America's Cyber Resiliency in 2024:
A Conversation with CSC 2.0 Co-Chair Sen. Angus King

September 19, 2024
Featuring Sen. Angus King (I-ME), Tom Fanning, and RADM (Ret.) Mark Montgomery
Moderated by Sam Sabin
Introductory remarks by Jiwon Ma

MA: Good morning, everyone. Welcome, and thank you for joining us for today's event hosted by the Foundation for Defense of Democracies. It's Thursday, September 19th, and today's panel will discuss the Cyberspace Solarium Commission 2.0's 2024 Annual Assessment Report. I'm Jiwon Ma, senior policy analyst at FDD's Center on Cyber and Technology Innovation and the lead author of the report that we'll be discussing today. We're pleased to have you here on Capitol Hill, some in person, some tuning in live and some listening to our podcast for this conversation.

As cyber threats against America's critical infrastructure continue to evolve, so must our defenses. Four years ago, the congressionally mandated Cyber- – Cyberspace Solarium Commission offered a new strategic approach to combat these threats and defend U.S. national security and economic interests in cyberspace with what we call a layered cyber deterrence.

Accompanying this new strategy, the commission issued 82 recommendations in its flagship report and followed up with a series of white paper recommendations. The implementation of these recommendations makes our nation more secure, and we believe will get us to effective deterrence in cyberspace.

This year's report shows that about 80 percent of these recommendations have been implemented or are nearing implementation, with another 14 percent making steady progress. It's evident that we're seeing measurable progress, thanks to ongoing executive and legislative actions and key initiatives with private-sector and international partners.

While much of the annual assessment report looks at what has been achieved over the past year, in this year's report, we're also looking ahead. We're highlighting 10 recommendations whose implementation by the incoming administration and Congress would have an outsized impact on protecting the U.S. economy and national security. While the Biden administration and Congress have taken steps to implement many of these recommendations, this top-10 list highlights where gaps remain and explains what practical steps are needed to continue this work.

To discuss the latest findings of the report, we have two former commissioners joining us today.

Senator Angus King, my state's senator, serves the people of Maine in the U.S. Senate. He was sworn in as Maine's first independent United States senator in January, 2013, and as co-chair of the Cyberspace Solarium Commission, CSC 2.0, Senator King has worked tirelessly to strengthen America's national security and cyber resilience.

Next, we have Tom Fanning. He is the former executive chairman of Southern Company, serving as CEO and president of the company for nearly 13 years. In addition, Tom served for nearly a decade as co-chair of the Electricity Subsector Coordinating Council and is a leading voice for strong operational collaboration with the government and the private sector.

And they are joined on the panel by Rear Admiral (retired) Mark Montgomery, who served as executive director of the Cyberspace Solarium Commission, and he continues to lead CSC 2.0. He also serves as a senior director at FDD's Center on Cyber and Technology Innovation. Mark has served 32 years in the U.S. Navy before serving as policy director for the Senate Armed Services Committee under the leadership of Senator John S. McCain, coordinating policy efforts on national security strategy, capabilities, and requirements and cyber policy.

Today's conversation will be moderated by Sam Sabin, a cybersecurity reporter at Axios, and author of the twice-weekly Codebook newsletter. Before joining Axios, Sam authored Politico's daily cybersecurity newsletter, covered tech policy at Morning Consult and reported on the Washington D.C. startup ecosystem at DC Inno.

And 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 government funding. And for more on our work, please visit our websites, FDD.org and CyberSolarium.org and follow us on X, @FDD and @CyberSolarium.

That's enough from me for now, and Sam, over to you.

SABIN: Thank you so much, and thank you, everyone, for being here. I recognize it is before 9:00 A.M., and the busiest month, probably, that – I say this. I'm jinxing everyone, but in a very busy month this year, so thank you, thank you, and thank you, FDD, for organizing that. This is so well-run. I'm usually very nervous and running around before these types of panels, and today, I just kind of – I looked at my email, and everything was arranged for me and I had questions ready to go, and the report is here, and this is so well-organized. So thank you for being here.

I know time is short, and I just rambled for a minute. I have one reminder: We'll have time for audience Q&A, maybe five to 10 minutes towards the end. So if you guys have any questions, I'm relying on you to fill that time. So please bookmark them in your brain. Be ready. We will come to you. So you guys, thank you for being here. I'm honored.

I – I want to start by maybe setting the scene. It's been about, what, four years since the first Cyberspace Solarium Commission report with all these recommendations. I know there have been several white papers since. I – before I maybe dive into the report itself, I want to make sure that we kind of understand what we're up against. So for whoever wants to take it first – I know you're each sharing one mike, so I guess wrestle for it, maybe? But I want to hear a little bit about how the threat landscape has changed. It maybe seems obvious, but I realize that not everyone here thinks about cyber 24/7. What's changed? How have the biggest threats evolved? Things like that.

MONTGOMERY: Look, I – I – first, I'm really honored to be here with Senator King and Tom Fanning, two of the real public- and private-sector leaders on this issue.

