FDD EVENTS

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

Featuring Rep. Mike Gallagher (R-WI), Sen. Angus King (I-ME), and Tim Starks
Introductory remarks by Dr. Samantha Ravich

RAVICH: Thank you for being here. I'm Samantha Ravich, chair of the Center for Cyber and Technology Innovation at the Foundation for Defense and Democracies. At CCTI, we focus on both strengthening U.S. resilience against cyber challenges, as well as seizing the opportunities presented by emerging and innovative technology. FDD is a nonpartisan research institute exclusively focused on national security and foreign policy. We proudly accept no funds from foreign governments or corporations.

I'm also a distinguished advisor to the CSC 2.0 project, which is pleased to cohost today's event with FDD. CSC 2.0 was established by the Cyberspace Solarium Commission and is continuing the work of the commission. I sit alongside my other former commissioners, Suzanne Spaulding, Frank Cilluffo, Tom Fanning, Patrick Murphy and of course, the members of Congress, Senators Sasse and King and Representatives Langevin and Gallagher.

Today, we have two of those members, Senator Angus King and Representative Mike Gallagher, here to discuss the 2022 Annual Report on the Implementation of the U.S. Cyberspace Solarium Commission's Recommendations. Anyone who has ever worked with these two gentlemen will understand when I say that it is one of the great honors of my life to count them both as colleagues and as friends. They each have a rare and precious combination of life experience, intelligence, curiosity, compassion and humility that is so rare and is so needed in our nation's capital.

Senator King has been serving as Maine's independent United States senator since 2013, before which he served two terms as Maine's governor. In his roles on the Armed Services Committee, the Select Committee on Intelligence, the Committee on Energy and Natural Resources and the Committee on Rules and Administration he has worked tirelessly to strengthen America's national security and promote prosperity. He brought to the Solarium the clear-eyed wisdom about the perils our nation faces if we don't harden the cyber infrastructure that underpins those two pillars of our country.

Congressman Mike Gallagher has represented Wisconsin's Eighth District in the U.S. House of Representatives since 2017. For seven years, he protected our country from adversaries as an active duty United States Marine, including two deployments to Iraq. He understands the price of freedom at the granular level. But Mike is also a scholar with a Ph.D. from Georgetown. If anyone knows the sources of strategic adjustment to deal with emerging threats, it's Mike. Read his dissertation for more about that.

We are also pleased to have Tim Starks here to moderate the conversation. Tim writes the daily Cybersecurity 202 Newsletter at *The Washington Post*. It is a must-read to understand not only the news of the day, but what it means and how it drives policy discussions. Tim previously was senior editor at *CyberScoop* and ran *Politico*'s Cybersecurity Newsletter. I see a number of his successors in the room today who I'm sure will pose thought-provoking questions during Q&A.

Before I turn this over to the people you actually came to hear, let me underscore a few points.

The original mission of the Cyberspace Solarium Commission was to, quote, "develop a consensus on a strategic approach to defending the U.S. in cyberspace from significant cyber attacks." We clearly met our mission. Over the course of the commission, we developed 116 recommendations, many of which were accompanied by model legislative language. But as Patrick Henry once said, "the battle, sir, is not to the strong alone; it is to the vigilant, the active and the brave."

Cyberspace itself and attacks against it are moving and evolving. It is not enough – it will never be enough – to reach a consensus and craft needed legislation. Implementation and execution of the legislation is needed, and so the second annual report which we just published under the expert guidance of Rear Admiral (Ret.) Mark Montgomery and Jiwon Ma assesses

each Cybersecurity Commission recommendation. Have they been implemented? Are they on track? Has progress stalled? Are there significant barriers to implementation?

These rankings were the result of hundreds of conversations between and amongst commissioners, staff, government representatives, subject matter experts and many others outside of CSC. I urge you all to read the assessment but let me give you some top-line figures.

Of the commission's original 82 recommendations, nearly 60 percent are fully implemented or nearly – nearing implementation, and more than 25 percent are on track to implementation. Last year at this time when we published the first annual assessment, only 35 percent were fully implemented or nearing implementation.

So, with that, I now turn it over to our panel to discuss where we have been, where we are and where we are going in our work to meet the urgent challenges facing our nation. Thank you.

STARKS: Thank you, Samantha, and good morning, Congressman. Good morning, Senator.

A little bit of a pet peeve of mine for events like this is when they never ask the big question that's in the advertising for what it's about, so let's just start with that big picture. How resilient are we in cyberspace today?

KING: More than we were, but not good enough.

STARKS: More than we were compared to, say –

KING: Five years ago. A couple of observations: I do think we're better off on a number of levels, in part because of the implementation of a lot of these recommendations. For example, the creation of the National Cyber Director, the development of a National Cyber Strategy, which is – he's working on right now, his office is working on right now, the development of a Bureau of Cyberspace and Digital Policy in the Department of State, confirmation or voted out of committee, a director for that. So a lot of progress.

