

October 22, 2025

*Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)*

*Moderated by Maggie Miller*

*Introductory remarks by Dr. Samantha Ravitch*

**RAVICH:** Welcome, and thank you for joining us today at the Foundation for the Defense of Democracies. I'm Dr. Samantha Ravich, CSC 2.0 advisor and immediate past chair of FDD's Center on Cyber and Technology Innovation [CCTI]. It's Wednesday, October 22, and whether you're joining us live or virtually, we're pleased to have you here for this conversation.

When the Cyberspace Solarium Commission was created, our charge was clear: to prevent a major cyberattack of significant consequence to the United States. We came together, Republicans and Democrats, policymakers and practitioners, because we recognized that cybersecurity is national security.

The threats we face today reach into every corner of American life. Defending against them demands more than technology or new authorities. It demands a strategy rooted in layered cyber deterrence, shaping behavior through norms and diplomacy, denying benefits to adversaries through stronger defense, and imposing costs when they cross the line.

But deterrence only endures when it is underpinned by resilience, our ability to absorb, adapt, and recover faster than the adversary can disrupt. That resilience is built through persistence, public-private collaboration, and a shared national commitment to staying ahead of the threat.

Moving our country, both our government and our citizenry, towards a mindset of resiliency won't be easy, but it is imperative. Five years after the commission released its flagship report, we have seen real progress: new offices, new authorities, and investments reshaping how the United States defends itself in cyberspace. But as this year's assessment shows, the work is far from finished.

With that in mind, today's panel will explore the latest findings of the report. We are joined by three former members of the commission and the lead author of this year's assessment.

So, let me introduce: the Honorable Mike Gallagher is co-chair of CSC 2.0 and served as co-chair of the commission. Before he joined Palantir Technologies as the head of defense, Mike represented Wisconsin's 8th District from 2017 to 2024. A former Marine, Mike brings the same candor, intensity, and sense of mission to cyber policy that defined his military and his congressional service.

The Honorable James Langevin is the newly appointed chair of FDD's CCTI Board of Advisors. It is a privilege to hand the baton to Jim, a trusted colleague whose integrity, expertise, and lifelong commitment to the mission are unmatched. While in Congress, Jim represented Rhode Island's 2nd District for over two decades and has long been one of Congress's true champions of cybersecurity, founding the Congressional Cybersecurity Caucus and serving on the commission.

Jiwon Ma is a senior policy analyst of FDD's CCTI and the lead author of the last four of CSC 2.0's annual assessment reports. Through her analytic rigor, Jiwon has helped shape these reports into a trusted benchmark for measuring the nation's progress in cyber resilience.

And Rear Admiral Mark Montgomery is senior director of FDD's CCTI and director of CSC 2.0. He served for 32 years in the U.S. Navy as a nuclear trained surface warfare officer, retiring as Rear Admiral in 2017, and was the executive director of the commission. Mark has been the engine behind both the commission and CSC 2.0. His energy, his leadership, and discipline continue to prevail the commission's mission forward.

Moderating today's conversation is *Politico* cybersecurity reporter Maggie Miller. Maggie has spent almost a decade covering cyber policy, both at *Politico* and during previous positions at *The Hill* and *Inside Cybersecurity*. Maggie, welcome back.

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI),  
Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

Before we begin the discussion, we'll turn to a short, pre-recorded conversation between Mark and Senator Angus King. Alongside Mike, Senator King was co-chair of the original CSC and is co-chair of CSC 2.0. Unfortunately, he was unable to join us in person today due to the ongoing shutdown. Senator King is a member of the Senate Select Committee on Intelligence, the Armed Services Committee, the Committee on Energy and Natural Resources, and the Committee on Veterans Affairs. Senator King has been both a source of insight and inspiration. His candor, his humor, and deep sense of duty remind us why leadership grounded in integrity still matters.

Before we keynote here – watch the keynote remarks from Senator King, 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.

Now over to Senator King, so run the reel. And thank you.

(VIDEO PLAYS)

**MONTGOMERY:** Hey, good afternoon. You know, I'm here with Senator Angus King, the original, O.G. chairman of the Cyberspace Solarium Commission. And, you know, we have a great opportunity here, sir. We're releasing the fifth of our annual assessments, you know, going back to our original release in March of 2020.

This assessment is different than the last few. It wasn't all, kind of, rainbows and unicorns. What did you think when you looked at that assessment?

**KING:** Well, it was really frustrating, Mark, because at a time when we're seeing the cyber threat increase dramatically, we're unilaterally disarming, and we're not making the progress that we ought to make. I mean, I could run through a whole series of things, but just a little thing like, one of the initiatives that was proposed in the Solarium was sort of a UL labeling of objects in your house that are all connected to the Internet. And that went – there was a long process that went on in the White House.

I remember going to meetings with industry. It was really moving forward. And this administration, basically, as near as I can tell, canceled it. And yet all of us now have, you know, two or three, sometimes as many as five or six, internet-connected devices in our house, each one of which is a security threat and an opportunity for malevolent actors to get into our personal lives, our bank accounts, and all those kinds of things. So, there are all kinds of examples like that.

CISA [Cybersecurity and Infrastructure Security Agency] at the beginning of the year had about 3,300 employees. Today it's 2,200. So, it's lost about a third of its people, and it's lost some really good people, some people that were experts and developed a lot of relationships.

The third thing that bothers me is that the administration is talking about offloading cyber responsibilities to the states and localities. They're not equipped to do it. I mean, the beauty of the CISA idea was to act as an interface between all the expertise that's available within the federal government and the private sector, and share that with the individual states, some of whom have pretty sophisticated operations, others don't. And so, EPA backing off of water cyber protections, SEC backing off of requiring companies to report cyber incidents – all of this essentially, as I say, is unilateral disarmament in the face of an increasing threat. Sorry to make a speech, but it's pretty frustrating.

**MONTGOMERY:** No, I mean, you and I signed a letter up front, an executive summary up front, where we noted that there was a – it was a regression from the norm.

**KING:** Yeah.

**MONTGOMERY:** It was, you know, either a stalling or a slipping in a lot of areas, and –

**KING:** It would be one thing if we were winning.

October 22, 2025

*Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)*

*Moderated by Maggie Miller*

*Introductory remarks by Dr. Samantha Ravitch*

**MONTGOMERY:** Yeah.

**KING:** But the threat is getting worse.

**MONTGOMERY:** One other thing you mentioned is state and local. You know, that's done just as the State and Local Cybersecurity Grant Program expires. So, we push responsibility and yank resources. And you know, we got to get that reauthorized.