Look, the – I think the biggest change is that we're now publicly discussing things like Volt Typhoon. I mean, we knew on the commission that our adversaries were putting malware packages into our critical infrastructure. Tom knew, because it was his actual critical infrastructure. But now, we all can have a public discussion of it, and I think it really helps. To me, having the threat infrastruc- – you know, having the threat named should help us in Congress and in the private sector, you know, come together now to really get that collaboration we need.

So for me, the biggest change is this kind of public acknowledgment of the fact that our adversaries are in our public infrastructure, and you know – and – and I would say real quick, Volt Typhoon, we report that they're in rail, you know, ports, electrical power grids, financial services. I promise you, they have our list of 20 or 23 critical infrastructures and subsectors.

And we say they're in Guam, Hawaii and the West Coast. I'm confident China has a map, and they know there's a Midwest and an East Coast. So they're everywhere, in everything, and if you have any questions about what it's like to have your supply chain penetrated with a piece of unusual material, you can ask 2,900 Hezbollah fighters what it's like to have your supply chain penetrated with an – with an inappropriate piece of malware or payload.

Tom, I'll pass it to you.

FANNING: Yes. Just give me my own perspective. I was really taken with the notion of the Cyberspace Solarium Commission. You know, Solarium was originally implemented by President Eisenhower post-World War II. And what he was doing then was to reimagine national security in that environment.

Looking at a map on the right was the emergence of the Soviet Union. On the left was the emergence of NATO.

And now the kind of idea of conflict was a tank battle on the plains of Poland. Now what we see is that the bad guys are in fact here. We are no longer protected by oceans to our East and our West and friendly neighbors to our North and our South.

And the bad guys are in our telecommunication networks, our financial systems, and our electricity grid. So what are we going to do about it? And I think that is the real challenge.

If you think about at least the lifeline sectors as defined in the American economy, something like 85 percent plus, 87, somewhere in there, is owned by the private sector.

And to me, the big idea that underpins all of the Cyberspace Solarium Commission, and all the work to come is really the idea that the private sector must collaborate, not cooperate. We have an authentic obligation to share in this nation's national security.

That is way different than for the past hundred years of laissez-faire government. And so we now have to act on that obligation.

KING: Well, first I should have mentioned in the – or it should have been mentioned in the introduction that Mark Montgomery should have gotten to Purple Heart for being McCain's policy director. [LAUGHTER]

I couldn't agree more.

I mean, I was on the radio this morning in Bangor, Maine, and they asked about cyber. I think that is an indication that we're breaking through in terms of public awareness of this issue.

And as Tom said, 85 percent of the target space is in – is in the private sector. So this – the conflict that we are engaged in isn't army versus army, although that's a factor. It's shadowy armies somewhere else, often in the world, versus the New York Stock Exchange, or the financial networks, or the energy system, or a water system.

I mean the list just goes on and on. I have to say. And these guys will smile. My principal concern, the unfinished business of our commission and of our country in this regard, is deterrence.

The cornerstone of our national security idea in this country is deterrence. If someone strikes us, they – we want them to know they're going to be hit back very hard, and it will cost them.

And so that has basically worked, particularly in the nuclear field. Cyber, we haven't had that. We haven't had that. We've had significant cyberattacks and we always hear, "we will respond at a time and place of our choosing." It never happens.

And so if you're sitting in Moscow, and I almost said the Politburo. I understand the Politburo is gone, it's just Putin.

But if you are sitting in Moscow and they say, well, "let's attack the American election this year and do all kinds of misinformation and hacking and everything." And the question is, "what will it cost?" "Not much?"

"Is there any danger that will – there'll be a response?" "Not really." Why wouldn't you do it?

And that's one of my principal concerns is that we do not have a serious deterrent policy in this country that puts our adversaries at risk and at some fear, frankly.

And that's – I think that – we've already learned we've got something like 80 percent of our recommendations enacted. All very important. They're all doing important work in a whole range of areas.

But we're never going to be able to patch our way out of this problem. We're never going to be able to solve the problem simply by defensive measures. So, these guys have been hearing me say this for four or five years now.

But I really think that's a national strategic policy priority is to establish a deterrent. And by the way, it's not a deterrent unless the other side knows it.

Remember Dr. Strangelove, why did you keep the doomsday machine a secret? Oh, well, the Premier likes surprises.

No, it's not a deterrent unless the other side knows you have that capacity and the will to use it. And therefore, they have to take that into consideration when they do their risk calculation.

So I won't go on any longer. Not to denigrate. I mean, these recommendations are really important. And what we've done is of critical importance, but there still is a missing piece in the larger policy strategic area.

FANNING: Hey. (Inaudible) I just want to underline something he said. And he serves way more than the people of Maine. He serves the people of the United States of America and really the free world. I'll say that.

Southern Company gets attacked about three million times a day. They're here. And one last comment I'll say, yes, deterrence is a big deal, but cyber defense is a lot like your body. There's a whole lot about your body that's designed to keep the bad stuff out. There's a whole lot about your body that's designed when the bad stuff gets in, white blood cells, et cetera.

We have to think about that as part of our layer defense strategy.

SABIN: Totally. Totally. And I want to follow up on the idea of layered cyber deterrence here, right?

