Senator King At Aspen Cyber Summit

Betsy Woodruff Swan: Do you have do you have thoughts in terms of the extent to which partisan tensions are affecting the ability to to make American cybersecurity policy better? It looks like you might be muted, so I would check that. Thank you. Do you have thoughts on that? And have you seen any of those, did you see those partisan tensions materialize at all with the Cyber Solarium Commission when it was putting together that first big report?

Senator King: Zero. I don't even know the parties of most of the members of the commission. It never came up. We've had 47 meetings as of last Monday, and there hasn't been a single moment of any partisan discussion or -- I agree with Representative Katko. This is absolutely not a partisan issue in the Senate right now. The action is at Homeland Security, where Gary Peters and Rob Portman are working together. My co-chair was Mike Gallagher, Republican of Green Bay. And so no, that's a non-issue. You know, there are differences over some of the provisions that we're talking about, about whether incident reporting should be in 72 hours or 24 hours or 36 hours, but they're certainly not partisan.

Betsy Woodruff Swan: If you could, Senator, if you could snap your fingers and magically implement one of the, as of yet not implemented recommendations from the Solarium Report, what would be at the top of your list?

Senator King: Well, I'm going to surprise you. There are lots of legislative proposals, and Representative Katko has a great bill in the House on notification. There are lots of them. There are three or four that I have that I'll be glad to talk about. But I think the most important thing is for the Administration and the President to develop a clearly articulated declaratory deterrent policy - deterrent doctrine - to put our adversaries on notice that they will pay a price for attacking us in cyberspace. I think one of the great gaps in our national response has been a tepid or a non-response to these series of attacks that we've seen over the past 15 or 20 years. We can never entirely patch our way out of this. We have to do all that we can in terms of resilience and pen[etration] testing and incident reporting and working with CISA and all the structural changes, all of which are important. But the best cyber attack is the one that doesn't occur. And right now, we're a cheap date in cyber. Our adversaries are not -- they don't really fear

consequences. I think the Russians are starting to figure that out. But I think if I could do one single thing, it would be to have the White House articulate a clear and definitive declaratory cyber doctrine.

Rep. Katko: If I might just talk, can I just follow up on that for just one quick second?

Betsy Woodruff Swan: Sure.

Rep. Katko: And I couldn't agree more with you, Senator. You know, before I came to Congress, I was an organized crime prosecutor. I did some of the most violent criminals in the world that I went after and the only thing bad actors understand is strength. And to follow up on what the Senator was saying, we're not projecting strength in the cyber defense realm. And I came up with the five pillars for cybersecurity. The fifth pillar is just what he articulated and that is, if the bad guys can act with impunity like they did with Colonial Pipeline and Kesaya and the JBS and some of the others they did, and there's no response even though we know who the actors are, we know that China was behind one or more of them. We know that it's China's government doing it. We know that in Russia, they have groups of bad actors that have the imprimatur of the Russian government and we're not responding with anything. The only thing they're going to understand is "we're getting away with it" and "we could do more," so I couldn't agree with you more. There's no deterrent effect right now in the cyber realm. We've got a lot of things that we're talking about and Yvette does a great job with all of this, from the Solarium on down, to harden our systems, make us less vulnerable, but the thing that makes us most vulnerable is not responding an nd there's no question about that, I yield back. Thank you for letting me talk.

Betsy Woodruff Swan: Thank you. Thank you for yielding. I appreciate a use of appropriate Capitol Hill terminology. Thank all of you for this panel. Congressman Clark, what's your view on how the Biden Administration is doing in terms of efforts to deter cyberattacks and communicate to bad actors that don't regret they attack American targets? Would you have a similar view to Senator King that there's there's room for them to do more? What's your sense six months in as far as how they're handling that?