The other thing that's sort of an intangible that I've noticed, I don't know if you have, Mike, but there's a much higher level of understanding of how urgent this problem is in Congress. It used to be I would go up to people and start talking about them, and their eyes would sort of glaze over. Now I've got members coming up to me and wanting to get together, wanting to have meetings. For example, Mike Rounds, a Republican senator from South Dakota who's the ranking member on this Cyber Subcommittee in the [Senate] Armed Services Committee, is having regular meetings in his office of a variety of people talking about these issues. It's a much-elevated discussion, and I think that will manifest itself in additional policy implementation and adoption.

Final point: Tim, as you know, one of the real problems in this area is that this isn't traditional conflict. This isn't army against army, navy against navy. The battlefield is the private sector. Eighty-five percent of the target space is in the private sector, and it's an unusual situation where we have to work out a partnership between the federal government and the private sector to effectively defend the country, and that's still a work in progress. I think the private sector's getting it. Some areas are way ahead of others, and some aren't doing so well.

And then the final step is you get down to the desktop. All of our work, all of our legislation, all of our appropriations, everything else, are no good if somebody in a major energy company hits on a phishing email. You can lose the whole thing right there.

So, it's a very complex problem that involves a new concept of the government and the private sector working in partnership, which doesn't come naturally to either party, in order to confront this issue.

So, the short answer to your question is, as I said at the beginning, we've made a lot of progress, but as Samantha said, this is a problem that – that isn't going to go away and it's not going to be the same tomorrow as it is today.

GALLAGHER: I agree with what Senator King said. Maybe I'll just add a few points.

Not only is there a greater awareness among our colleagues in the House and the Senate but perhaps that is a function, I think, of the greater awareness among the American people. I mean, everyone, you know, who has a cellphone, particularly anyone who works in a business it doesn't need to be a massive Fortune 500 company, it could be a small business in northeast Wisconsin, I think now understands the salience of cybersecurity or just the threats that are out there in cyberspace.

So, you know, where are we along the 12-step program of resilience? I don't know. At a minimum, we've admitted we have a problem and perhaps we've recognized there's a higher power in the form of Angus King.

But not only, I think, you know, are we taking steps as a commission and as a Congress to improve our resilience, I think my sense is that a lot of the dedicated cyber warriors at NSA [National Security Agency] are building upon the foundation of concepts like defend forward, hunt forward.

We've learned some hard lessons over the past five years, in particular, and General Nakasone and his team, I think, are applying those lessons around the world. So I think that's improved our resilience.

And then just finally, to dovetail off everything Senator King said about, you know, the dilemma of deterrence in cyberspace remains, which is, you know, so much of it is playing out in the private sector.

And if you read our initial report, I think you'll see a genuine attempt to strike the right balance between, you know, the federal government, you know, kind of nudging the private sector to take cybersecurity more seriously without having an overly onerous approach and dictating to the private sector everything that they must do.

So that's a tough balance to strike, that's a problem that remains, but I think we're at least heading in the right direction.

STARKS: Yes. Senator, you mentioned Chris Inglis. He's been in the office a little bit more than a year. One of your top, if not your top, achievements, I think some would argue, is getting that office created or helping to get it created.

KING: And getting Chris appointed.

STARKS: And getting Chris appointed, sure. A little bit of nepotism sort of in the family, if you will, because he was a Solarium commissioner as well. But what I wanted to know is what do you think of how he's been doing? This is for both of you of course, but can you point to a tangible difference that that office has made, keeping in mind the short time he's been there?

KING: Well, one of the reasons that we set up this office was that cyber was scattered all over the federal government and there were different authorities and different agencies and, you know, competition and a lack of coordination.

So, when you create a head of that, part of it is that new office finding its footing with regard to all these other agencies, and the other agencies saying "Yeah, OK, there is somebody that has this overall responsibility."

I think the best sign of success or of progress was the fact that the President gave Chris the pen on writing the new [National] Cyber Strategy, which is in progress, which will be done in a matter of, I think, a couple of weeks or months. That's an indication of the recognition of the status of this office, that it's not just something that Congress imposed on the White House.

And I have to tell you, from having worked through it, and I think Mike will agree, I can remember a lot of phone calls. First, we had to persuade the Trump National Security Advisor that this was necessary and why it wasn't an encroachment on the National Security Council. Then, the election came and then we had to do it all over again with Jake Sullivan and the Biden administration.

So, it wasn't easy to get the White House to accept this new position but it's happened, and I think that that's an indication that that office is having an impact. And Chris has called – he's finally built his staff, he's got funding, and my sense is that he's settling in.

Now, you know, there's still going to be tensions in who's in charge and that kind of thing, but I think he's worked out a good relationship with Jen Easterly and Anne Neuberger. Those are the important top relationships. So, I feel like they're on the right track.

GALLAGHER: I'd say, in addition to having the pen on the National Cyber Strategy, which is absolutely essential, as Senator King mentioned, two other areas where he's already had an impact is kind of tackling the cyber workforce issue head on. He's in a variety of things to proactively do outreach on that topic. Obviously, it's not something that can be solved with a silver bullet, you know, solution coming out of the White House or Congress. But also, my understanding is he actually has productively worked with OMB [Office of Management and Budget] in order to kind of really establish guidelines for various funding goals among all the agencies that play in cyber.