**KING:** And the other piece that I think is a little more subtle, but – and I saw the evolution of CISA's relationship with the states from the beginning. And the states were frankly suspicious at first. They didn't want to share information, they were afraid of federal engagement, you know, getting involved with their election systems. And I saw over the years it was – the trust was built, same thing in the private sector. And trust is the key to any relationship. And now the trust is diminishing. I'm hearing that states don't want to work with Washington. They're not – they don't trust what's going on. And that's a sort of intangible, but a very real loss.

**MONTGOMERY:** And the Multi-State ISAC [Information Sharing and Analysis Center], which was the vehicle that was used to help with not just election security. And I know that's what caught the administration's eye, but it was the boring security. And that's been detached –

**KING:** Just the mechanical, the mechanical stuff, and here's another one: the ambassador-at-large at the State Department. One of our major recommendations, or first, one of our major realizations was that this is an international problem and it affects every country, every society. And there's a commonality of interest. And that commonality of action could be much more effective.

For example, if we have sanctions and say, you know, this bad actor from Russia can't go to New York or Miami. It's also more powerful if he can't also go to London or Nairobi or Canberra. And that's been essentially dismantled. I mean technically it still exists – they haven't appointed anyone to replace the leader, the ambassador-at-large, Nate Fick. And they've changed the reporting requirements. And again, it just – it's puzzling because this is a very real attack that's going on in this country every single day.

**MONTGOMERY:** Now I appreciate that, and I know you didn't just bring up Nate Fick because he's a Mainer and a Dartmouth grad. But you know, you're right. And well, look, I know there's some language going through in the State Department Reauth[orization]. I'm hoping, again, not necessarily the language gets followed, but that the Congress comes in again hard on that job.

**KING:** Yeah, but one of my observations in being in this business for some time is that implementation is as important as vision. So, we can have a good idea, we can put it in a statute. In fact, the Bureau [of Cyberspace and Digital Policy] in the State Department is in statute. We already created that position and so we shouldn't have to come back and re-legislate it. They ought to do it because it's important.

**MONTGOMERY:** Thanks. Speaking of implementation, one of the most important recommendations, I think at the Solarium Commission, was the National Cyber Director. And you know, you deserved a lot of the credit for getting it done and sent it along with your partner [Sen.] Mike Rounds, and then Jim Langevin and Mike Gallagher in the House. You know, you've met with Sean Cairncross. What do you think? You know, what's his likelihood of success or what do you think he needs to do over the next couple years?

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

**KING:** Well, I think his heart is in the right place. I think he has a good knowledge base. I think he's – he understands the threat. I handed him, when I met with him, a printout from ChatGPT of the problems with cybersecurity that this administration has created. I don't know if he – he put it in his pocket. I don't know if he's looked at it again. But as I say, I mean – but the question is, does he have the support? Does he have the authority? Will [Secretary] Marco Rubio listen to him? Will, you know, will the people, will [Secretary] Kristi Noem listen to him in terms of the organization of CISA? And that's the question. I don't want that position to be just a nominal, honorary position.

**MONTGOMERY:** I agree with you. I think he has one advantage that two very good leaders had before him that they did not have – that Chris Inglis and Harry Coker didn't have – which is I think he has a, he has that relationship with the chief of staff, allegedly. And I think that that really is important. As you said, relationships matter. So, I'm hoping that this allows the NCD to get that kind of groove that you and I and Samantha Ravich and others wanted, which is, you know, that access to the front office.

**KING:** Well, and the other thing he can do, I think, is sort of take an inventory of what our capabilities are, what the gaps are, and you know, what gaps have been created, frankly, in the last 12 months. And then it gives him a roadmap of where we got to go.

**MONTGOMERY:** OK, so next year, when I schedule our next update, and it's not going to be the first week of October for fear of being in the middle of a shutdown, I'm going to have to get a little smarter about that – in the last couple, in the first two weeks of September. What are you hoping that a year from now we're commenting on having gotten done?

**KING:** I'm hoping that, number one, we're commenting on the recognition within the administration that this is something that needs to be attended to, and that some of these reversals of policy have been addressed. Now, I will say we've been pretty negative so far. This administration seems to be more interested in developing a deterrence strategy than the prior administration. And [Sen.] Tom Cotton and I have an amendment in the National Defense Act on that issue. I call it the King-Cotton Bill.

But anyway, the idea is to compel, if you will, as part of the National Defense Authorization, the development of an assertive cyber deterrence strategy. My argument throughout the commission, as you know endlessly, was we can't patch our way out of this problem, and that our adversaries have to understand that if they attack us in cyberspace, there will be a response. It may not be cyber. It may be anything else, sanctions or whatever, but they have to realize they're going to pay a cost, because right now there's no cost. They can attack our infrastructure, attack our elections, attack, you know, critical infrastructure throughout the country, and everybody says, well, we'll respond at a time and place of our choosing. Well, we still haven't responded to the Sony hack.

**MONTGOMERY:** Yes, sir.

**KING:** And so, I'm hoping, and believe, working with Tom [Cotton] that this administration understands that principle and will develop a declaratory cyber deterrence strategy. Just having the capacity isn't enough. You have to say you have it, and you have to indicate the willingness to use it.

**MONTGOMERY:** And the adversary has to believe it.

**KING:** That's right.

**MONTGOMERY:** And that's so, sir, you were consistent on that, I have to say, from meeting one to meeting 50.

**KING:** Consistent is another word for boring.

**MONTGOMERY:** No, no. And that and organization as policy. I mean, I have a list of four or five King-isms.

October 22, 2025

*Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)*

*Moderated by Maggie Miller*

*Introductory remarks by Dr. Samantha Ravitch*

Sir, listen, you've been a leader on cyber over this, the eight years or nine years now of this trip you and I have been on, and I think you've gotten a lot done. We have more to do. I know you feel that way. I feel that way. Jim Langevin feels that way. Jim took over chairmanship of my center at Foundation for Defense of Democracies, and he's running his center at Rhode Island College. So, we're all in this game, working hard. I look forward next year to seeing you in person during the assessment.

**KING:** Thank you, man.

**MONTGOMERY:** Thanks.

**KING:** Good work, Mark. Thank you.

(APPLAUSE)

**MILLER:** All right, well, I think that was a really great way to kick off the panel. Mark, I have to compliment you on your interview skills with Senator King. You really went around the horn right there.