Rep. Clarke: Yeah. Well, you know, this is an administration that had a very short runway, in terms of building out its administration from the job, but I think they clearly

understand, given the volume of attacks on our critical infrastructure in particular that we've had, that they have to get on the ball. I think that's certainly what Senator King and what Congressman Katko has stated about sort of building out an international framework and making sure that, you know, we enter into a new realm of understanding in that space is critical at this time. I have no doubt that the Administration recognizes the bad actors from nation states and what that means for our infrastructure, given the interconnectedness that is the internet and that they will indeed put forth the type of foreign policy initiatives that will serve as a deterrent and also strengthen our ability to react when need be. So I do agree with these gentlemen, but I also know that this is an Administration that is firing on all cylinders, trying to address a number of various implications of these cyber attacks coming from overseas.

Betsy Woodruff Swan: I'd love to pivot a little bit and talk some more about your mandatory reporting bill. One thing I'm curious about, taking a bit of a step back is why you think so many companies don't want to tell U.S. Federal Government entities when they have when they get attacked or hacked or intruded upon? Do you have a sense of sort of why that hesitancy exists and sort of what makes, in your view, this type of mandate necessary?

Rep. Clarke: Yeah, I think that there are a number of different reasons that they've articulated themselves. Number one, being proprietary information about how their companies operate, what makes them competitive and others, you know, fear of repercussions. The other being the connection they have in the private sector with organizations that help them navigate their systems and identify threats and attacks. So it's, I think, a combination of things, fear of market share of affecting the markets should they make public their their attacks and what it could mean to civil society. My bill is important because we've got to build a bridge of trust, and that's that's so very important. The more that we understand about where these threats are coming from, how they infiltrate systems, both information and control the better off we are at a globally in terms of defending, mitigating and being able to forensically understand what took place and mitigate against that happening again and also making sure that it does not cross sectors that that's a very important component of why it's important that we report and so, you know, after having dealt with, you know, pipeline and supply chain incidents that have already proven to be extremely harmful to the American people, I think that it's clear that we must have a uniform reporting mechanism in place that

protects, you know, all of the proprietary information that is required, but also creates a partnership with CISA to enable us to assist these organizations and in some cases alert other similarly situated industries of what took place and then be able to go after bad actors in a timely manner so that we can prevent the worst from happening.

Betsy Woodruff Swan: One of the issues that I think Jen Easterly, the director of CISA, might have highlighted about your bill is this question of enforcement, sort of how to make sure that companies that have those intrusions happen actually report them to CISA and what the repercussions are for companies that don't? Report intrusions in the timely manner? I think the Senate version of this reporting legislation has fines that could be levied levied against some of these companies. My understanding is that your legislation doesn't have fines. Is that something? Is that something that you've thought about? Is there a reason that your legislation doesn't include the threat, the threat of fines for companies that would potentially try to keep these intrusions secret against the law?

Rep. Clarke: Yeah. You know, we've had a number of conversations with stakeholders, industry stakeholders and just observing the behavior of most industries. And what we find is that for many, fines are really just the cost of doing business. What our legislation does provide for is CISA issuing subpoena and I think that that threat of subpoena and responding to it creates an urgency in the case of someone not reporting, but that subpoena means that should that group or that organization, that entity not respond you know, we can legally hold them responsible. And that should the subpoena be responded to that information becomes public, right? So in this case, we're using what we believe is a much more effective means of getting our cyber entities engaged with us as a trusted partner, if you will, in reporting and partnering to again address, you know, what can be, in some cases, an embarrassing incident or very costly incident to the entity itself, as well as the greater society.

Betsy Woodruff Swan: When it comes to the relationships between society and stakeholders that seems to be one of one of the key conversation points for a lot of this legislation. Congressman Katko, you've got legislation that has a really fun new acronym, SICI, systemically important critical infrastructure and your bill, in my understanding, is that it would require that CISA determine which companies are entities are considered SICI, critically, critically important infrastructure and then make

certain benefits available to those companies. The first question is, just from looking quickly through the bill text, it seems to me that for CISA to assess what counts as SICI, your legislation would require some to consult with stakeholders. So that would state and local governments, you know, tribal territorial governments, as well as the companies and industry groups themselves that would potentially have that SICI designation attached to them. Have you thought about whether or not there should be a voice for people who don't fit in either of those categories when it comes to deciding what the most important critical infrastructure is? I mean, should there be a voice for people who both are in government and our industry when it comes to deciding what pieces of this country, or sort of this country's, you know, companies and government entities are really critical?

