLER: OK.

GALLAGHER: We got a response on Continuity of the Economy from the administration that was a joke. So turning it into something real that's not a joke, I think, is a priority.

Was that — sorry, was that too harsh?

MONTGOMERY: No, fair.

(LAUGHTER)

INGLIS: What gets measured gets done. So I'd continue with the implementation plan. It's broad-based. It's wider than it is tall. Let's just continue apace.

MILLER: Well, with that, I want to thank all four of you for your continued leadership on cybersecurity and for being here today. We'll be watching this space closely and using the Solarium's recommendations as benchmarks to judge if our country is moving in the right direction on national cyber resilience.

And with that, I want to thank all of you in the room and those of us watching on livestream for joining us for this conversation. Thank you so much, and take care.

KING: Could I add one thing?

MILLER: Oh.

(LAUGHTER)

KING: There is so much expertise in this room. If you have ideas or thoughts of things that we could work on, let us know. Let Mark know. It's ...

(CROSSTALK)

MONTGOMERY: ... CyberSolarium.org.

KING: And we're still at it. So let's — share what your thoughts are, reactions, things that we're missing, please. We need your help.

GALLAGHER: And I'll give you Senator King's personal number, if you want to call...

KING: Yeah.

(LAUGHTER)

GALLAGHER: ... any hour of the day...

(LAUGHTER)

MILLER: Thank you.