So, I do think he's having an impact. Obviously, this is very early stages for the Office of the National Cyber Director. I remember we had an event kind of honoring everyone that worked on the commission and Chris was there and kind of gave us, like, a little memento from the Office of the National Cyber Director, and I think if memory serves, he had kind of fished the material for that out of the trash in the Eisenhower Executive Office Building.

So clearly, you know, there's a lot of work that needs to be done, in terms of resourcing the Office of the National Cyber Director, but Chris is the perfect person to do that. He has the right temperament, obviously the right background.

And I think it's fair to say, and push back, Angus, if you disagree, we expect him, you know, because we have confidence in him as an honest broker, to come to us and say "OK, here's what's working and here's what isn't working, in terms of this initial model for the Office of the National Cyber Director."

This, you know, we got it past in legislation but it's still going to be an iterative process going forward to figure out precisely the level of authorities and resources that that office needs to be successful.

STARKS: That National Cyber Strategy both of you mentioned, do you have any insights into what will be in there? Do you have any insights into what you think should be in there?

KING: I think it'll be an exact copy of our original report.

I mean, why bother to rewrite –

GALLAGHER: Why mess with perfection?

KING: I will say, I don't know but I'm sure that the broad outlines will be what we all understand, in terms of resilience, norms and standards of behavior, deterrence, and cost imposition. You know, I think that's going to be a part of it.

I'm hoping that it will be a little clearer on the deterrence, on the cost imposition piece, because I think that's been a gap in our strategy going forward, although the president I think has significantly helped by outlining, you know, what's off-limits and putting in some lines about where civilian infrastructure and that kind of thing.

So, I don't have any inside information about what's going to come.

GALLAGHER: Yeah, neither do I. I guess what I hope will be in there is a – you know, some nod to the signaling strategy that we've called for in the final report. And Senator King and I had sent a letter to the White House asking them to move out on a more transparent signaling strategy in cyberspace.

Second, you know, Chris obviously was a very active member of our commission and influenced the strategy that's in the final report. So, it wouldn't shock me to see the basic idea of layered cyber deterrence that is in the Solarium report find its way into the National Cyber Strategy.

And I think, third and related, one of the ideas behind that is that you're not going to have perfect deterrence in cyberspace, right?

I mean, in contrast to strategic nuclear deterrence, there's just going to be a level of failure. So, you need to have a respectable posture of deterrence. And that is, kind of, where the layered strategy comes in, in order to get at that.

So that's what I hope will be in it, but we'll see– as well as, you know, a recognition of the brilliant prose that was in our report.

STARKS: Of course, naturally. Why not?

I want to try to make this one a quick one. And I realize this might be a little difficult because it's a little like asking a parent to choose their favorite child, but –

If there is one thing that you have not gotten done yet, that you would pick, that you would like to do – if you had to pick one thing, what would it be?

GALLAGHER: Well, maybe this is a cheat, because we technically got this done, but we still need to do oversight. And I want to highlight –

STARKS: I think I'm thinking of one recommendation.

GALLAGHER: Well, that's why I'm saying – it would be the Continuity of the Economy planning led by CISA [Cybersecurity and Infrastructure Security Agency]. CISA still needs to do it. And I just want to highlight the role. That was really Samantha Ravich's idea. She was the brainchild behind all of that. So that's an area where we got it [legislation] passed, but we still need the actual plan to come out of CISA.

That's just a reminder that, as my good friend Angus King often says, "execution is just as important as vision." We need to make sure that that is executed appropriately. If that didn't satisfy you, I can come back and think of a different one.

STARKS: It did.

GALLAGHER: Yeah.

KING: I think the biggest missing piece right now is almost done. And that is the Cyber Diplomacy Act, the establishment of the Bureau [of Cyberspace and Digital Policy] in the Department of State, whose job it is to coordinate international activities with regard to cyber and establishing international standards [and] international coalitions. Multilateral sanctions are always more impressive and more oppressive than unilateral sanctions. So, engaging the international community – if you think about it, we had 1,000 years to work out the law of war and get to the Geneva Convention and other kinds of rules. We've had 25 years to work out the law of cyber war, and we're not there yet. And we need to figure out what's off-limits, what are the cyber version of chemical weapons?

And so, I think this, and where we are is the Senate Foreign Relations Committee, last week, voted out Nate Fick as the director of this Bureau, which the administration created on their own, to their credit. But they also reported out the Cyber Diplomacy Act, which gives more full description of the work of the bureau. And I think that's one of the major pieces of unfinished business.

There's also Strategically Important Critical Infrastructure, [and] Bureau of Cyber Statistics.

STARKS: Sure.

KING: There are three or four things that are still cooking that we need to get done.

STARKS: Let's talk about Systemically Important Critical Infrastructure or PSIE'S or SIE, depending on who you talk to –

KING: We call it SICI.

STARKS: SICI, yeah. That is one that there has been some progress, in terms of getting included in the House version of the NDAA. It's also one where there's been some industry pushback. Could you talk about whether you think that pushback is fair and how you might be trying to overcome or address it?