Rep. Katko: Yes. Let me take a step back though, and I appreciate the question. Congresswoman Clarke's bill about reporting and my bill about a system looking for critical infrastructure are emblematic of one thing, we need to develop a much more robust public-private partnership, right? We cannot, as a Federal government, solve the cybersecurity problems in this country and help make our systems more secure by ourselves. The private sector can't solve the problem by themselves, right? We need that flow of information back and forth, and we need to have a much more synergistic working relationship than we do right now. Right now, for example, CISA gets about one percent of the information on cyber attacks and malware information that they can't possibly see the playing field and help give advice back to the private sector and other security systems if they really don't know what the state of play is, so that's at the guts of what Miss Clarke's bill is, that's it, right? Trying to get them to have a reporting system that both incentivizes them and really rewards it because it helps them and the industry as a whole makes their systems better and more secure, so that's her side. My side is basically saying if everything is critical infrastructure, then really nothing is because you're not really drilling down and what's systemically important amongst the critical infrastructure community and so Senator King and the Senate, you know, he's been working with us and he's got a companion bill, I think, and I appreciate his support on this as well, and basically what my bill does is say, look all of the critical infrastructure community, and there's like 16 different categories, we've got to get together and figure out which ones are the, you know, the big dogs amongst critical that if something happens to this particular infrastructure, we're in deep doo doo, right? And what do we do? And so the idea is to have as many people as possible contribute with

CSA to determine what are, what is critical infrastructure and systemically important critical infrastructure, our SICI, and then develop things that basically get them special attention, right? And obviously pipelines, we probably know that. We know, you know, grids, electric grids and things like that, but you know, there's a lot of other things that you know are important, but they're critically important, but you know, there's going to be the A-Team of critical parts, basically, and that's what this bill does. So the more information we get from people and the more input we can get, we welcome this bill kind of sets a framework, but I don't think it has to be all-inclusive. If there's others that want to weigh in, I clearly encourage them to do so, but what I like about this bill is obviously it's bipartisan and I know that, I'm sorry, Congresswoman Clarke has a markup next week or next month on her cyber subcommittee, and I hope this bill gets there because we need several before it with this. But, with the bad guys moving forward at the speed of light, and we're not really moving forward as quickly as needed to shore up our vulnerability, so this bill helps. I think Miss Clarke's bill helps. I hope we get 'em both marked up soon.

Rep. Clarke: I agree, I think that the work that John is doing in this space is important. You know, I also serve on the Homeland Security Committee, and one of the issues has always been the issue of metadata, too much data to really get to the heart of the issue. And I think that what John is doing, through his legislation, really distills us to the elements that we must, must, must focus on in order to build out a robust protocol to address what we know are the constant bombardment of our critical infrastructure, so we're building momentum, and I thank John for his vision in this space.

Rep. Katko: Thank you. Thank you, too. See we like each other, Republicans, Democrats it happens, for God sakes.

Rep. Clarke: We're New Yorkers. We can't help ourselves.

Rep. Katko: That's right. That's right.

Betsy Woodruff Swan: It's a deeply heartwarming. Senator King, you've obviously been watching congressional efforts to change a lot about security for a long time. I'm curious for all of your member's views on this next question, but I'll start with you, Senator. Why, given that there doesn't seem to be partisan acrimony when it comes to

cybersecurity, nobody's going to lose a primary because of their position on enforcing mandatory incident reporting requirements, given that like the political temperature is so low, why do you think Congress hasn't done more than it's done already? And what do you see as the hurdles to Congress taking sort of bigger, bolder steps to combat these deeply, deeply scary cyber threats that we face? Senator, I'd love your thoughts on that.