And I guess, Senator, I'm – and then anyone else has thoughts on this. I – I'm curious what the biggest hurdle is to getting to a place where there is this stronger deterrence that you're looking for. I don't know if it's just a fear of retaliation or – it doesn't sound like it – or, you know, a fear of looking like a bad guy like our adversaries or I don't know what it is that's kind of holding us up. Because you're right, we have been hearing this for years and we need stronger deterrence and –

KING: Well, it's a calculation used generally on the part of the administration or the president.

And the challenge with deterrence, and I've thought about this a lot, the challenge is when does deterrence become provocation?

SABIN: Mm-hmm.

KING: In other words, how do you draw the line where you are threatening to the point where the adversary feels they have to act in a pre-emptive way?

So it's a – it's a – I don't – I don't mean to make it sound easy. But right now, essentially, there's no deterrence. I mean, I haven't seen – we've had – as I say, we've had multiple serious attacks over the years and there's never really been a serious response that I've seen.

Other than – other than in 2018, there was a definite work on the – on behalf of the CYBERCOM in terms of Russian interference in the 2018 elections, which appears to have worked, but we need to build on that.

And I don't – again, I don't – we don't contend that it's easy and it's got to be done carefully and thoughtfully. But if ever there was a case where escalation was a threat, that's in the nuclear field. And yet deterrence has been our basic strategy since 1950.

MONTGOMERY: If I can pick up on one thing. I don't need the mic for this. I'll just say right off the, first of all, our staff has to drink a shot every time Senator King says deterrence. So, it's going to be a rough night. But look, deterrence is a capability or capacity and a willing belief by your adversary that you'll use it.

And that second part is not queued up, because we don't do – there's parts in our report, original report, Senator King had us lay out deterrence by denial, deterrence by cost imposition, deterrence by entanglement. We work at heart – this paper, this report is really about deterrence by denial and entanglement.

How do you defend yourself? How do you work with your allies and partners? There is cost imposition things in here. But what we don't see the government do, and I would think Senator King's frustration is we don't do deterrence by cost imposition, where we go out and punch somebody in the nose when they've done things to us and –

KING: Or tell them that we will.

MONTGOMERY: And credibly have them believe that it will happen. So, we – that is a – that's beyond a programmatic or appropriation or authority. That is a policy decision to do the right thing. And I just think over – this is not a partisan thing, because it's over multiple, multiple administrations. There's been a failure to do – to execute that part of the cost imposition part of deterrence, and therefore, our adversaries don't think we'll do it.

FANNING: If you go back to the structure of the Cyberspace Solarium original report, there were really three pillars that we dealt with. One was define acceptable behaviors so that we now start to put some kind of guard rails around what we do in cyberspace. The second is to deny the benefits to the attacker. So, what can we do to harden our infrastructure? And third was to create consequences for bad behavior. And that's what these guys are talking about.

The other kind of big idea I just want to get back to that goes to this layered defense thought, is the notion that what does collaboration, what is this reimagining of national security really look like between the private sector and government? As an aspiration, this is our north star.

This is where we continue to drive the nation, I think, is, first, to illuminate the battlefield. That's going to require the participation in a physical and virtual sense of the intelligence community, our sector risk management agencies, the private sector, and those that will hold the bad guys accountable. DoD, FBI, Secret Service, U.S. Cyber Command.

And so, first, we must understand what's happening, and that should be in as much real time as possible. You hear sharing. Sharing is an interesting concept. It is totally inadequate to where we need to go as a nation. It must be real time illumination of the battlefield. Secondly, once we all see what's going on, the attack surfaces change, the attack vectors change, then what we need to do is take action to harden our attack surfaces, to deny the benefits to somebody that wants to do ill to our nation. And then third, and this comes under the heading of COTE [Continuity of the Economy], we can get to it later.

But what do we do on that bad day? How do we have a unified response to getting America off the canvas and back on our feet?

SABIN: Amazing. And I want to make sure I get to the reason we're all here, which is the new 2024 annual report. Right? I mean, we can keep talking high-level cybersecurity all day with you guys, and I'm sure we'd all stay in the room and enjoy it.

But Mark, maybe to start with you, as someone whose name is on this lovely report here, I don't think many commissions can boast that nearly 80% of their recommendations have either been implemented.

KING: That would be zero.

SABIN: Right, right. Thank you. I was accounting for, you know, miy was – my – maybe if I forgot about one random commission somewhere, but I'm going to take Senator King's word for it. No one else can boast that record. Can you tell us a little bit about just the context of what that 80% means?

I've been covering this for a while. I know that a lot of those recommendations aren't just things like get a committee to do a report. Some of them are, but not all of them are. This is a lot of heavy lifting. I want to make sure we kind of all understand what the 80% number means and what went into it?

MONTGOMERY: Thanks. So, I'll just say, first, it is a high number. Full credit to the Biden administration and Congress over the last three years. The first year, which was the end of the Trump administration, the beginning of the Biden administration and Congress, was 35%. But each year, they've added on to that. It's an incremental approach.

Senator King's theory was, if we go hit three, like a baseball player, hit .300 a year, you know, bat .300 a year, we'll incrementally get there and we'll get a ten-year contract for $500 million. But it's an incremental approach. I can't say enough how important it was to have Senator King, Representative Jim Langevin and Representative Mike Gallagher.

If we did not have their staffs and those members, we would not have gotten here. So, the staffs for those personnel, those leaders, were incredibly important. They're a part of our process from the beginning. It helped to have the Executive Branch at the beginning for some good access to information and validity and knowledge that the administration wouldn't completely oppose us, although they did on some issues, including ones that we got completed.

So first, I would say it was good bipartisan work. I will say the interesting work that no one watches is the approp's work. So, Senator Sasse, Senator King, Gallagher, and Langevin, and then sequentially less of them as they left the Senate or House, would do an annual letter to the appropriators. The truth is, the way the stuff moves into partial implementation and then full implementation isn't just that you pass a law; it's that you pass the resources to get it done.

Frank Cilluffo, one of our commissioners, used to say, you know, strategy without resources is rhetoric. And you know, we did a good job, I think, of moving past rhetoric with that. The one other thing I'd say is – it is – some things do walk backwards. We had COTE at full implementation when we had the annual plan passed, and we thought they were working it. We saw the CISA report.

The work that – what we felt the National Security Council did to implement it actually walked it backwards, and the color got worse. That does happen. It's happened to several of them. Last thing I'll mention, and I say this mostly for Senator King. We had 35% the first year, then 20% more the next year to get to 55, then 15, then 10. This is a declining returns, which is good, because there's less to do. I know he thinks we're going to get to 100, and we're not. And maybe next year is only 5%.

But that's how you – the way you win the game is you keep showing up every week. And I want to say one last thing, because we talk about deterrence. Nate Fick yesterday gave a speech on the importance of deterrence in cyberspace. The fact that that's happening is a direct line, you know, from Senator King's pushing this for four years.

So, it isn't just that we're getting things done; it's the narrative that's talked about, about how we defend ourselves in cyberspace, has changed irrevocably, I think, because of the work of the commission.

KING: You all may be aware, but it should be noted that Nate Fick is the kind of ambassador for cyber in the State Department, which was one of our principal recommendations, to create that position, and he's doing a fantastic job.

I will mention something and this is sort of a detail, but you question why did all these things get enacted. And I credit Mark with this. We had lawyers draft our recommendations into legislative language, so when we went to the committee staff we handed them a drafted bill.

We didn't say, here's a good idea, work on it. And they'd say, yes, sure. And it goes to the bottom of the pile. It really, I think, made a huge difference that they were handed completed pieces of legislation, which then they could – they could modify and amend. But that was much – I think that probably increased our throughput by 20 or 30 percent because everybody's busy around here. And if you ask a staff member of a – of a committee, senior staff member to, you know, draft a new bill around this concept, that's going to be very difficult.

So, that – and I credit Mark with that idea. I've never encountered that before, but I'm convinced that that made a significant difference. And also, I think it helps somewhat that Mike Gallagher and Jim Langevin were on the requisite committees in the House and had important positions. I'm on Armed Services and Intelligence. Ben Sasse was engaged in this process. So, having legislators on the commission was, I think, a key part of it. It wasn't – it was four legislators, four members from the executive and six members from the private sector. Kind of unique structure and I think that's one of the things that made it work.

And did you notice on the cover, Gallagher's talking and I'm listening.

(LAUGHTER)

FANNING: That's to your credit.

KING: Yes, just so you know.

FANNING: Hey, and let's not forget the private sector in this process because, you know, their constituents and they weigh in. They have the ability to influence both with voice and with money.

Look, everybody, I think, we're benefitted by the fact that everybody on the Hill and everybody in the private sector understands cybersecurity and let's not ever talk about that independent from physical security. One will manifest into the other.

That this is a big problem but very few people know what to do. And I think part of the success that underlies the Cyberspace Solarium Commission work was that we developed, right or wrong, a playbook for the first time on how to deal with this comprehensive problem.

Now, not everybody agrees, whether it's the administration or Congress or the private sector. But son of a gun, it's a way to start moving forward. And I think with that motion we created some momentum. And now, we have at least a way to travel and get something done. Still a lot of work to do. But I think that's been one of the hallmarks of effectiveness.

KING: I want to emphasis a point that Tom made. Again, we're in a very different situation than prior conflicts because of the engagement – the necessary engagement with the private sector. And what we're trying to do is something that's somewhat against history. We're trying to get the private sector to trust the U.S. government. And I saw an evolution during the period from 2016 to 2018 and 2020 where, at the beginning, this is analogous, the state governments, the state election officials were very suspicious of CISA. They weren't very cooperative. They weren't very forthcoming.

Chris Krebs broke down that. You could – you could sort of see the trust building during that period. We're now doing the same – we have to do the same thing with the private sector. It's not – it's not routine to have the federal government and the private sector, large institutions and small, work together collaboratively. There's a kind of tension in that relationship and that's something that is going to take time. But I think it's happening.

FANNING: And to get the government to trust the private sector.

KING: Yes.

FANNING: When you think about this Joint Collaborative Environment, the last thing the intelligence community wants to do is share their information with the private sector. We have to go both ways. This has to be a joint accountability or it won't work.