GALLAGHER: Well, the pushback we heard from the banking sector, in particular, was "Hey, we're already, you know, awash in regulation, we're already investing a lot of time and money at this problem. You know, why should we have to deal with this other new layer of regulation?"

And we didn't dismiss that argument. I think we've made a good faith attempt to meet them halfway and kind of have a, in the latest iteration. Mark, you can correct me if I'm wrong – kind of have a process through which the reporting we're already doing would be counted as satisfying some of the SICI reporting. Yay or nay?

[Mark Montgomery signals yes]

So that's one.

Some of the pushback we heard from the software industry, you know, we're trying to internalize and meet them halfway. I guess the bottom line is we've modified it substantially, we've listened to our colleagues that had objections, and I'm, I guess, cautiously optimistic that there is a path forward.

And I guess it gets to the point I made at the beginning, which is, you know, we're trying to strike that balance, right, between the federal government saying "Hey, private sector, we need everybody in the C-suite to understand why cyber is important, but we also don't want to, you know, get the regulatory framework wrong."

So, I don't know. I think we've made progress. Let's hope we can get it done.

STARKS: Certainly, I saw some clear attempts to address their concerns in what the language that got into the NDAA [National Defense Authorization Act], but even as recently as last week, they seem still unhappy. Don't know if there's anything that can be done. I don't know, maybe down the Senate side, you could take something up?

KING: Well, obviously we're going to try to ameliorate their concerns but without gutting the bill. I mean, that's the challenge. I should say one of the really hard parts of this whole thing is the multiplicity of jurisdictions in Congress with regard to this subject.

In order to get our first set of recommendations adopted in the National Defense [Authorization] Act a couple of years ago, we had to get 180 clearances from minority, majority, subcommittee, and committee. You have no idea what a nightmare that is. And there were a couple of ones where we ended up with one person on one committee – it was cleared by nine other people – said "No, not going to do this," and it –

STARKS: Do you remember what it was?

KING: I do vividly but I'm not going to tell you.

STARKS: Disappointing.

KING: But that's one of the problems. I mean, the least likely recommendation of our Solarium Commission is to set up special committees on cyber in both houses, similar to the intelligence committees. In 1976, they realized that intelligence was spread all over Congress and they set up those committees on intelligence in the Senate and the House to consolidate that jurisdiction.

I don't know how they did it because trying to do that with cyber, we have found, is virtually impossible. Nobody wants to give up their little piece of the jurisdiction. So that's one of the real hold-ups.

STARKS: I feel like I have a suggestion for what happened there and what has also happened when any other time Congress has created new committees, there were some pretty big scandals in the 1970s on intelligence that seemed to create a lot of momentum.

KING: Yeah, it was the Church Committee.

STARKS: Right.

KING: Yeah.

STARKS: Then there was, you know – I hate to bring it up – after 9/11 the Homeland Security Committees were created.

GALLAGHER: Yeah.

STARKS: And I don't know what kind of event you think it might take for Congress to say, "We really have to do this."

GALLAGHER: We tried to paint the picture of what such an event might look like in the opening pages of our report with a sort of dystopian future, teasing out the aftermath of a cyberattack. But we're obviously hoping to prevent that from happening.

As we became fond of saying, it's we want to be like the 9/11 Commission just without the cyber 9/11 happening.

But it's a challenge, and to cut across the committee jurisdiction that Angus talked about, I think it's important to recognize how pivotal our colleague Jim Langevin was in doing that. You know, he is the chair of the Cyber Subcommittee on the [House] Armed Services Committee, and because of both that position as well as just his indefatigable efforts in this space, we were able to get a lot passed. And I don't think it would have been possible without his help.

KING: No.

One of the reasons this commission was so successful – and by the way, if we were a centerfielder for the Yankees given the implementation percentages, there's no end to the money we could make.

I mean, if you're batting .600 in the major leagues, you're in the stratosphere.

But one of the reasons it worked so well was the unusual structure and having started with four sitting members of Congress and then four members from the administration, from the executive, and then six members from the outside. And so, in a sense, our commission started with four fifth columnists, if you know what I mean. In other words, we had active members of Congress. Mike's on [House] Armed Services [Committee]. I'm on [the Senate] Armed Services [Committee]. I'm on [the Senate Select Committee on] Intelligence.

You're on the [House] Foreign Relations committee I think.

GALLAGHER: I'm on [the House] Intelligence [Committee] now. I wasn't at the time.

KING: Oh, OK.

GALLAGHER: Yeah.

KING: So, we weren't on the outside knocking on the door; we had people inside. And I think that really helped in order to – in terms of getting these things moving.

Jim Langevin was an absolute star given his position on the Armed Services Committee, and he is retiring, which is a huge loss to Congress. Yeah.

GALLAGHER: To extend the baseball metaphor, the value of a replacement is tough on that one in Congress.

KING: Yeah.

GALLAGHER: And two of our fifth columnists just walked in, the Honorable Mr. Murphy and Frank Cilluffo.

KING: Oh, yeah. Great.

GALLAGHER: They do great work. Yeah. There you are. Perfect.

KING: Patrick and Frank, good to see you.

STARKS: There were a few people who submitted questions beforehand. I'm going to combine a couple of them.