Senator King: The answer is one of the most fundamental of all human instincts: territorial imperative. No committee wants to give up an ounce of its jurisdiction, and cyber is scattered all over the Congress. We have pieces of it in Homeland Security and Foreign Relations and Intelligence and Armed Services - that's on on the Senate side. When we had something like twenty five amendments that were adopted last year in the National Defense Act, to get those amendments into that bill required 180 clearances. From committee subcommittees, Republicans, and Democrats. One of the recommendations of the solarium that absolutely went nowhere was the idea of creating a select committee on cyber in both houses, similar to the Select Committee on Intelligence, which was created back in the seventies, when we realized that intelligence was too important to be spread all over. I don't expect that proposal to go anywhere, but that's just the reality of how Congress works, and we have different committees with different jurisdiction and nobody wants to give any up. And so it's just a long slog and if you want to get a bill in somewhere, you've got to get clearance from the Republican side, the Democratic side, on four or five different subcommittees or committees. And that's just the nature of the legislative process. But the answer to your question is not complicated. I suspect our two Representatives will agree. I hope that they will.

Betsy Woodruff Swan: Congressman Clark, would you would you agree with that or would you add any other barriers or challenges that you face when pushing for cybersecurity legislation?

Rep. Clarke: Well, I know that in our Homeland Security Committee, we are moving with all deliberate speed to do what we can within our jurisdiction. But clearly, you know, the territorial disputes that that can arise do arise and do throw some cogs in the wheel, if you will. You know, I agree with Senator King that it would be great to move towards a select committee specifically around cyber. I think that we are lagging in that space. You know, there's no doubt that not many folks are aware or have reached the level of consciousness about what our virtual life means and our connectedness thereby and

the significance of that in the midst of all of the crises that we face as a civil society. It has not risen to the same level of urgency, unfortunately, that say, you know, climate change or a whole host of other sort of physical world issues have particularly in light of the pandemic. So, I'm with you 100 percent, Senator, you know, we can begin a bicameral, you know, campaign to establish a select committee I'm all on board for that because indeed, you know, we're dealing with layered threats, but the cyber threat is a constant and while most people don't recognize it, it does become apparent when you're dealing with ransomware, malware, a whole host of other attacks that do come to fruition, but we are sort of protected from to a certain extent we don't feel the entire blow of it, but we're one step away from, perhaps, the grid going down and I think Texas provided us all a view into what that can mean in terms of our way of life.

Senator King: Having said all that, though, I think it's important to observe that we are getting things done. We had about, I think, 55 or so proposals out of the Solarium recommendations. Twenty five were adopted in the National Defense Act last year. Another half dozen or dozen are in play right now. That's a heck of a batting average. If we were a Major League baseball player hitting .400, we'd be, you know, we'd be pretty happy on the free agency market. So it is frustrating. It does take time. It's a messy, sometimes difficult process. But on the other hand, you get a lot of input and it improves the bills. So I don't want to sound like it's impossible because we we've gotten an amazing amount done in the last year.

Betsy Woodruff Swan: Congressman Katko, you talked about the importance of public-private partnerships and cooperation when it comes to cybersecurity, specifically looking at your legislation, obviously, but also more broadly, obviously, anytime you start talking about regulations or about changing the relationship between the Federal government and industry, folks and industry their ears up and sometimes get a little exercised. On on your bill, and on cyber security legislation more broadly, do you see the role of industry trade associations and the companies themselves as helpful, as a hindrance, a little bit of both? How do you interact with industry when you're putting together these bills that could have a huge impact on the way you work?

Rep. Katko: Oh, we always try to get input from all corners and you know, I know Miss Clarke did on her bill and I did a mine and the many others. Before I answer that, so I just really want to just add one more thing to what my colleagues are talking about with