SABIN: I want to kind of follow that thread that you guys just pulled a little with public/private partnerships and the collaboration there. I find that, yes, there's a lot of improvement and I really don't want to undermine that. That took a lot of hard work, and it takes a lot of like consistent engagement to build that trust to get people working together. But I am still, also, finding that I'm in meetings with industry representatives who maybe feel like, you know, they're giving to government, what are they getting in return, right? And that asymmetry is still kind of working on becoming symmetrical.

I'm curious to hear a little bit about what progress still needs to be made. What it will kind of take to get to maybe that more symmetrical information sharing, understanding that, you know, the government's also dealing with highly classified work, I don't want to make seem like they now need to give everything to the private sector all the time. But, you know, what progress still needs to be made on that front and how do we do it?

KING: Well, one of the – the term Joint Collaborative Environment is an important term because fundamentally one of the important things the government can do is just set up a place where this information can be shared. In other words, it doesn't necessarily mean – a clearinghouse function, if you will. And if you have, for example, the financial sector with the leadership meeting together with CISA, with the White House to discuss these issues and sharing what they're seeing so that each individual sector or company isn't dealing with the issue by themselves. And also, if we know what's going on in one area it can predict what might be going on in another area.

So, I think – I don't want to dodge the question, I think. But I think the government has a role to play just by convening. Just by convening and creating an environment where information can be shared. And yes, Tom's absolutely right, the – I've learned in a – in some years on the Intelligence Committee, the intelligence communities first instinct is to hold everything, you know? To keep – to hold secrets and, you know, that's just not always the best policy. And so, that's where this is a – this is a growth.

I did want to mention, if you count today, this is something like the 58th meeting of the Cyberspace Solarium Commission. We're still going. This is the commission that won't die. We still have meetings, mostly Zoom meetings, and – but we've got people engaged all over the country. And I – this is – if there ever was a problem that will never be finished, this is it. Because no matter what we do, the advisories are – and we had a hearing yesterday in the Intelligence Committee, the advisories are becoming much more sophisticated about the nature of the attacks and how they disguise the attacks and those kinds of things.

So, the – we're just – as far as I know we're going to just keep going, Mark, and keep getting together and keep refining our work. And this is a pretty substantial report, four years after the founding of the commission.

FANNING: Some of the other recommendations of the Cyberspace Solarium Commission were really important. And one is this Office of the National Cyber Director, effectively to act as a coach across the administration to direct all the activity of that administration in a consistent, constructive way.

When I think about this Joint Collaborative Environment and we also look at these top 10 for 2025. They've made a lot of important progress, but boy, there still needs to be a whole lot more.

So let us think about it for a minute. The government really doesn't understand how to work with the private sector. That becomes the private sector's problem. So as I was leading the energy sector for so many years, one of the things that just struck me was that how inextricably-intertwined we are with other sectors. There's no such thing as electricity; we are vitally important to the financial sector. We are absolutely dependent upon the communication sector. And then you think about railroads and ports and water and everything else.

So as a private sector, when I say that, one of the learnings we have is how do we work together? And how do we provide the government with an architecture where they can understand and effectively work with us? It can't be "phone a friend" during a time of crisis. We have to set something up, and the government has to use those architectures in order to respond to problems. And also, once we have learnings of this Joint Collaborative environment, to spread the defense-oriented activities to make us tougher and to deny the benefits to the attackers.

COTE will be a fascinating problem. As we're working on it, we have a – a wargame, the private sector itself, through something called the Trisector Group; is staging a conflict next week. And we will learn, I think, how the private sector is going to work together and how we need to work with the government during time of crisis.

But it isn't just time of crisis. That will inform all the activity we need to do before a crisis manifests itself.

SABIN: Awesome. And I'm going to try and squeeze in one or two more questions before I toss it to audience Q&A, so make sure you're bookmarking those questions that you have.

But – but – and you guys have already referenced this lovely, display of the top 10 priorities for 2025. I'm going to ask an unfair question, which is which one for each of you is the most important?

KING: I knew you were going to ask that.

SABIN: Yup. Yeah, I mean, it's on – it's on the document.

(LAUGHTER)

Which one is the most important to prioritize? And it's just – they are all important, but there's just no way in 2025 all 10 – I mean, maybe they could. I'm jinxing myself now – will happen. Which one for each of you? It – it – top – yeah. Take my mic.

KING: That is a rotten question.

(LAUGHTER AND CROSSTALK)

KING: But – but – yeah, which one do your children do like a lot better?

(LAUGHTER)

If I had to choose, I think two and three are – are critically-important. The – the – we need much more work on continuity of the economy. How – how do we react if the worst happens? And – and if you don't have a plan, it's going to be chaos. And so I think that's incredibly-important.

And then we've talked a lot about the – the Joint Collaborative Environment for threat-sharing. I think that's – I think that's one of the most important. So that – that would be – those would be my two.

Mr. Mark?

MONTGOMERY: Yeah, I was just moving the mic away, but I – I'll go – to me – because I'll take – since you took two, I'll – I'll slide in with two. To me, it's priorization.

SABIN: Yeah.

MONTGOMERY: The systemically important entities. We – we – it's good to fix the whole cyber ecosystem. That would be fantastic, but that's like boiling the ocean.

SABIN: Yeah, yeah.

MONTGOMERY: We – we have to – we have to know what's the most important things. By the way, nearly every other country does this. But once we identify what they are – and I think the Cybersecurity and Infrastructure Security Agency, CISA, has started to create that. The National Security Memorandum 22 acknowledged it. But what we haven't done is say, what are the benefits and burdens of being those important entities, you know, the Southern Companies, the Norfolk Southern Rail, the Port of Charleston – whatever we decide those top 500 things are, what do those entities have to do to maintain a certain level of cybersecurity to deter the adversary?

And then what do we, as a government – which gets at, what information do we need to share – do we need to be able to push to them? How fast can we get them in a speed-of-data transit – transmission of threat information process – can we do? And I think if we have a limited number – we had thought 200; I think the government thinks 500 – we'd be great.

The second one for me is one we don't talk about a lot, and one that was low initially in our – in our commission, but has raised its head over the last two years, and that is, what is the role of the National Guard? I mean, we're starting to realize now that the National Guard has unique authorities to operate in public and private.

It has unique state – you know, gu- – gubernatorial – governors and federal authorities. It has the ability to move back and forth. I think at some future time, they are going to be a critical part of the cyber defense of the United States at – at the point of – of impact, at the fed- – at the – at the utilities in a way that we do not want the active-duty military or the intelligence community to be doing.

And to get to that point is going to take work by Congress for authoriz- – first, the gov- – the federal – the DOD's got – Department of Defense has got to tell us what are the – what's the art of the possible, then the Congress has got to authorize, and then appropriate the possible, and then they'd have to go out and exercise and – and get the trust of the private sector to be with them side-by-side. And you can't be – have it so the state of Virginia has a brigade of cyber operators, and the state of North Dakota has a squad of, you know, cyber operators. We've got to have a way of leveling the playing field between the states on that, too. Those are my two.

FANNING: Let me just illuminate number one here also. It – I would have answered the question one through three, so I'm – I'm with you, Senator.

(LAUGHTER)

One and three, to me, are my most important children. But one needs to be refined. I've always said this. When you go to the Cyberspace Solarium Report, the acronym we used was a little unfortunate. It was called SICI, S-I-C-I, Systemically Important Critical Infrastructure. And I know we ended up with SIE, Systemically Important Entities.

Southern Company is an SIE. We're an important entity, but not everything we do is central or critical to national security. There are those things, though, that we do that are absolutely critical. And when you think about this Joint Collaborative Environment, in order not to boil the ocean, we need to get as refined as possible and as granular as possible to those things that we do that are central to keeping America as strong as it is today.

So we – this National Risk Management Center inside CISA has to work with the private sector and with government to really understand within an SIE, what is SICI? What is really important? I would argue, at the asset level to keeping America strong one.

SABIN: Awesome. And then I have one last question before I turn it to our audience here, which is I – I – I feel like the important thing, when we're talking about 2025, is just knowing that we're – someone else is going to be in the White House. Then we have several major Senator and House elections happening this year.

We hear about the cybersecurity is, like, maybe the one bipartisan issue left standing. How much does the election factor into the work that the commission is doing? And how do you get, you know, your favorite children to – to be successful coming into 2025?

KING: Well, the – the – of course, whoever the president is makes a hell of a difference. I mean, that's where the – that's where the policy starts. But on the other hand, when – when – pe- – people don't really think about this. When you elect a president, you're really electing about a thousand people. You're electing their advisors. Who do they have around them? Are they people that care about these issues? Are they people that are going to take them seriously?

And so that's – that's a – that's a major consideration. So I think the – the answer is it is a bipartisan issue, and we – we worked the – remember I mentioned we had four members from the executive on the commission? They were members of the Trump administration, and they were very productive and – and – and there was no – you know, there – it – this – if you had watched the commission work over the course of two or three years with hundred – not hundreds, but dozens of meetings, you couldn't have told who was of which party or – you know, it was – it was totally non-partisan and – and – and non-political.

And so – so I – I think this will be an important priority for whoever the next president is, but who they put in these positions in charge of CISA or in the White House or the – the ambassador position, all of those things will make a huge difference in how this is treated in the next administration.

FANNING: In my role as Chairman, President, CEO of Southern Company, I've worked with three administrations – Obama, Trump, Biden. Everybody has taken this seriously. Every briefing I've ever done, they – they basically start with what do you want? And it's our job to explain why. And we've gotten, I think, terrific response by everybody.

So I am actually reasonably confident, optimistic that this issue will advance, and I think the good work that these folks have done to put a playbook in place for people to follow, I think we will see that no matter who wins.

MONTGOMERY: Now, I agree with that. I've had a chance to talk with transition team people, and I think whether we have a future Harris or a future Trump administration, I think they'll be the right people to execute things.

I think the harder part is whether we have an effective Congress. In other words, you can have a bipartisan issue in a non-functional Congress, and it's hard to get things done. And I'll be honest, the NDAA became a less effective tool for fixing cybersecurity issues outside of the Department of Defense over the last two years over some House Rules Committee decisions.

And – and I think we'll see that again in the – it happened last year, and I think we'll see it in the – about three months from now. So having a – a – a House and Senate leadership that understand that cybersecurity is not anti-submarine warfare, air defense, tank warfare, it is a national security issue that stretches across multiple committees of jurisdiction but still requires the NDAA to give it that persistent annual update.

What's happening right now is they recognize it belongs in all these committees and they say, "Committees, do something." Well, committees don't do something in non-functional Congresses.

KING: By the way, one of our original recommendations was that Congress create a special committee on cyber that would have exclusive jurisdiction like the Intelligence Committee. You know where that went.

(LAUGHTER)

KING: No where.

MONTGOMERY: Within thirty minutes, it was out of order.

(CROSS-TALK)

KING: No where.

But, you know, that – Mark makes an important point, that – well, for example, in the first round of our recommendations getting enacted, we had to get 180 clearances from minority, majority, subcommittees, full committees. It was a Herculean feat because of the – the structure of – of the Congress, because you've got so many committees that have pieces of this jurisdiction.

MONTGOMERY: Can – can I have it back for one second? I – one other thing I want to mention. We don't just use the NDAA, we've used approps, we've used others. This year, we actually, in the Farm Bill, have two of our recommendations, and there's two other very good cybersecurity recommendations put forward by others that we support.

Who – four cybersecurity things in a farm bill? And normally the farm bill gets done, but in a dysfunctional Congress, I think there's a reasonable opportunity that the Farm Bill will not get done in – in the next three or four months and those four cybersecurity things will fall away.

So again, lost opportunity, and – and ag – I will tell you, food and ag cybersecurity is something that should make us all very nervous, the low level of – of security that we have right now.

SABIN: And I want to toss it to the audience if – we have a few minutes for Q&A, and I think we have someone with a mic already.

FRIEDMAN: Hi. Sara Friedman, Inside Cybersecurity. Now that ONCD is approximately four years old at this point, we're asking for new authorities when it comes to regulatory harmonization and putting the FASC, the Federal Acquisition Security Council, under ONCD.

I want to find out what you think about how the office has evolved, and what they should be doing in terms of getting more authorities to do stuff to be more effective when it comes to cybersecurity?

SABIN: Yeah. And for the livestream, the question was how does the panel feel about how ONCD has evolved, and whether they need new authorities, things like that?

KING: I – well, first, it took a year or more to get it stood up, so it really hasn't been four years. It's been more like two and a half.

Secondly, Chris Inglis was the ideal first director. Did a great job of getting it set forth and getting a National Cyber Strategy established. Harry Coker's, I think, doing a great job. You've got to understand, this position wasn't designed as a – a line management position. It was designed more as a coordinator of disparate federal actions throughout the – the federal government, and it has some enforcement authority in terms of – of budget – controls of – of budgets.

So I – I think – I – I'm not sure that – that it needs additional authorities. I think the leadership that's been provided thus far has been important. But again, this is a – a – it's a – it's a complex area involving not only a lot of congressional committees but a lot of – you know, everything from Homeland Security to the Department of Defense to – to NSA, the Intelligence Community.

But I think that principally it was designed to be a – a coordinator and a – and a – and accountable executive for what's going on throughout the federal government.

FANNING: And I will add one of the jobs of CEOs of private sector companies is every day, you've got to have the humility to understand you can be better and to act on things to always get better. One of the things I see sometimes in government is the reflexive action to say everything's fine.

What we have to have is that sense of humility, especially in an area like this, which is so new and changing every day. The humility is – boy, we've got to get better as a nation. There are existential threats. And we must all kind of put our egos at the door and work together more effectively.

And I think that's a tough thing for everybody to do but that's the mindset we have to have, and some patience to understand that what we do today may not be sufficient for tomorrow. And so we always have to think about how are we going to get better, today better than yesterday, tomorrow better than today, and make the changes where we need to. And that takes some courage.

MONTGOMERY: Thank you – first, Sara, thanks for asking about NCD. We'd mentioned it a little bit, but we should have really – that really was one of our premier recommendations.

So Senator King insisted when we wrote the NCD legislation that they be responsible for the cyber – the National Cybersecurity Strategy, and that it be done in a recurring timeline, and that was done. And I think one of the key elements of that was the regulatory harmonization idea. I see Nick Leiserson is here, who is on Jim Langevin's team, is – and now with the National Cyber Director.

I think these additional authorities, to the degree they need them, I think we would support them if they specifically are to execute things that were brought up, identified by the National Cybersecurity Strategy, which we task them – which the Congress tasked the NCD with doing.

I also want to shout out Kemba Wal – you know, we've been very lucky. Chris Inglis, Kemba Walden in an acting role. And then Harry Coker. We've had three good deliberate – this is a – they're like our commission, persistent, deliberate, you know, thinkers to get to a long-term goal.

And I think we've been fortunate with all three. But I do think, over time, they'll need new authorities, but only in the sense that they're carrying out the original tasking to Senator King and Representative Gallagher and Langevin gave them to write a National Cybersecurity Strategy, identify a way forward and execute to coordinate and collaborate properly with the rest of the federal government and the private sector.

SABIN: (Inaudible). Yes.

MILLER: Hi. Maggie Miller with POLITICO. Thanks so much for doing this.

Senator King, you know, you've been on the Solarium since the beginning. But at this point, you are the only currently sitting member of Congress that is still part of CSC 2.0.

So, you know, given we've had Senator Sasse, we've had Congressman Gallagher and Langevin leave, have there been other members of Congress that have expressed interest in joining CSC 2.0, helping out with the work here? How do you keep it moving forward with sitting members of Congress?

KING: We haven't formally talked about adding members, but there are members, for example, Mike Rounds of South Dakota and is a – is a critical cyber player and is involved in all of the issues that we're confronting in the Congress.

Gary Peters on Homeland Security has been very engaged in these issues. Kirsten Gillibrand has been very engaged, particularly in developing cyber talent. She's created a wonderful program that's sort of a cyber-West Point.

And so there are different members. We haven't really talked about adding new members. It's probably not a bad idea as I look around behind me and there's nobody there.

MONTGOMERY: If I could comment on the House, I would just say we've been – again, I agree on Senator Rounds, by the way, and Senator Ossoff has really stepped up on a few.

But in the House, you know, Representative Houlahan has always supported our legislation. She's on the Democratic side. On the Republican side, we've had Representative Garbarino and Fallon and Luttrell come forward on these.

Mark Green is working – Representative Green, head of the Homeland Security Committee is working some workforce legislation that we really think is promising and very reflective of our recommendations.

So on a broad – and Representative Khanna has worked the same legislation. So broad bipartisan level. You know, I don't think the OG is taking anyone on, but at the same time, they're doing it.

And one thing I would say, even when we put out the legislation, we should be clear. Congress never did exactly what we said. They did exactly what they thought was right. And that's their job, not ours.

And I think in the end, every Senator Peters team made several pieces of our legislation better. And you could – you could see it.

I will say on occasion, Congress waters down our legislation and I wouldn't call it better afterwards. But we've been very, very fortunate that the broad premise of our legislation is carried through on these 80 percent.

GAUL: Good morning. I'm Patrick Gaul, I'm the Executive Director of the National Technology Security Coalition headquartered in Atlanta.

Four years ago, when you launched the initial report, artificial intelligence was in the labs of Google, Georgia Tech. Today, that's not the case.

How does what's happening with AI today impact your thinking across everything you're still doing on the commission?

SABIN: For the livestream, the question was, how is AI impacting everything that the commission is doing and how they're thinking about these issues?

FANNING: So we're getting in various forms classified briefings about what those impacts may be.

And I would just add to AI because that is new relative to the beginning of the – of the CSC – is also quantum computing. I think that's going to be a major inflection point in all of these issues.

Look, what you're really talking about is scale and speed. And where is human intervention possible? And how do the outcomes of AI impact our own thinking?

We know that bad actors can infiltrate what ultimately is generative AI production. So these are all things that we have recognized in the past and that people are thinking about right now.

But boy, that genie is getting out of the bottle in a hurry. And this idea of regulation. I've always been nervous about regulation. It is always based on historical observations. It probably is out of date by something, and it really doesn't contemplate future changes very well.

So regulating AI, yes, I know we got to do it. But boy, it better be process oriented as opposed to say outcome oriented. And I think it's just something we're going to have to continue to evaluate over time.

MONTGOMERY: You know, one thought I'd have is we were very – I would say you can see in our recommendations. We got pretty granular pretty quick. You know, we did not mess around with esoteric thoughts.

In this AI, if it had existed the way four years ago now, I think we would have very much said, we need a – and it's regulatory, but I think in a very focused way, we need to protect the model weights. We need to insist on a certain level of security, physical, and cybersecurity at the six or seven firms doing this about the core intellectual property, the model weights and others, the algorithms that drive this thinking.

Because if that is not protected, I'm worried about foreign countries getting in it, but I even more worry about a bad actor getting it who has absolutely no goodwill or intentions. And then being able to, you know, use these tools for really nefarious purposes.

KING: By the way, parenthetically, deterrence doesn't work on a non-state actor. They don't care about dying and they don't have a capital city. They're worried about losing. So that's a separate issue.

But I view AI as accelerating the danger, but it's the same fundamental danger.

FANNING: Yes.

KING: It's something that will make it easier to multiply attacks, to have attacks hit multiple sites. But the fundamental issue of how do we defend ourselves and how do we develop a deterrent strategy, I think is still there.

AI doesn't change the – it doesn't change the elemental risk, but it makes it much worse. It makes it much more dangerous. I think an accelerant is the way I would characterize it.

SABIN: And I want to be mindful of time because I realize it's after 9:30 and we were supposed to end at 9:30.

But, you know, I think we'll just wrap it up there. I was going to try and sneak in one more question, but I want to be mindful of your time.

So thank you all for being here and taking time this morning. Thank you to our audience for being here. And, yes, best of luck in 2025 to the commission.

KING: I just want to say this is a –

SABIN: Yes.

KING: It's a very common experience for a senator to talk to an audience, every one of whom knows more about the subject than me. And it's a little daunting, but thank you for joining us.

And final thing is, we're still in business. We're still looking for ideas. We're still looking for thoughts. Be in touch. Be in touch with Mark and the – and the commission because this is a never-ending process. Thanks.

END