Here's something from Sara Friedman of *Inside Cybersecurity* and Debbie Taylor Moore with IBM that they wanted you to discuss. CISA has released a request for information and details on 11 listening sessions to implement the March incident response law. What do you think about these efforts, and what should CISA be keeping in mind as it moves ahead?

Also, can you comment on any feedback we've heard so far from all the potentially affected parties?

GALLAGHER: It's a long listening session process. I get it for those of us who feel a sense of urgency, but I think it's important to get it right, so I think it's a useful effort. And, you know, I have confidence in Jen Easterly and her ability to get this right.

So, I think it's a positive step forward.

KING: I think it's important for a subtle but essential reason, and that is remember I said at the beginning a lot of what's going on here is trying to build a relationship of trust between the federal government –

GALLAGHER: Yeah.

KING: and the private sector. And for Jen to be taking this time and having these sessions and consulting and listening is essential to building that relationship of trust. And if she just said, "OK, here are the [regulations], boom," I think it would've been a disaster.

So, as Mike says, it's going to certainly take a little longer to do it, but again, we are trying to do something new here, and anything that's done, and by the way, CISA's doing a great job. I participated in Maine, and they're sending people around the country to meet with people in the private sector to have these seminars about cybersecurity and just alerting,

you know, businesses in Portland, Maine, about what the risks are and what CISA can do. They're really doing some serious outreach. I think it's working, and it's essential in the long run to give people the confidence to report, you know, to share the information, to share it in real-time, to get ready for this joint collaborative environment which we hope we can establish where people can share in real-time. But there's the law, and then there's the sort of human infrastructure and attitudinal infrastructure that has to be built, and I think they're doing it the right way.

STARKS: This one's from – it's related. It's from Patrick Gaul at the National Technology Security Coalition. They ask, "With the proliferation of cyber instant reporting legislation across multiple agencies – because this isn't just something that's happening with the law – what are your thoughts about harmonization?

GALLAGHER: I'm in favor of harmonization.

KING: I'm for it.

GALLAGHER: Yeah, I'm for it. I think, and this is, an area where empowered CISA director – and remember, elevating and empowering CISA was a key finding in our report. We've gotten a lot of that accomplished in legislation, but there's more that needs to be done. [CISA] who has a productive working relationship with an adequately resourced and empowered national cyber director, I think, can go a long way in achieving that harmonization.

KING: But again, I sound like a broken record, but if we're going to establish credibility and trust with the private sector, we can't inundate them with regulations from six different agencies. At some point, they're just going to throw up their hands and say, you know, "This is not working." They'll just fill out the form and move on.

So again, I think some kind of harmonization – I mean, that's one of the reasons we created the National Cyber Director, was to bring some coherence and –

STARKS: Is he involved in that process? I guess – is he on the commission that is looking at harmonization?

KING: I don't know.

STARKS: OK.

KING: I don't know. If he isn't, I'll call him this afternoon.

GALLAGHER: Get on it, Chris.

KING: Yeah.

STARKS: Yeah. This is one from Natalie Alms with FCW: "CSC 2.0 released a workforce report this year. What are the top priorities you'd like to see addressed on workforce, and what are you working on going forward?"

KING: Well, I'll start just in general by saying it's one of the most serious problems we face. Everything we're talking about doesn't work if you don't have people that know how to deal with this issue, and it's a huge shortage. I've seen various estimates – 30,000, 50,000, 100,000. There are tens of thousands of vacant positions in both the private sector and in the government, in the military. There are a lot of initiatives. [Senator] Kirsten Gillibrand, for example, has a proposal to create

what amounts to a cyber West Point, a school program for young people to be able to learn about the subject, learn about what to do, and then have a variety of options when they get out.

I can't really give you as fulsome a response to what's actually happening. I do know that there's a lot of work going on in this subject. But ultimately, we need young people to view this as a career option. I mean, in Maine, for example, at one of our branches, the University of Maine, we have a cybersecurity graduate and undergraduate program that's fully subscribed, and that's what has to happen across the country.

GALLAGHER: I say three things come to mind. One is we want to see a tripling or a quintupling down on the CyberCorps Service Program. That was a key element in our final report. We've made some progress but it's not sufficient. We think that's a useful model that can be expanded.

Second thing is – and I may be going a little bit astray from the Solarium Report language, but it's been my observation on the [House] Armed Services Committee that we've actually given the Pentagon enormous authorities to hire people from all over, and they can make them majors, lieutenant colonels, they can even make them admirals if they wanted to get really creative.

KING: I'd like to be an admiral.

GALLAGHER: Yeah –

I'd like to be a Viceroy. That's always appealed to me. But our sense is they're not really using those authorities aggressively. Why is that? We want to understand that. Is it just because that's not the right model? Is there institutional resistance, status quo bias? That's an area where I think we don't need to pass legislation, we just need to do basic oversight to understand.

And then the final thing I'd say is we have an interesting Solarium-related event in my district in Green Bay. Microsoft has formed a partnership with the Packers to do kind of, like, a tech innovation hub, an incubator, and the president of Microsoft came –

KING: It's right next to the Lambeau Field.

GALLAGHER: That's right. Angus came and visited, we went to a game together. His wife's a Packers fan. I always need to note that.

Then we went with the president of Microsoft to a local high school where Microsoft is investing in – in basically a cyber apprenticeship program. And when we talk about apprenticeship, usually we're talking about the trades, right, reviving manufacturing, welding, pipe-fitting, things like that, all great stuff we need, particularly in the industrial Midwest, but I think the apprenticeship model in cyber is interesting, particularly for those really talented kids who have a unique aptitude and maybe the traditional path at a four-year liberal arts college is not necessarily the best path that that harnesses their cyber talents.

So those are kind of three areas that stand out.

KING: Let me touch again a little bit on the military. A couple of problems is that, again, we're talking about change here, and change is hard. You don't need to be able to do 100 push-ups to be an effective cyber warrior.

So, you know, the question is how does the military modify their requirements and who they're looking for? But also, the military and this has struck me. I mean, maybe it struck everybody long before me, but the military's one of the few organizations in our society that doesn't do lateral hires. You join the military at the age of 22 and you stay until you're 60 and you move up.

But, you know, we've got to be able to have them think "Oh, here – we need a cyber – let's bring a person in who's 45 years old, who has had a lot of experience with Microsoft, and either bring them in as a civilian or make them a Colonel."

I mean, we've got to rethink how the structure works and also the criteria because a cyber warrior may be the person that wins the next war, and it may be somebody in a wheelchair who couldn't possibly do a pull-up but who has the brains and the talent and the imagination to defend the country.

So, I think that's something the military and the military is not an institution that, you know, is a – anxious to embrace change, but I think that's part of what's got to happen.

STARKS: Right. We're about to move into a Q&A phase, but I wanted to get one last question off perhaps, make it a two-parter.

Looking at what you have on your agenda going forward with CSC 2.0, what work most enthuses you or excites you that you really want to dive into?

And I don't know how to ask this one exactly, I struggled with it. Do you worry about a shelf life? Do you worry about people tuning out, you know, what you're saying? Do you worry about overstaying your welcome or thinking, you know, "We've accomplished our mission, let's stop?" What's the end game, of sorts?

KING: Yeah. Well, the reality is this is a problem that's not going to go away and it's probably going to get worse. And I don't think there's any – I think there's still an expanding awareness certainly among policymakers, the general public, one of the things we haven't talked about is we need a UL for home routers, we need labeling, and there's no legislation involved there. Somebody needs to pick that up. Maybe this organization should set up an Office of Cybersecurity Certification.

So, there's plenty left to do. I mean, there's always a danger of sort of relaxing and saying "Well, we've done all these things, and therefore, we're OK." Unfortunately, I think we're going to get periodic reminders, like Colonial Pipeline or OPM [Office of Personnel Management] or those kinds of things.

That's going to keep happening. I met last week with a Maine credit union, OK? They're being attacked hundreds of times a day, Maine credit unions. This isn't, you know, ConEd or Wells Fargo, these are little community institutions. So they know what's going on and they're very aware of it. Mike and I did a letter recently on hospitals. Hospitals are sitting ducks, and that's an area of great concern, and they're starting to figure it out.

So, the short answer to your question is I don't think this issue's going to go away and I don't think we're going to go away and I don't think the concern is going to go away.

GALLAGHER: I say I – in addition to the low hanging – well, not low hanging, but let's say the legislative issues that are in the red zone that we need to punch into the end zone, we've mentioned SICI, joint collaborative environment, Cyber Diplomacy Act.

I'm most interested, as I mentioned before, in doing oversight of the Continuity of the Economy planning, of the cyber force structure assessment that we've mandated, as well as digging into the National Cyber Strategy and really kind of having a debate. I think that's going to be interesting intellectually.

Intellectually, as well, I think there's more work that needs to be done on, you know, really teasing out the connection between cyber war and kinetic conflict, or where cyber operations could have kinetic effect, right, particularly as we think about what is perhaps our most stressing national security problem, a potential confrontation over Taiwan, what is the role of cyber in that, right? Could the Chinese potentially attack some of our aerial and seaports of debarkation, as part of an overall effort to put us on our heels in a Taiwan confrontation? I think there's a lot of really fascinating work that could be done at FDD [Foundation for Defense of Democracies], in the broader think tank community, and in Congress that really excites me.

And as for the shelf life of my political career grows, you know, smaller by the day.

KING: – this guy's running unopposed.

He has no primary, no general election. How the hell does that work?

GALLAGHER: Yeah. Family delivers babies and has a pizza restaurant in Green Bay –

people feel indebted to you after that. But I don't know, I think there's still interest among our colleagues, and I enjoy working with Angus King on national security problems. So, continue doing that.

STARKS: All right, let's [go to] Q&A. It looks like we do have some microphones available. And we already have one person booked. We'll come to you next.

FRIEDMAN: Hi this is [From Sara Friedman of] *Inside Cybersecurity*. It's been over a year on the cyber executive order, E.O. 14028, and there was another memo just last week on securing software. How do you think implementation has gone on that so far? And do you think that there are areas related to that that need to be improved or worked on more?

GALLAGHER: Oh, gosh, I'll get the hard one. Yeah, I think there's more work that needs to be done on implementation. I mean, I think the overall framework in both documents you reference was good. I think there are lingering questions remaining about compliance or understanding within the private sector.

And it kind of brings up a point that we didn't get to mention. Part of the reason that we are advocating for the Bureau of Cyber Statistics and that remains an issue that still needs to be fixed – is to be able to have the data that would send signals to the cyber insurance market, for example, and make that work, and that's not working right now.

So, there's a lot of areas that kind of relate to those executive orders that remain unresolved, and we have work to do on that, obviously.

KING: I think the executive orders are major steps forward, and I don't have any specific criticisms or suggestions, but I think that the National Cyber Strategy will sort of inform the next round. But I'm pleased with the administration. I think this administration has taken this very seriously from the beginning, once we got Jake Sullivan to understand why we needed a National Cyber Director. But I think they've been very active. Anne Neuberger's worked a lot with our allies. Working internationally has been very successful. The administration has been very, I think, forward-looking on this. And just things

like the president a year ago telling Putin point-blank, here's where the red lines are. You know, do not attack our electric infrastructure. Do not put civilians at risk in cyber, I think has been the right approach.

STARKS: My question, by the way, was exactly on –. People could, you know, keep it to an actual question. I always like that when that happens from audiences. I think we're up here next.

VISNER: Thanks. Sam Visner. I'm with the Space ISAC and MITRE, but I'm also an advisor to the commission. This is not a question. I'm sorry about that.

But it's an observation, and I would ask the commissioners to take it to heart. I've been teaching for a number of years as an Adjunct Professor at Georgetown. I've sent a number of my students into the government and a number into the private sector, and I thought that workforce report was excellent, and I was pleased to review it. But I think a part that's going to need more work is, what happens when these people come into government? The young people I've sent into the private sector get interesting, meaningful work.

GALLAGHER: Yeah.

VISNER: A number of the people I've sent into the federal government are asked to continue to do essentially scut work. They're not, in essence, being given an opportunity to use the analytic or technical skills that they've developed, and I think it's demotivating. So once people are brought into the federal government, if, in fact, we think that they have a special capability to offer, they should be given the opportunity to offer that capability as soon as possible, rather than being treated as, "Well, you're 23, you're a GS-7, you're a GS-8. You know, let's wait until you're 39 before you do something meaningful." And I'll stop at that point, but I do hope that we can take that problem on and give these people meaningful opportunities. Thank you.

KING: Yeah, I think that's a fabulous observation, and I suspect that it varies from place to place. If some of your students went into Chris Inglis' office right now, I suspect they'd find they were getting meaningful opportunities. On the other hand, if there are other agencies that are sort of tired and aren't engaged that much, I'm sure what you say is absolutely accurate.

And again, that's really one of the hard parts of this, is it depends so much on the leadership and the attitude of the people. We can pass a perfect law, but if it's poorly implemented or if the leadership isn't committed it's not going to happen. That's a great insight, though.

VISNER: One is going into Chris's office, so I've got –

GALLAGHER: There you go.

KING: Well, let us know and we'll I know a guy, if that doesn't work.

GALLAGHER: Yeah, I'm reminded of something General Petraeus always used to say in the context of counterinsurgency, which is, you know, "rank is nothing, talent is everything." And it strikes me that that applies even more so to cyber.

And your point is all the more important because I think we concluded that even with flexible hiring and pay authorities, you just never, you know NSA, CISA, and DoD they are never going to be able to compete with Amazon, Microsoft, when it comes to salary, right?

KING: But it's the mission.

GALLAGHER: Exactly. It's [the] mission they can compete on. So if you allow young, talented kids to work on a cool mission and test them at the limits of their intellect and energy, well, then you can compete for talent, I think.

STARKS: Sorry – yeah. It looks like the mic is going back there, then we'll come back to the second row.

STAFF: Last question.

STARKS: Oh, no. OK.

GALLAGHER: Sorry, second row.

KING: Two more. We'll be brief in our answers.

GALLAGHER: Make them easy.

MILLER: I hadn't put up my hand, but hi. Thank you so much for having me. Maggie Miller with *Politico*. I wanted to know how the conflict in Ukraine has potentially influenced the work of CSC 2.0, and what we're going to see going forward, just coming from seeing cyber warfare in the field this past year. Thanks.

KING: Well, my first reaction is the dog that didn't bark in the night. When the Ukraine activity started, when the war, the invasion started, I think everybody anticipated cyber was going to be a huge piece, and generally internationally, but also within Ukraine. Ukraine was much more resistant and resilient. They did attack Ukraine through cyber, but it wasn't as successful as anybody expected. So, the first thing we've learned is that you can defend yourself, and that work that we did, NSA did, and others did really helped, I think, the Ukrainians to resist.

The second piece and I can't prove this because it's a negative – I believe that we would've seen more of a cyber intrusion into the West, but Putin is afraid of General Nakasone. I think Putin is deterred, frankly, by the capabilities that we have and by what Nakasone and what NSA demonstrated in 2018 in the midterm elections. So, I think, there's been – now, again, I can't prove that because they didn't attack. My belief is that an attack might've been more likely but for the concern of the Russians that they were at risk, and in that case, I think deterrence has made a real contribution.

GALLAGHER: I'll just make a few related points. One, I do think it enhances the value of our Hunt Forward teams we have. As of August, they'd done 35 hunt forward operations in 18 different countries. I think we have new relationships with Lithuania and a few other countries in Europe. That's all good. I think if you ask people that are involved in that they would say one thing that surprised them positively is just some of the capabilities in cyber that our European allies bring to the fight, and we need to do a better job not only of helping our allies, but leveraging, you know, capabilities they have that could help us.

A third point that may be, I don't know if it's an area of disagreement, but yeah, and my bias is that I think part of the reason deterrence failed on February 24th was because we didn't sort of have a hard power aspect of deterrence. I just think

it's a reminder that, you know, as we talk about cyber, and it's obviously related to hard power, you know, there are broader deterrence questions that are going to require actual guns, bombs, missiles and human beings.

So, put differently, I think a cyber deterrence strategy needs to be connected to an overall deterrence strategy. And that's an area where I think we still have some lessons that need to be learned from what happened on February 24th that could then be applied to Taiwan, in particular.

KING: I tried to get Paul Nakasone's term changed to eight years in the National Defense [Authorization] Act this year, but I was not successful.

STARKS: It turns out we are able to get in just a little bit more Q&A.

COFRANCESCO: Thank you guys for everything you've done. John Cofrancesco from Fortress Information Security. Our company protects the supply chain, more than 40 percent of all electricity production in this country. Our primary concern is the vulnerabilities that we keep buying. Really powerful provisions you guys have put in NDAA 889, but these aren't being enforced. Do you guys have plans to introduce a more thorough oversight over some of the existing supply chain regulations that will prevent the acquisition of Chinese solar cells or Chinese software going into joint strike fighters and things like this?

GALLAGHER: Yeah, the joint strike fighter, I dug into this issue, what was it was like a lube tube or – I don't know–

KING: My nightmare is somebody in Beijing pushing a button and all the bolts fall out of every tank in the American arsenal.

COFRANCESCO: No joke, they turn off the toilets.

GALLAGHER: Yeah.

COFRANCESCO: Not kidding.

GALLAGHER: But in the F-35 example, what we discovered in this particular case is that part of the reason this went forward is because the initial regulatory or compliance framework goes back to 2003, right? And our approach to China in 2003 was dramatically different than our approach to China in 2022, right? We were still laboring under the notion that, if we could integrate China into the global economy, they'd become a responsible stakeholder.

So, we're having to go back, and that program's been going on for two decades – and figure all this stuff out. So that's not a good answer to your question, but –

KING: But you're right. Supply chain is a huge problem. Because all it takes is one chip or one valve or something in a very, as you know, a product that has 100,000 pieces.

COFRANCESCO: You guys have done, actually, a good job of getting stuff, even shockingly, and it's awesome. But then getting the executive branch to apply –

STARKS: Yeah, the enforcement piece is what he seems concerned about.

COFRANCESCO: So I'm hoping that you guys will have some regulatory oversight –

KING: Well, here's what I would invite you to do, is to be in touch with us about where you see the shortcomings, so that we can know where to direct our energy.

GALLAGHER: The dilemma, as indicated by what's on Angus' tie, which is the Constitution, is that it's a different branch that ensures the laws are faithfully executed.

So we have to do oversight so that they ensure it, yeah.

STARKS: And we have to go to the last question.

ALMS: Hi, guys, thank you for taking the time. My name's Natalie Alms. I'm a reporter at *GovNext*. You've mentioned those hiring and pay flexibilities at DoD. Some, including CSC 2.0, have recommended that Congress extend those to other agencies beyond DoD and DHS.

So, I was wondering what you guys think of that idea.

GALLAGHER: Well, as I indicated before, I would want to understand, I think it makes sense to me, but we also want to understand why DoD is not, sort of, using those aggressively. But the idea still makes sense. And I, you know, right now, it's a yes; let's expand it, because we need all the talent we can get. But we have this problem where we don't understand why DoD isn't using that.

KING: I agree with Mike. But before we close, I want to acknowledge Patrick Murphy and Frank Cilluffo and Samantha, who are all members of the commission. We're now on something like meeting number 53. And these were substantive one, two, three-hour meetings and really – and high level of attendance. And then our executive director, Mark Montgomery, in the back, who has been absolutely brilliant. The smartest thing we did, Mike and I agree, was to hire Mark, and has done so much to assemble a really all-star staff and, you know, take a look at this. This is a major piece of work right here. And the original report is something that we're very proud of, and a lot of it is attributable to Mark and the staff.

I just wanted to get that in.

STARKS: Yeah, well, I want to thank the –

KING: That's in lieu of a pay raise, Mark.

STARKS: So thanks, everybody, for attending. Thanks, Congressman. Thanks, Senator.

If you want to read more, cybersolarium.org is where you can see all these things.

KING: Thank you all.