respect to where we are. I think a select committee would be great because I think cyber is a pretty obvious right, like I said, and it crosses all sectors, but we have made progress, and I'll just point to one. We have a National Cyber Director now, which is going to be very, very important and I think if we properly empower that National Cyber Director, who I think by the way, the Biden Administration did a whole mung with, just like they did with Jen Easterly and CISA and Ann Newbeurger on the intel side. We've got really good people in good positions and that cyber director, to me, is someone who can really bridge the gap and unless and until we have a select committee that that is charged, look at the entire panoply of the threat and making it give me advice accordingly, including when and how we should respond to malicious actors and to kind of fortify what Mr. King was saying earlier. You know, moving forward, a public-private partnership is be built on trust, right? And I hear sometimes, refrain from the private sector is that we give out we give information to CISA, but we never get things back and sometimes CISA is like, well, it's hard to get information we need more information so we can better see your playing field. They're both right. And so, I think our legislation is designed at kind of, you know, Miss Clarke's mind and others. And Mr. King, all those great recommendations to head up this commission they're designed to kind of break down some of those areas of mistrust by kind of institutionalize in what the sides can be responsible for. I'm very confident, once I do that, it's going to work, and I'll give you one quick example. I had a roundtable cyber roundtable discussion in my district about eight weeks ago, and I invited CISA there, the regional CISA director, I brought about 50 stakeholders there. About 25 to 30 of them were already using CISA's services, which include coming and taking a look at your system and telling you where your vulnerabilities are. Completely free service. These are these are government agencies and private sector and by the time we get done with that roundtable, almost everybody signed up for CISA's help. So those types of things, getting the word out there that, you know, "we're the government, we're here to help" sometimes people recoil, but actually since the concept is being developed the right way, and I'm confident that the more we work together, the better it's going to be. It's kind of like the same concept with the Joint Terrorism Task Forces. People very leery about getting under the same roof when it first happened, but now federal, state and local are working incredibly well together, and the exchange of information back and forth is a thousand times better than it was before 9/11, when I was a prosecutor I know that's true and it's and I think I envision the same thing is going to happen here, so it's going to take time. It's not perfect yet, but I think

the bills that we're talking about and the Cyber Solarium recommendations are very, very important to break down those barriers.

Senator King: There's one other provision that fits in exactly with this discussion and that's pending in the Senate Homeland Security and we call it the Joint Collaborative Environment. It's basically a meeting space. We have to re-imagine conflict. We think of conflict as army versus army, navy versus navy. But what we're really talking about here, where 85 percent of the target space is in the private sector, is there has to be a really new connection. And this -- I know I'm restating, but I think it's really important to emphasize that the private sector of the federal government have to really be in sync. And sharing information - that's the incident reporting, the collaborative environment, the working together to identify threats, to attribute threats - that is really essential. As Representative Katko said a few minutes ago, the federal government -- we could do everything right, but we can't solve the problem. This is a joint problem, and a lot of it comes down to the desktop. We can do everything right. But if somebody's in a critical industry clicks on a phishing email, we're in trouble. So everybody is on this boat and has to be pulling in the same direction. But the idea of new relationships between the federal government and the private sector in this area is absolutely critical. We just can't do it without it.

Betsy Woodruff Swan: You know of the cybersecurity pieces of the infrastructure bill and do you have any guesses on what's next for that legislation?

Rep. Clarke: Well, well, I'm sorry.

Senator King: No, no, you go ahead. No, it's in your court.

Rep. Clarke: Exactly. Well, you know, I think we are we are poised to see this legislation move in the House and you know, the bottom line to it is that there is no opposition to what has to be done next and so we're looking forward to its passage.

Betsy Woodruff Swan: What's your sense of the cybersecurity components of the infrastructure bill? It seems like those those pieces that haven't gotten a lot of play. Do you view that as significant, meaningful change?

Senator King: Are you speaking to me?

Betsy Woodruff Swan: Congresswoman Clarke?

Rep. Clarke: Yeah. Well, you know, we're taking this as we, you know, can gain as much consensus as possible. There's a lot more work to sort of build out a robust framework for the interaction between the private sector and you'll hear us repeating this over and over because so much of our critical infrastructure is within the private domain. And, you know, it really drills down to things like cyber hygiene and I think, you know, Angus spoke about that. We can't control what's happening in every corner of the internet, particularly in the private space, but we can create a framework, a robust one, that enables us to communicate in real time to address the number and the volume of attacks that we're under, the sophistication of the level of attack that's coming in, and mitigating that, perhaps even stopping it, as we become more agile in the space. So, you know, I think that we are gaining momentum. The Biden Administration has demonstrated through a series of EEO's and, as has been stated, the the position of the director that we are taking this far more seriously and moving to to address what has really been a lag in our understanding of, you know, just the level at which we are under attack and what we must do commensurate with those attacks to protect ourselves.