But to kind of start from the top point down, I want to start with our author of the report that we had this year. As Senator King pointed out, as Mark pointed out as well, this report did see regression in a lot of the recommendations being implemented. A "regression to norm," I believe was your quote, Mark.

So, can you talk about how you assessed how each recommendation did this year and where you think we saw the most backsliding, generally?

**MA:** Sure. So, thank you so much for joining us today. It's always great to see you.

So, over the years, I've noticed that it's become a little bit more difficult to parse out just the cybersecurity policies from the security issues that affect all of us every day. And what I have noticed is that there has been endurance, but the national resilience is also eroding at the same time.

So over the last four years, when I do assess these recommendations, I am looking at whether there have been executive action taken, where appropriate, whether there has been legislative action to mandate – sort of like institutionalize the things that we want to build, and also whether there have been appropriations to just consistently fund and build up the things that we're building, and in many areas that have backslid, I would say it's either one of the two. At least two of those things have failed. I know that that is a strong language, but I think that we haven't been doing well in terms of preparing. We're good at standing up the things – like the ONCD got stood up. We gave it the funding, we brought the personnel, but then we didn't consistently think about what it needed as it grew. So, I think that was why one of the top five recommendations and the top one we listed was to provide more authorities to the ONCD.

And I think generally, I think people in this room are all aware that we're really backsliding on our efforts in cyber diplomacy and how we have really treated our cyber workforce. So, without the manpower to do the mission and also without the vision to sort of prepare our allies and partners while we take our own cyber assets and protect them over time in the domestic area, I think those are some of the really big struggles that we have seen in the report.

**MILLER:** Mark, do you have any follow up there?

**MONTGOMERY:** Oh no, the regression to norm is mostly manpower. I mean, I'm very frustrated with the reductions in CISA. Look, I don't think everybody, and I agree with the Trump administration that CISA was not – that everything they were focused on was the right thing to be focused on. And I think any administration would have come in and said, "I need to change the focus." That's OK. But I would also say it's kind of hilarious to hear senior leaders say, "Yeah, this 33 percent cut in my workforce is – I'm just as efficient as I could have been otherwise."

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

And that's just not – I've never, 35 years in the military, I never had a subordinate come up to me and say, "Sir, what I really need right now is a 35 percent reduction in workforce." I heard quite the – in the kind of challenging environment we're in, like Senator King said, with a growing threat from China and Russia, with a China that's doing operational preparation in the battlefield against us, we need to have the right people. I agree with that. But we need to have people, and I think the – that reduction hurts. There's a few other areas, but to me, that's the one that stings the most.

And I just wish they'd get over it, say, "We made a mistake. We're putting the money back in and getting it." I'm really looking forward to Sean Plankey getting in charge of CISA because I think he is a mission-oriented leader who will take responsibility for his actions.

**MILLER:** And I'm glad you brought up CISA. That's been a big focus of my reporting this year. Well, always, but this year especially. As Senator King said, there has been about a third reduction in staff since January, and of course, in the shutdown, as we are seeing with many agencies, many more are furloughed. We have around 900 still working.

So, having, you know, previously served in congressional roles, Congressman Gallagher, Congressman Langevin, you know, what's your take on, you know, how the administration has approached CISA? And where do you think they can go to kind of put CISA in the best place to defend our nation's critical infrastructure? And we'll start with you, Congressman Gallagher.

**GALLAGHER:** Well, I think with all these things – first of all, the caveat being, when Mark asked me to be on this panel, I said, "Mark, I now have a real job. I'm not immersed in these things." I now admire [CSC 2.0 advisor] Tom Fanning for his ability to have a real job and also serve on our commission, because I am not smart enough to do both. So, my knowledge is stale.

I would, however, say, like, it is too early to be definitively judging how things are going. I mean, like, key administration positions have just gotten confirmed, right? We could have a whole panel about how the Senate confirmation process is totally jacked up, and like, if the president, regardless of their party, deserves to have their team on the field. So, I don't know how many days Sean Cairncross has been in the job, but it's like not that long. He's phenomenally talented. He's getting after it. Like, I think he has an opportunity to get that position right. When it comes to CISA, I emphatically agree with what Monty said about Sean Plankey. Like, he has a ton of energy, a ton of ambition. I think he can revitalize and reimagine what that office does.

So, I just would say, like, we – there's a little bit of time that needs to elapse before we pass definitive judgment on all these things.

I'm also – and by the way, I was a co-chair of this commission. I fully stand by the recommendations. I think one of the top three things coming out of our initial report is that CISA – we need to elevate CISA's authorities. It also needs to be able to attract world-class talent, and we've given the Pentagon, we've given other agencies all these flexible authorities to hire talented people from the private sector, not in a full-time role, but in, like, Cyber Excepted Service. We're still not using these authorities sufficiently and getting creative with those authorities.

But I'll tell you, now with the perspective of being in the private sector at a technology company, the gap in talent is larger than I understood when I was in government. I mean, it's very difficult, if not in some cases impossible, for even our leading government agencies to attract these genius 23 year olds that work for me at Palantir. Like, we have to come up with a different model. I mean, you can compete on mission, but you can't compete on salary, and that's just, that's something I didn't have a full appreciation for until I got out of government and was fully immersed in the private sector, if that makes sense.

**MILLER:** And just – just before we go to you, Congressman Langevin, to talk about CISA, I just want to press you on that.

October 22, 2025

*Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)*

*Moderated by Maggie Miller*

*Introductory remarks by Dr. Samantha Ravitch*

**GALLAGHER:** Yeah.

**MILLER:** I mean, we have seen so many cuts at CISA, but also many other agencies, you know. Are you worried that that, sort of, amount of cuts might disincentivize people further who want to work in cyber for...

**GALLAGHER:** Well, listen, I mean, you mentioned the government shutdown. We – obviously, I hope we can find our way out of a government shutdown. Like, you can't just stay shut down forever.

More than anything else, what has concerned me for the last decade as a staffer, as a member of Congress, even now as a private citizen, is just the unpredictability of our budgeting process. You know, in the military domain, how much money have we lost? Tens, if not hundreds of billions of dollars due to continuing resolutions, budgetary unpredictability. It's why, you know, in my last year Congress, I was working with other members to try and put an end to shutdowns entirely. There's legislation on the table right now that would allow us to get out of this constant shutdown cliff game we play, right?

In the state of Wisconsin, if you don't pass a budget, the government doesn't shut down. You just sort of revert to the previous year's level. So, we don't actually have to play this budgetary chaos game. So obviously, like, we want to get out of that and have a more coherent process for funding our government. But that's a congressional problem, right? Like, Congress needs to reform itself.

**MILLER:** And speaking of Congress, Congressman Langevin, having served on the House Homeland Security Committee with oversight of CISA, where do you judge what's happened there this year, and where we can go in the next year to get it sort of at its best?

**LANGEVIN:** Sure. Well, first, before I get to your question, I want to thank you for moderating, Maggie, and I just want to take a minute to thank FDD for hosting this and for the support, the continued support on the CSC 2.0 and making sure that we have eyes on the implementation of the Solarium recommendations.

And I also want to thank Dr. Samantha Ravich for her outstanding leadership at – leading CCTI Board and honored that she passed the torch to me. And she's been an early cyber pioneer. And of course, the other, the downside is, you know, being from New England and loving the New England Patriots, we have a saying that, you know, you don't want to be the quarterback that comes after Tom Brady, right?

So that's kind of how I feel. And she set a high bar, and I hope to continue the high standards that she set at CCTI.

And then I would just, finally, I want to thank Mark Montgomery for the amazing leadership as our executive director of Solarium. It was a Herculean effort to kind of herd the cats, keep us on mission, on focus, and it really did take a Navy admiral to make sure that we got the ship across the finish line. So, Mark, thank you again for your leadership of Solarium.

Great being on the panel today with Jiwon and my colleague, Mike Gallagher.

To your question about CISA, I'm deeply, you know, concerned about the level of cuts. Mark hit the – you know, right on the, on the mark there with – you know, you have to have the people doing the job, and it's really important that you continue to build capacity there. And you know, CISA was growing, and it was on pace, so I don't how they're going to recover from that and do the important aspects of the mission. But I'm hopeful that it's, you know, Congressman Gallagher, my colleague, pointed out that OK, you know, we're still getting the team in place. They want their people in place. I'm willing to give the administration the benefit of the doubt that we are going to, you know, build that capacity and we are going to continue the mission.

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI),  
Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

You know, one bright point that I'll point out that I see is the executive order that was put in statute on threat-hunting on government networks that it gave to CISA. Even though it was in the previous administration's cyber executive order, it really wasn't implemented, or at least, it started until the kind of closing days of the administration. We were too slow to adopt that.

This administration is actually, as I understand it, implementing that – the threat-hunting so CISA can actually go on other government agencies' and department's networks, and they are doing threat-hunting. So, you know, if my information is correct and that is happening, that is a positive that I'll chalk that up, you know, in the positive column for this administration. And you know, again, for it to be effective in securing – and I'll put it in these terms, the administration has talked a lot about securing our borders. Well, it's important also to secure, not only physical, but our digital borders. And that's what going threat hunting is doing, it's securing our digital borders within the government, and then hopefully it's going to spill out into, you know, helping the private sector do threat hunting on their networks.

**MILLER:** And another issue – and again, thank you to Senator King for teeing us up so well, that I know you talked about with him, Mark, was the State Department's Cyber Bureau, which we've seen a lot of changes to this year as part of the larger reorganization of the State Department. We've seen it split into three different bureaus, one of emerging threats.

You mentioned in your conversation with Senator King that there is legislation in the House, House Foreign Affairs, with the State Reauth bill that could build up some of its authorities, fully establish the Bureau of Emerging Threats. Where do you see that going in the coming year? And also, you know, we still don't have an ambassador in place, you know, what are you hearing on that?

**MONTGOMERY:** So, I, first, I think Representative Mast in the House Foreign Affairs Committee did a good job writing up legislation that acknowledges what the administration wanted, which is an emerging technology shop and assistant secretary, and preserve the cyber diplomacy. I think that's the right answer. I hope that can carry through in conference and become the final language.

Look, I agree with what Senator King said which is, hey, we already had a law, just follow the law. But you know, elections have consequences, and this administration wanted to change it. The normal way would be to write up some legislation, send it up to Congress, have Congress then execute that legislation and make the changes. That's not how it happened. That's OK, though. I mean, I agree with Mike that you know, when you have an election, you're going to have perturbations, that's democracy. And this is one of those perturbations.

And what I do like is Representative Mast said, "I got it," and got this legislation – he and Representative Keith Self, who has a subcommittee that handles cyber and Europe – said you know, "We're going to take action on this," and they went ahead and got legislation done.

This is going to save us a year in getting to an easily authorized and appropriated solution. If the SF – Senate Foreign Relations Committee allows this legislation to go through without too many modifications and then the Reauth actually carries on the NDAA [National Defense Authorization Act], which I think is highly likely, not because of this, but because of other things in that bill.

So, I think there's a path to success here. And this is actually how democracy works, right? Election happens, I want something done differently, again, the exact path, not normal, but the end result could be within one year of the administration taking over. They had the lineup they want.

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI),  
Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

As for who is going to run it, you know, there are names floating around for both those billets, but I think without them actually existing, I think that's probably why the administration's holding off. They know this legislation's out there. I would not be surprised if – that these billets take all the way through the NDAA conference before we see names pop up for placement. Because they're fundamentally different descriptive billets than the current ones that exist in law. And you can't nominate somebody for a billet you wish existed. You have to – in this case, since you need the compliance of the Senate, you have to nominate them for the billet that does exist.

**MILLER:** And, Jiwon, you know, in terms of the recommendations around the State Department, those were some that regressed this year because of the reorganization, but would you say, you know, what Mark's outlining if, you know, the House was able to push through that legislation, become law, would we see those recommendations progressing next year?

**MA:** Yeah, and I think we've seen that over the years too. So, if you look at the board over there, we see that several of the colors are moving up and down, and I think that even from previous reports, we have seen recommendations that went backwards but then jumped up later on. And I think that's definitely possible.

And I also believe that these are not mistakes that, you know, will forever just remain as mistakes. These are things that we can fix, and I think that's why these recommendations are great, because as long as we are aware of what is actually happening that we need to fix, we can actually address those issues. So, yes, I am optimistic that that will be the case.

**MONTGOMERY:** If I could pick up on that, a good example is cyber capacity building, where we had a good program going, especially for Costa Rica and Ukraine with the USAID kind of – you know, dropped the grenade in the tank and closed the hatch – it went away temporarily. But the Costa Rica one's back, and I think the Ukraine one's coming back, and we just did a short report on Ukraine. I came back from a couple of weeks there. I will tell you, our cyber support to Ukraine – cyber capacity support to Ukraine – A, helps them hold off Russia, and that's not a small thing. And we spent \$60 billion in US weapons, spending \$135 million in cyber seems like a pretty good deal to help keep the electrical power grid up.

The other benefit is they share back with us the fingerprints – the digital fingerprints and the tactics, techniques, and procedures they're seeing there with our intelligence community, and that has real value.

And I've seen the administration start to pump the money back into that, so – you know, this kind of gets at what Representative Gallagher was saying, which is that as the right people get in the right positions and can see the right thing, some of the right stuff gets restored.

That's not everything, but in cyber capacity, but I could easily see what was a regression this year, pop right back up next year into that, if this continues. And there's a couple of ifs in there.

**GALLAGHER:** Can I make an obvious point? My goal is not to be like a contrarian on this thing, my goal is to just like not, you know, reveal my ignorance, which is hard to do. I'm not sure we adequately paid enough attention to this in the original report, which is to say like all of this could be green. It could be dark green, right, and yet, deterrence in cyberspace could be getting worse if not actually connected to conventional and strategic deterrence.

And I think the analytical mistake we often make in the cyber world is to consider its own universe, right? Like if it is not meaningfully integrated into a concept of how you make your enemies scared of you, then like, it does not work, right? And there, I think, you have to credit the current administration for restoring deterrence, at least in key regions, right, like the Middle East. I think it's fair to say that the president's willingness to use actual kinetic force helps us in the cyber domain. So, my only point is that these things can't be disconnected from each other. Monty, now you can push back on that.

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

**MONTGOMERY:** And I remember you...

**GALLAGHER:** This is an Angus King thing, it's like you know, every once in a while, shut the lights off in Moscow.

(LAUGHTER)

**MONTGOMERY:** And those – I see there's seven or eight Committee – some of our staffers here, they'll remember that routinely, he said, "Well, Mark why can't we just attack something, you know?" And you're like, "Sir, it doesn't work that way."

But you're right – you know, you did a pretty famous deconstruction of integrated deterrence as a concept when you were chairman of the Select Committee on China, but no, I think you're right. And that's what I was saying, it is a penny wise and pound foolish to not put that cyber money alongside the other money. And I think we're starting to see that come back. And this administration – DOD's never suffered, I have to say. If there's one trough that has been full it's DOD's and the Reconciliation Bill puts quite a bit more in there, especially oriented towards INDOPACOM. I'm not sure how they're going to spend it yet, but the money's in there.

And of course, Mike, you're really making a deep state argument for the Cyber Force, and I appreciate...

(LAUGHTER)

**GALLAGHER:** Well, to be clear – I'll shut up after this...

(LAUGHTER)

**GALLAGHER:** ...is my critique of integrated deterrence is that nothing can substitute for hard power. If you don't get the conventional balance of hard power, right, no matter how many non-military instruments of power you integrate into your theory of deterrence, it's like, you're not going to actually produce peace on the world stage.

**LANGEVIN:** Yeah. And maybe we could tie it back to the report. When we are working with, for example, Ukraine, and this is all public, right, and other partners and allies, we are defending forward. So, we are – that goes with integrated deterrence, it is denying benefits, and it is imposing costs. You can think about that. By denying benefits, we've helped Ukraine harden its systems. We then benefit, as Mark mentioned, back from that information. We see what the Russians were up to, what things they were planting on critical infrastructure, for example. We can then take that back home to harden our critical infrastructure.

So again, we are denying benefits and making us more resilient, and we're, in a sense, imposing costs because it's like when we're in Ukraine, it's like we turned down the lights, if you will. We've earned all of those Russian tools that they spend, you know, state treasure, in time and effort getting into those systems. And then it's all gone and, you know, they're useless, in a sense. And so, that is imposing costs. All that money was burned by – that the Russians had spent trying to get in there, and then we can help Ukraine harden its systems. So again, brings us back home to that layered deterrence and denying benefits and imposing costs. We want to see continue to see that and hope this administration will.

**MILLER:** Yeah. And I'm going to take back the mic just for a second and then give it to you for a second, Mark, because I want to ask you about the Cyber Force, and I know you can go on about that for a long time.

**GALLAGHER:** Oh, gosh. There goes the rest of my afternoon.

**MILLER:** I know. I'm going to ask you maybe your elevator pitch.

(LAUGHTER)

October 22, 2025

*Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)*

*Moderated by Maggie Miller*

*Introductory remarks by Dr. Samantha Ravitch*

**MILLER:** Where do we stand on this, in terms of where Congress is? I mean, we have a study in the NDAA. We have a couple members of Congress, bipartisan, that are behind it. But that is actually something – a positive note in this year's report, that U.S. cyber forces remain strong but needs to be reformed, more resources funneled in.

So how would the creation of a cyber force help to push that forward?

**MONTGOMERY:** So, you're right. In his final death blow to the system, Representative Gallagher dropped some legislation that got us a study. Look, the study – I'll be honest with you. The study, in my mind, was if the presidential election had gone the other way, I thought the only way we could convince Harris, or Biden administration at the time, was to just run them down with, like, this was going to be done by the National Academy of Sciences or something and just, you know, just kind of wear them down over two or three years.

It's obvious, right, that our force generation is broken. Mike wrote the front piece with me on a report on that last year with Dr. Erica Lonergan. And then we did a new one this year on how you do it.

Look, I have a total different theory with the Trump administration, which is we all know, you know, the line – and I've used this line with President Trump, that, you know, one president created two military services. That was George Washington, the Army and the Navy. Who can be the second? Donald Trump, with the Space Force and Cyber Force. You should drop the mic and walk out of the room.

But realistically, the enemy's helping me here. I'm not too worried. The adversary's pushing, pushing. The people we want to generate forces – the people you want to recruit into the Cyber Force are not the same people that I want as SEALs or infantrymen or even surface warfare officers or pilots. It's a different cut and it's a different mix of military-civilian, it's a different pay scale, it's a different ability to go in and out of government. All these things are different. And you start at the e-gaming lab and the robotics lab and the chess club, not at the basketball and football and soccer locker rooms, like you do for the rest of the military.

So, we will get a Cyber Force. I hope we do it without failing otherwise. I hope we do it because we recognize it's the right thing to do. But we'll get it. And I appreciate Mike's leadership on that. Also, Morgan Luttrell was strong, Pat Fallon, Representative Houlihan, Senator Gillibrand. This has a wide swathe of political feeling in the House and Senate, but people who study this issue, bothered to read the reports and the write-ups by the individuals who supported us on this, made the right decision. We're going to get there. I think we'll probably get there slightly quicker in a Trump administration than a Harris administration, but that's, you know, neither here nor there.

**MILLER:** And Congressman Gallagher, now that you're out of Congress, one, this was something you had pushed right before you left, but two, you know, from the private sector perspective, you know, how do you think a Cyber Force could kind of help to hit back at some of our, I guess, enemies, given that the private sector is so often the target?

And as a follow-up, we have seen a lot of leadership changes, well just generally, you know, with a new administration coming in, but with the head of Cyber Command at NSA, General Timothy Haugh, and now we're hearing that Lieutenant General Hartman's not going to be nominated. So, you know, are you – do you have any concerns about that change in leadership and how that impacts things?

**GALLAGHER:** Well, I guess more than, you know, whenever we talk about force structure, whether it's in the cyber domain or the naval domain, which is where I spent most of my time in Congress and where Monty is also an expert – it's actually infuriating that Monty's very smart. It makes him very insufferable.

(LAUGHTER)

**GALLAGHER:** I'm constantly asking for advice.

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI),  
Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

I spent a lot of time thinking about, like, the perfect – we need X number of ships or X number of humans in the cyber mission force. More than anything else, I just kind of want the Pentagon to make a decision and move out smartly on it, right, cause we can just spend all our time coming up with different perfect constructs for what the force looks like.

Similarly, I would say, when it comes to NSA and the, you know, eternal dual-hat/don't dual-hat relationship, like, you know, at some point, we've got to just make a decision and move out smartly and get someone competent to execute the decision.

I agree with the way Mark laid it out. I think the basic thrust of what we were arguing was, the geopolitical environment continued to deteriorate, and yet the size of the force stayed the same. So, if anything else, it needed to grow. What the precise number is, I can't tell you, but it needs to be bigger. And again, to get back to the point I tried to make inelegantly earlier, perhaps you need an even more flexible arrangement for getting top-level talent to work in the Cyber Force. The Army right now is experimenting with direct commissions for highly talented technology executives to leverage their expertise. That's an interesting experiment. One of my colleagues at Palantir is part of that experiment. Like, maybe we can do something similar with the cyber mission force, taking advantage of the very generous authorities that Congress has given the department.

**MILLER:** And on a different topic, I want to pivot to you, Congressman Langevin, on the Office of the National Cyber Director. We talked about that a little bit earlier on the panel. You know, we now have Sean Cairncross in the role. I know that you were – well, everyone on the panel was a big proponent of establishing the office. But, you know, now that we're seeing kind of the reorganization of how the National Security Council approaches cyber versus how it did in the last administration, how do you think that the ONCD can kind of operate at the White House, in conjunction with the NSC, and also in conjunction with CISA, now that we're seeing so many changes there?

**LANGVIN:** Sure. That was my number one priority serving on Solarium, is to establish the National Cyber Director in the Executive Office of the President, Senate-confirmed. And it took Solarium to finally get it across the finish line. 10 years I had been working on it and pleased that it's there.

I like the direction that it seems the administration is moving to give NCD more authorities and combining both the NCD role on strategic coordination and focusing on defense, but also the previous administration role of the deputy national security advisor for cyber, kind of combining the two authorities and roles. It seems like that's the direction that they're moving. And so, I think that could be a positive, to have that kind of authority. So, it's kind of to be determined. And Mark may have more to comment on that role. But I think it's so important that we continue to make the National Cyber Directors, ONCD, as robust and strong as possible with the broadest support.

One of the things that we did get through in the original NCD Act is to have budgetary review authority. I wanted it to be stronger, and I wanted it to have directive authority. We didn't get there but that's something hopefully in the future will happen. But basically, it allows the National Cyber Director to look at the departments' and agencies' budgets and comment as to whether or not they're doing enough on cybersecurity and cyber focus, and they can make recommendations to OMB. I would love to see ONCD have the authority to have directive authority to force agencies to do more. But, you know, again, to be determined down the road.

But, Mark, I don't know if you want to comment on that.

**MONTGOMERY:** I agree. I mean, Mike and I both spoke a lot with Sean Cairncross as he came in, and I have a very high opinion. And I think he does – you know, the key thing in any White House job is relationships and your relationship with other senior members. I think he has that.

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

And then I think the other thing is that the – you know, I think this NSC recognizes its job as offensive cyber operations, some international aspects of cyber operations, and I think they're properly, deferentially giving NCD the battle space to manage the very significant defensive issue. And the defense is also about the offensive protection of your defense. So, it's not purely just, you know, building defensive networks.

So, I think it's important. And I think it's important that they provide the guidance to the agencies and that they work with Russ Vought at OMB. We were very lucky that Ms. Young and Chris Inglis were able to get a memorandum of understanding together on the OMB-ONCD role. I hope they can repeat that. I can't believe Russ Vought would ever turn down an opportunity to hear bad things about federal agency budgets. And so, with that data flow coming in from the NCD, I think that would be very helpful. So, this is one of the areas where I'm excited, you know, where I think that this administration has a real opportunity to make a breakthrough. And I hope they do.

**MILLER:** Congressman Gallagher, where do you hope that that's going to go in terms of the NCD and the NSC, given that, you know, as you saw, it was kind of two different entities in the last administration?

**GALLAGHER:** Yeah, my sort of like – you know, I have four kids under five, so everything is like a children's book in my mind right now. My understanding of the history, and push back if I get this wrong, is because of Jim's heroic efforts, we created NCD. We should have just called it "The Langevin" to give him credit. We recruited like the best person ever to be the first NCD, Chris Inglis. Like if, you know, Brett Favre, Aaron Rodgers, and Bart Starr combined into one human being, like that is Chris Inglis in the cyber world.

Like then there was – we didn't anticipate the Biden administration reviving the NSC role for cyber. That sort of clouded whose authorities were where, and then that kind of slowed the progress we had on NCD.

Now, we have this phenomenal opportunity with the new administration, a new person in the role to actually realize the original vision for the NCD. I think the need for it still remains. We need to run the experiment fully. And I am very bullish about Sean's ability to effectuate real change.

**MILLER:** Yeah. Yeah. And I want to go back to the report's author here on private-public sector cooperation. I know that there was some language in this year's report, you know, kind of pointing out that it is really at a breaking point a little bit. It's really been challenging. What did you base, kind of, that assessment on? And, you know, where do we go from here?

**MA:** I see that there have been a lot of reports, as you're familiar with, about the degradation of the legal frameworks that facilitate information sharing between the government and private sector. I have read many articles and spoke to people about how they fear sharing information due to backlash for whatever information that they're sharing.

And I think I also found it interesting that the private sector is sort of filling the vacuum where the federal government is lagging behind. So, we see a lot of philanthropic work to invest in cybersecurity. We see a lot of private companies also investing into organizations. And I kind of see the separation happening. That's really unfortunate because they have so much information, so much data that they could really fortify the federal government and help them shape the strategy. And that was sort of visible all across the board, across the pillars, even in the white papers, especially for the recommendations that focus on supply chain and research and development.

And I think even information like how 2.2 billion dollars of funding for research and development just vanished – none of that. And I think even just from that perspective we're thinking about, that is just one vacuum that the private sector is trying to fill right now. And there is clearly not enough information that is being exchanged in order to understand why we need to invest in these research and development opportunities.

So, I think it's really all across the board. I could point out probably a recommendation in each pillar where it's very telling that the private sector is sort of slipping behind a little bit. So, I think that was just sort of the general consensus.

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI),  
Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

**MILLER:** And this is being put out, you know, we're now three weeks, I think, since the expiration of the 2015 Cybersecurity Information Sharing Act, which you know very confusingly, is also called CISA.

And I wanted to ask you, Congressman Gallagher, in the private sector again, you know, what has been – if you've seen any sort of impact of the expiration of that law. And what are you hearing from other, sort of, cybersecurity professionals on the need for, if not that law, then something similar that allows for sharing?

**GALLAGHER:** Well, I mean, we're not a cybersecurity company, so I haven't seen a day-to-day impact. But, you know, it's interesting. Just general reflections, being in the private sector now, reemphasize what I said before, like talent is everything, right? I mean, it is. There's an absolute war every single day for top-level talent. And it's hard enough that, you know, a leading-edge software company, it's even harder for the government, and we don't make it easy for people.

Other concerns from the private sector? You know, I think as I look back on the report, a lot of what we tried to do in our work and subsequent legislation was to get the government from this, sort of, like need to share, you know, when we call you, you have to give us everything. And other than that, like, you know, just do what we say or don't bother us, to like a proactive – in fact, this is the theory behind the NCD. Like a single person who's proactively engaging with the private sector, even elevated CISA, right? I'm not sure we've had the cultural shift, a complete cultural shift necessary to realize that vision of public and private sector collaboration.

But if anything, and I forget the stat that Angus would always cite, if 85 percent of the critical infrastructure was controlled by the private sector when we wrote the report X years ago, I actually think the role of the private sector has become more critical since then. So, it just emphasizes the need for a lot of the recommendations that we put in the original report.

**MILLER:** Yeah.

**MONTGOMERY:** I want to pick up on – I'm glad Mike mentioned workforce. I mean, one of the things that bothers me the most is the reduction in the funding for a program that Jim and I have been championing for six or seven years; in fact, I helped create about 26 years ago, and that's CyberCorps: Scholarship for Service.

You know, we routinely bring in about 450 kids a year across about 70 to 100 universities and colleges and community colleges who come into government service almost on a ROTC-like program. I think this will be the first year coming up where we basically just maintain the current scholarships and give no new ones. That's a mistake. You know, we need this – I don't know the final number of federal cybersecurity employees you need to have, I know it's going to be more than 450 a year that have either, you know, community college, undergraduate, or graduate degrees. So, we should have kept that program going. It has a very high retention rate, much higher than ROTC...

**GALLAGHER:** Yeah.

**MONTGOMERY:** ... in terms of how many people are there four or six years later. And it brings in talent. It also creates – it helps fund and keep programs at 70 to 80 to 100 community colleges, universities, and colleges around the country that produce students that go work for the private sector as well.

So, it was just one of those things that government did routinely, and we didn't think about, but it was really helpful. So, I'm a little – I know they're studying it. I'm confident the Trump administration will fund it, but they need to do it now so that the national – and it's at National Science Foundation, which is not the number one agency in the Trump administration, but I know they'll come around, and when they do, we need to make sure we do it fast enough that they can fund scholarships for the next year, because scholarships are kind of backed up six to nine months on actual accession, you know? So, we need to make sure we...

October 22, 2025

*Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)*

*Moderated by Maggie Miller*

*Introductory remarks by Dr. Samantha Ravitch*

**LANGEVIN:** ... I want to emphasize that – what Mark is saying – 100 percent, because it goes back to what Senator King said. You know, it really does come down to people, right? You can have all of the laws that we've passed and policies that we implement, but you have to have the people. And things like Scholarship for Service are so important.

In my next chapter, I created the Institute for Cybersecurity and Emerging Technologies at Rhode Island College, and we're educating the next generation of cyber professionals, cyber defenders. We were recently able to get our NSA CAE [Center of Academic Excellence] in Cyber Defense, and we want to have a Scholarship for Service program at Rhode Island College and, again, continue to grow the pie, if you will, of cyber professionals that will work both in government and then, of course, in private sector as well. It's so important to the country's future and to securing our nation's cyber infrastructure.

**MILLER:** Well, on that note, we only have a couple minutes, but I want to give a chance for Q&A. I think we have one right here. Chris? I don't know if anyone's bringing you around a mic. If you want to say who you are?

**PAINTER:** So, Chris Painter, formerly at the State Department. So, I'm going to talk about that particular issue.

Look, I mean, the role of the commission was not to do recommendations that were acceptable to one party or the other, it was what is the best result, right? And with respect to the Office of the State Department, the best result, and the recommendation you made, which was based on actually a Republican bill, [Rep. Edward] Royce's bill, was to create this consolidated system where you brought all of the things together. We had a higher level at the deputy level there. And now what you have now is it being split into three separate sections, where it's at a lower level, which is a recipe for bureaucratic infighting, which the State Department's very good at.

So, the question – not the only agency that is, but is one – so Mark, I'm a little surprised to hear you, like, talk with joy about the fact there's this congressional action that's essentially validating this, rather than saying what is best? And what I want to hear from the panel is, is what has happened the best solution or is what you recommended the best solution, that's something we should strive to get back to?

**MONTGOMERY:** So first, I want to say on the actual Cyber Diplomacy Act, it had the poison pill put in, of, you could put it at the deputy, but then the deputy would make a recommendation of where they put it in that bureaucratic infighting scheme. So, we never did get the Royce bill. So, what I would say is, first, let's acknowledge that bureaucracy wins because that was a State Department technical assistance put in from the Biden administration to say, "We're going to push this down into one of these bureaus."

So, look, in a perfect world, I'd have the CDP [Bureau of Cyberspace and Digital Policy] that's in the Cyber Diplomacy Act at the deputy, mostly cause, like you, I think the State Department is a complete cluster-f, right? And if you put it below the deputy...

**PAINTER:** I didn't quite say that.

**MONTGOMERY:** Yeah, but I know you believe that. And if it goes below the deputy, it's going to struggle between T, E, and I didn't even mention P, but, you know, P could screw this up. We had this exact discussion with Senate staffers about this issue because, you know, I think we all realized the right answer is elevate it above. We all realized that no State Department – the State Department is bipartisan, in the sense that in any State Department, they will work hard to not allow you to dictate stuff to the D-level, the deputy level. So, we'll have to see what happens. What I was saying was my joy is that we're going to fix – we're going to get CDP back up at the assistant secretary level with this, if this bill were to go as is. And now, I think State Department antibodies will try to decrease the value of both of these billets, you know?

October 22, 2025

Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI),  
Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)

Moderated by Maggie Miller

Introductory remarks by Dr. Samantha Ravitch

And so that's why I'm for the bill the way it is, versus where it may end up, or the current system, which is very broken. I think we can all agree. It has as many people as haven't left, right, in the office. So, it's a complicated way of saying, I love perfect. In the absence of perfect, I'm going to grab the best thing for the Office of Cyber and Digital Policy, which I think is an Assistant Secretary at this point.

**MILLER:** Does anyone else on the panel have thoughts before I move on to another question?

**MONTGOMERY:** I think I handled it.

(LAUGHTER)

**MILLER:** OK, all right...crickets. Anyone else in the room? Yes? I think we have a – oh, actually, I'm sorry. I think the mic was already with someone there. We'll come to you next.

**HUNTER:** Thank you. Good afternoon. My name is Joyce Hunter, and I'm the executive director of Mission Critical, which is a non-profit cybersecurity critical infrastructure think tank. I had to write this down because I will go off the reservation if I didn't.

So, given the evolving threat landscape and increasing complexity of digital infrastructure, what strategies are proving most effective not just in planning for cybersecurity resiliency, but in ensuring the effective execution across both public and private sectors? And how do we close the gap between high-level policy and operational readiness?

**GALLAGHER:** Oh. Well, wouldn't doing the Continuity of the Economy [COTE] and stuff, we recommended be a useful step in that direction, Mark?

**MONTGOMERY:** Yeah. It would be.

**GALLAGHER:** Yeah. That's a big one.

**MONTGOMERY:** So, we actually need to plan and exercise for the threat we see, I think is the number one thing, and that will drive the right level of solutions.

I think to get at your thing of, how do you properly organize it, I mean, one of the things we've learned is we're not going to – no Congress that any of us can imagine is going to allow us to regulate ourselves into proper – into success, which regulation has worked. It's worked in nuclear power for cybersecurity; it's worked in financial services.

But that's about where the Americans – American people are comfortable having their nuclear power regulated, having their money, security of their money regulated. They're pretty good with air safety. If they thought about space, they'd be OK with space. But that's about it. And so, what we really have to do is come up with incentive schemes. We wrote a lot of legislation this last year, our FDDA arm did, about incentivizing the cybersecurity of rail, aviation, and ports. Zero of those incentive pieces or provisions made it into the final bill, but it remind – you know, to me, that's the hard work of the current Congress of getting it done. We expect people like Representative Garbarino and others, you know, who Jim and Mike have worked with to get that through.

But I agree with Mike broadly that Continuity of the Economy planning is kind of where you define what work needs to be done in your prioritization.

**LANGEVIN:** Yeah. And I think also, and this is something that Dr. Samantha Ravich has championed, others have championed, of COOP [Continuity of Operations], COG [Continuity of Government], and COTE, and prioritization of, you know, at least, you know, what is your top five things that you need to do in order to get back up and running if you do get hit. And I think that prioritization really needs to take place.

**MILLER:** And I think we have time for one last question. There was someone in the front row here.

October 22, 2025

*Featuring Former Rep. Mike Gallagher (R-WI), Former Rep. Jim Langevin (D-RI), Jiwon Ma, RADM (Ret.) Mark Montgomery, and Sen. Angus King (I-ME)*

*Moderated by Maggie Miller*

*Introductory remarks by Dr. Samantha Ravitch*

**GARDNER:** Thank you. Tommy Gardner, I'm a CTO at HP Federal. I know CISA's done a great job, and I applaud the work done at NIST [National Institute of Standards and Technology] in the cyber realm, and the funding cuts are lamentable. But my understanding was that some of that money that was cut from CISA went to FBI for cyber enforcement, which was desperately needed.

So, could you comment on the balance between the different agencies in a total picture of our cyber capabilities, and specifically with the enforcement side at the FBI?

**MILLER:** You want to take that?

**MA:** From my research, I have noted that the FBI has increased its ability to respond to ransomware and also to work with other law enforcement agencies, whether it's our domestic ones or the ones from international allies and partners. So, it's very clear that they have been ratcheting up their skills.

I'm not sure how the money that is taken from CISA is directly impacting or helping grow the FBI's law enforcement capabilities in terms of cyber, but I do think that you're on the track here in terms of how FBI is growing in that.

**MONTGOMERY:** Yeah, but I wouldn't take a dollar from NIST for anything else. NIST – you and I did a study of this, and with Nick Leiserson, who's here. We thought NIST was 40 percent under-funded through the four years of the Biden administration and the last year of Trump 45, which were the five we looked at. It was consistently 40 percent under-funded. Every executive order ever written or national security memorandum said NIST shall do X, Y, or Z with, you know, there's zero money in executive orders and NSMs [National Security Memoranda].

So NIST was, by the time this administration took over, I think it was about 60 percent under-funded in its cybersecurity division, and that's with about a 25 percent plus-up over those five years, you know, by the Biden administration. So, I'm not saying they did nothing, the problem was the threat, the challenge grew faster than the money coming in.

So, any cuts to NIST are inappropriate at this point, especially the cybersecurity division. And if you need proof of that, there's something called the National Vulnerability Database, and you can read what happened last year and what a sad sack story that was of under-funding NIST and its, the contracting authority it had.

So, from my point of view, NIST should be left alone, and if anything, it should be grown. Even if it means the FBI doesn't get the money that they might have gotten from it. Sorry.

**MILLER:** I want to thank you all for your questions and to our panelists for being here today and thank you for joining us in person and online. For more information on FDD, CSC 2.0, and the latest analysis on these issues, we encourage you to visit [fdd.org](https://fdd.org). And hope to see you again soon. Thanks so much.

**GALLAGHER:** Thank you.

END