Betsy Woodruff Swan: Senator King, what do you see is as likely to happen in the next six months on the Hill involving cybersecurity legislation?

Senator King: Well, there are all kinds of initiatives pending, as we've been talking about today. Our two Representatives have important bills, very important bills. The incident reporting is really important. SICI is very important. Some kind of collaborative environment is important. One thing that hasn't been mentioned that I think is important, that we recommended, is a Bureau of Cyber Statistics -- somebody to collect the data. You can't deal with the problem unless you understand it and understand what the scope and scale of it is. So I think that's an important piece. I think you're going to see a series of provisions that are going to be in -- there already some in the infrastructure bill. There is going to be a package coming out of Homeland Security in the Senate. The House has the bills that we've been talking about. So I think you're going to see a substantial amount of activity. And you know, I think we're getting somewhere. And it has been mentioned there's been a reorganization in the executive with the creation of

the National Cyber Director. But having said this -- before getting on this call, I was on a call with ISO New England, which is the grid operator. And the closing of my comments there was: 'You guys are under attack every minute of every day and you've got to do everything you possibly can to defend yourselves. And it's a job that's never done.' Our adversaries are working on new ways to get into our systems, new ways to compromise our systems, all the time. So we have to continue to innovate, to work, to do everything we possibly can all the way from deterrence strategy to cyber hygiene on the desktop. But I do think, in answer to your question, there's going to be a lot of good progress out of the Congress this year.

Betsy Woodruff Swan: There's not, there's not a huge amount of time, right? I mean, there's sort of the folk wisdom that Halloween is the deadline for anything challenging, controversial deal. That doesn't seem to be particularly controversial, but you know, the clock might be making this difficult, do you think that there's going to be a mandate for reporting incidents to system by the end of the year?

Rep. Clarke: Well, let me just say that we've been fortunate in that our NDAA includes our cyber incident reporting language and so now, you know, it's really a matter of coming to a meeting of the minds on the Senate side. This can pass, you know, very quickly. It's a hurry up and wait scenario. But I'm very, very optimistic that with Senator King and his colleagues understanding the magnitude of what's before us, we'll get this done in this session of Congress.

Betsy Woodruff Swan: We've got two minutes left, so very quickly. Congressman Katko, do you have any any big predictions for what Congress is likely to do soonest on cybersecurity?

Rep. Katko: Yeah, I can tell you. I think we're going to continue to get a ton of wins. I think Senator King mentioned that this cybersecurity has been a raging success. Rarely do you have a commission issue a report with recommendations and then, well do a next to half of them become law? I did it when I did the Foreign Fighters Task Force, then we had ISIS had all of those attacks in Europe and United States. That was a blueprint to deal with it and be able to get those bills passed and I think we're experiencing the same type of success here with the Cyber Solarium. When you have good, thoughtful, bipartisan legislation it can move faster, to Congresswoman Clarke's

point on the NDAA was a great place, we got a lot of bills put in their man, and I think we're going to get a pass. I think if even we have to go to conference, there was a lot of those bills are non-controversial and they're going to stay in, so we've had a ton of success so far and I anticipate given the bipartisan nature of this issue, like I say at the outset, I anticipate we're going to continue to have those successes going forward. No question about it.

Betsy Woodruff Swan: Well, thank you so much and thank you to Aspen for making this all happen. It's been really interesting and revelatory, and I appreciate you making time. I know you have a lot going on so thank you and I hope everyone has a good rest of their Wednesday.

Rep. Katko: Good see you, take care.

Senator King: Thanks very much,

Rep. Clarke: Thank you guys. Have a great one.

Betsy Woodruff Swan: