Chris Teale:

Hi, my name is Chris Teale. I'm a reporter with GCN. We do state and local government technology. "What does that mean in reality," people always ask me. Recently I've written about TikTok and about pornography, so make of that what you will.

Before we get started on today's panel, we do have a Poll Everywhere question for you guys. Unlike George with his multiple choice stuff, I'm going to make you guys work. The question is, when you think of whole-of-state cybersecurity, what's the first thing that comes to your mind? Which is apparently not what we're doing now, but what is the greatest challenge to embracing a whole-of-state approach to cybersecurity? If you come up with the open-ended answer, come find me at lunch. That's totally fine. I'd love to hear it.

Discussing today's panel, I've got two great panelists. I've got Carlos from the Center for Internet Security and Netta from the state of Maryland. So please welcome to the stage.

Take a seat. Well, it's great to have you both. Thank you for being here.

Carlos Kizzee:

Thanks for having us.

Netta Squires:

Thanks for having us.

Chris Teale:

I want to start by just having yourselves introduce yourselves a little bit better than I just did, and tell us about the work that you do, and yeah, we'll go from there. So Carlos, why don't you kick us off? Tell us about yourself.

Carlos Kizzee:

Chris, thank you. My name is Carlos Kizzee. I'm with the Center for Internet Security. I'm a senior Vice President for stakeholder engagement operations. I get to work with great people like Netta here with the state of Maryland and other state, local, tribal and territorial entities that affiliate with our organization. The Center for Internet Security is a nonprofit organization that helps people, businesses, and state governments to be more secure in the connected world.

Chris Teale:

Great, and Netta?

Netta Squires:

Hi. Good morning, everyone. My name is Netta Squires. I am the Director of Local Cyber Security for the state of Maryland, and I sit under the department of IT, specifically in the Office of Security Management. So this is a new position that got created in legislation last year, really with the intent of understanding how we can create a whole-of-state approach, and really understanding how we can integrate our locals into our state systems as it pertains to cybersecurity.

Chris Teale:

Good stuff. Well, thank you both again for being here. And Carlos, I want to kind of set the stage a little bit, set a baseline so we know what we're talking about here. When someone says whole-of-state cybersecurity approach, what does that mean?

Carlos Kizzee:

It's a really, really good question. Whole-of-state. Think about an environment where you're required to put together a football team. You aren't paying the players, so it's a pickup game. It's purely voluntary, but you want to win. You have to win. So whole-of-state approach is really that coordinated voluntary environment where you're developing processes for assessing and managing cyber risk and developing mechanisms and capabilities to effectively manage those risks and to do them in a most effective manner across an entire state.

On the football team, somebody may pass really well, someone may receive really well. How do you align those two capabilities? In a state environment, you have resources at the state level, you have resources and requirements at local and municipal levels. How do you more effectively align them? Because the threat actor's not necessarily making distinctions between a state or local agency. They're targeting wherever they can make the most money.

Chris Teale:

So we had a golf clap for ransomware, and now we've got a football team for whole-of-state cybersecurity. I'm liking the sports analogies. Carlos, I'm going to stay with you. What prompted this shift? Where has this all come from, because is it a new concept, more to the point?

Carlos Kizzee:

So I won't say it's a new concept, but I know for us in the Center for Internet Security, we partnered in 2021 with University of Albany, with NASEO, with NGA, with other agencies, trade associations that work in state, local, tribal, and territorial government arenas. We recognize that like we noticed in... Well, let's just say in World War II and the Manhattan Project, we needed to accomplish something that is really, really hard to do, a very complex problem. We had to bring together multiple resources to do that.

In 2021, we basically developed a white paper that said if you were to most effectively manage cybersecurity risk, you have to do it in a whole-of-state environment. We identified some best practices, we identified some recommendations and so on.

But what the real genesis, the real initiator, I think, for the importance of whole-of-state is what you just heard. You have threat actors that are going to work together in an environment where they're sharing infrastructure, where they're sharing capability. So it's not just that little kid in the basement targeting and attacking NSA or something. It's leveraging great tools and capabilities by all sorts of threat actors with all sorts of motivations.

Chris Teale:

Absolutely. And Netta, from Maryland's perspective, tell me about what prompted your shift towards whole-of-state cybersecurity and your journey, even though you are just one state out of 50.

Netta Squires:

Sure, thank you. Well, I think one thing, to Carlos's point, is that the threat actors are out there. They're continuing to go. But the resources at the local level and the state level are just not the same across. So

within one state, you have multiple jurisdictions with very different tax income basis capacities. We have in Maryland, for example, some jurisdictions that have just for cyber 10 people who are on the team. Very rare. But the majority have zero allocated to cyber security. They might have one or two people that are the IT people, but they don't have any cyber people. So over 60% of our jurisdictions have zero budget for IT. Or for cybersecurity, sorry.

And so really understanding that they're still our constituents from a state perspective, we still have a responsibility to protect them, to make sure that their 911 systems are safe, to make sure that their services they receive from government are available. And so it's inevitable to have to be able to start looking at things in that environment. So that's a huge thing, is just being able to leverage resources and make sure that everybody has access to cybersecurity, just like we expect them to have access to any other kind of security measures.

And then the other thing is using economies of scale. Everything is so siloed in cybersecurity, and maybe that's an IT thing, but it's unfortunate and it's unnecessary. We saw this in law enforcement agencies decades ago. Everyone was so siloed in how they did things, and quickly we realized that doesn't work. Information sharing is important, collaboration is important. That's how we can actually achieve better results.

And so it's the same thing now. Instead of every jurisdiction doing its own thing and being siloed, being able to have that collaboration, information sharing, and for the state to be able to leverage that as well, to be able to, if one jurisdiction tells us, "I'm seeing something, I'm seeing a indicator of compromise, I'm seeing some things entering my environment," and then being able to tell everyone else, alert them to that, and that's how we can help mitigate best, prevent things from happening in the first place.

And then also using economy as a skill financially in terms of why would we all be paying full price premium dollar for a specific product where, if we pool together and we can... And now the smaller jurisdiction can have the same rate that the state is having. Now they can afford it. Now maybe they can use that tool that they weren't able to afford and use before. So all of these factors together are really big driver to try and to implement a whole-of-state approach.

Chris Teale:

Now I'm looking at our polling data here, and 56% of our guests say that the greatest challenge is intergovernmental collaboration. Sounds very difficult from the outside. How do you promote something like intergovernmental when you've got, as you say, big jurisdictions, small jurisdictions, medium size, I guess? How do you work in Maryland to make that a reality?

Netta Squires:

Yeah, that's a great question. So I think collaboration, collaboration, collaboration. And that's a challenge, but it's setting the stage for it. So for example in Maryland, we realized very quickly that there's certain sectors that... We have, for example, our NCRUSE, or our Baltimore USC, our urban area security initiative areas that they have their own meetings, but then everybody else doesn't. All those smaller eastern shore jurisdictions, for example, don't have those forums.

So it was creating a forum. So for example, in Maryland, we created the Maryland Local Cybersecurity Collaborative, literally an environment in which everyone, all our jurisdictions, can come to and get access to the same information, the same resources, be able to share and receive information through the same area, be able to tell us what they're seeing. And then in addition, creating the MDISEC. So the Maryland Information Sharing and Analysis Center. Be able to actually get indicators of compromise, have people signed up to it so that we can share that information forward.

So I think it's creating an environment where you start developing those relationships, creating my position, frankly, having someone whose responsibility it is to be attentive to the locals. So I think those are all ways to be able to start building those relationships, going out, talking to them, seeing what their issues are. Those were ways that we were able to just begin to create that collaborative environment.

And then frankly, also legal requirements. You add sort of legal requirements to that, that they have to report certain things, that they have to... So they begin to have to engage with you, and then you add money, and it's really an incentive. The federal funds, the state and local cybersecurity grant program has been a huge incentivizer. You add that to the table, and really it helps everybody come to the table together.

Chris Teale:

So continuing with our sporting analogies since we've already had two this morning, I have to ask, would you say you are a coach? Would you say you're maybe a traffic cop or a referee?

Netta Squires:

Oh wow.

Chris Teale:

I mean, how would you describe your position relative to a sport, and the more obscure sport, the better?

Netta Squires:

Oh, geez. That's a good question. That's a great question. I'm not a great sports person, though. So I mean, I think it's more sort of being the scout, almost. It's learning to identify the talents and the challenges, and then being able to bring the right resources to the table to address those. So not necessarily just like the coach, but it's being able to go out to the field and say, "All right, this person's really great at that. This jurisdiction's good at that. This resource in terms of industry tools answers that question, problem, addresses that challenge. Let me match you up and put you together, because I think those would go together." And then being able to create forums in which everybody can share and benefit from that kind of information.

Chris Teale:

A hundred percent. I didn't have scout on my list, but-

Carlos Kizzee:

Beautiful answer.

Chris Teale:

Yeah, absolutely. Carlos, based on your research over at CIS, what are some of the best practices that you are identifying from states that are looking at this whole-of-state approach?

Carlos Kizzee:

So within the Center for Internet Security, we've got the Multi-state Information Sharing and Analysis Center. It's like Netta mentioned, there's a Maryland ISAC, but we have a multi-state where all of the

states and territories come together. We've got about 15,000 members, but every one of our states, all of our six territories are participants in that.

Some of the things I think that we see as best practices, you've heard examples of some of them here. Innovation I think is one, having states and municipalities being willing to innovate. Perhaps there are no existing authorities for what Netta is describing, but that doesn't mean that they're not going to build out a voluntary collaborative network in order to do that. So a best practice is having the state in a position where it's empowered. I think the federal government providing a state local tribal grant program in 2021 empowered the states a little bit, because it identified 1 billion dollars across 50 states and six territories, but 1 billion dollars for states, municipalities, and tribes to work together state by state and state cyber security planning committees and leveraging authorities or developing authorities where those authorities don't exist or working in a collaborative environment, I think is a huge best practice.

Now also listening to what Netta described, you now have a collaborative environment where you're looking at who does what well? How do we partner more effectively together? How do you sustain that collaborative environment? A best practice for identifying how do you measure what is effective in terms of that cross and multidisciplinary environment, measuring the effectiveness of it, and then being able to sustain that effectiveness year over year.

And I think, using the scout analogy again, being able to define roles and responsibilities and being able to shift and align those roles and responsibilities to match the ever-changing threat environment that's impacting the states and their municipalities.

Chris Teale:

That's the way you sustain it? Because I mean, it's one thing to show up to a kickoff meeting and say, "Yeah, we'll do this." And then 18 months go past and nothing's happened. But for you, that's the key way to sustain something like this?

Carlos Kizzee:

I think looking at the models that are developing, the whole-of-state models, more and more states are adopting this approach because their municipalities don't have the resources, as Netta described. So more and more states are adopting it. We've created an environment in the multi-state ISAC where those states can come together. We actually have a whole-of-state working group where they're sharing best practices, lessons that they're learning, and so on. They're learning from each other. And I think that that is a huge, huge value proposition, because then they're able to see what does work, what might work for us, let's apply it. If it is working, let's keep it going, but let's also share it with our peers and continue the learning process.

Chris Teale:

All right. Sounds good. And Netta, from your perspective, where are you guys in the planning process for this approach, and how are you incorporating some of these best practices yourselves? Because there's a lot to do, I imagine.

Netta Squires:

Yeah, absolutely. So as Carlos mentioned, the state and local cybersecurity grant program is a huge instigator for coordination. And we were chatting about that a little bit before the meeting and saying, if

nothing else, because people hear a billion dollars, and every jurisdiction calls me to say, "How do I get that billion dollars?" I'm like, "Well, it's over four years for the entire nation and divided by..."

So the reality is that per jurisdiction, it is not that much funds, but the greatest value it's bringing to the table is that everybody's coming to the table, is that sort of captive audience that you have, the forced collaboration or incentivized collaboration to come to the table. And so that's huge.

And so I think where we are in the process is really leveraging that, kind of jumping, riding that train and saying, "Hey." Waving those funds and saying, "Hey, come to our meetings, come to be part of that conversation so that you can help determine how we can best spend these funds."

And so for example, what we did through the state and local cybersecurity grant program, but also to benefit us at the state level, was put out a survey to all the jurisdictions saying, "Where are you? What are you seeing in terms of your environment? Do you have a 24/7, 365 SOC capabilities? Who is that? Is that you? Are you the 24/7, or do you have an actual SOC? What does your EDR look like? What are your gaps? Have you identified any solutions to address those gaps that you would like to see?"

So taking that data, that was a huge first step for us. It was like a 200 question survey, admittedly perhaps too long. But we were trying to be thorough. And analyzing that, going back and figuring out, taking the results and then putting that into recommendations. And that's kind of where we're at.

And we're saying, "All right, now we have our data. We've seen what our jurisdictions are saying that their needs are." Now we are bringing it back in front of the committee. There's a committee that has to go, and saying, "What are some of the investment justifications that we can come up with based on these recommendations, based on the data that we've collected?" And then the MDISEC has been a huge incentive for security, huge, huge part in helping that is learning from other states. What are they doing? What's working, what's not? What are the options? And so going out and seeing these are some ways. That if it's MFA, if a lot of our jurisdictions need MFA, how do we achieve that? If a lot of our jurisdictions need EDR endpoint detection and response, how do we achieve that at scale? How do we achieve that to make sure? How do we do it from a practical perspective, because you might not want all the same tool. Not everybody wants to switch tools. Not everybody wants the one that you may be using. So how do we do that in a way which maximizes the money, but also maximizes resiliency, but it's also practical? It has to work for them, just because we have a solution.

So trying to bring all those things together. And then procurement. Procurement in government is challenging. And so how do we deal with procurement at the state level, at the local level? How do we make those match? And so it's a lot of really trying to build all the pieces of the puzzle right now and put them all together to make sure.

And I think to your point just earlier on, sustaining the program, I think ultimately it'll be success. So one of the things that we're doing now is creating the metrics. How are we going to measure program success? Because if we can show that over the next three years of this grant program that we have measured results and success and that they're less, that we've managed to mitigate and prevent X many attacks that we wouldn't have otherwise, that will, I believe, help leadership want to continue to implement and sustain the programs long term.

Chris Teale:

It's all about getting points on the board, huh?

Netta Squires:

Yes, exactly.

Chris Teale:

There you go. Another. And I think that's, what? Number four sporting analogy? That's embarrassing, really. All right. Let's talk challenges for a second. Carlos, what are some of the challenges that you see with states trying to implement this kind of strategy?

Carlos Kizzee:

I think the poll that you did early on really identified very effectively the biggest one, in my opinion, at least, as I look at the states and the local entities. We're saying that there's an infrastructure for a whole-of-state, but that structure does not exist. Most states don't have centralized IT management or centralized security. Most states don't have centralized budget for IT. Some do, but most do not.

And so you're building something that doesn't exist. So you've got these intergovernmental relationships. And the biggest challenge, I think, is finding people like Meta who have vision and empowering that vision within the state, but just be aware as you're doing that. Security threats are still happening. IT still needs to be managed, and it's still being managed in a decentralized environment. So it's kind of building the airplane. Sorry to use a different analogy than sports, but building the airplane while you're flying it. I think that's one of the biggest challenges.

I think one other one is resource. There is such a significant resource differential. In order to be cyber secure, there are some things just that we could do individually that are essential. Strong passwords. Don't reuse your passwords, things like that. Now, take what one person could do. Now apply that to a workforce. How do you indoctrinate that workforce? And then how do you do that across a whole jurisdiction like a county, a township, or even a state? How do you resource doing that when perhaps there's not a budget for that type of thing at some of those small municipality levels? If I'm the bad guy, if I'm the threat actor that Sandra Joyce was just briefing us about, I'm targeting those locations where they're not resourced. So creating an environment in this sort of asynchronous area, that's a really, really big challenge.

Chris Teale:

Netta, at the risk of throwing the entire state under the bus, I mean, what are some of the challenges that you've faced as you [inaudible 00:22:14]?

Netta Squires:

Everything's going great.

Chris Teale:

Yeah.

Carlos Kizzee:

Yeah. Maryland's [inaudible 00:22:16].

Chris Teale:

I knew it.

Netta Squires:

I think, I mean, so many similar things. But I think a big part is lack of trust, frankly, by the locals in the state. Not just in the state, but how are you going to do this? How are you going to implement this? How are you going to manage it? We're never going to see any of that money anyway. And that really just all goes back to that relationship building and starting to gain that trust and to begin to show results. I think you have to start somewhere. Even if you start anywhere, you got to start somewhere so they can start seeing the actual impact in the results.

And then another one of the challenges that I feel like I face every day is, how do I really maximize those funds? Because again, they're so minimal at this point that you want to make sure that they really do get the best use. How do I make this the most effective? And that's something that... Because if we sub-grant everything, for example, if we just say, "Here's 5,000. Everyone's going to get a UBI key." There's not enough money to go around equally to everyone. So how do we make sure that really we are maximizing the ultimate impact with the maximum amount of dollars so that not everyone's paying admin costs? But that falls under one.

And then just being able to make sure that we are addressing the actual gaps that we're seeing, being able to make sure that we're not just answering any challenge, but that it's what they actually need.

And then I think the final thing is just making sure that how do we build? Because not everything is going to happen on day one, so how do you determine who is that first round of... Is it the ones who need it the most? Is it the rural jurisdictions and the ones who need it the most, and potentially is it K-12? Are those the ones who need it the most? And then how do we build those programs to then be able to be more inclusive and more inclusive and more inclusive so that everybody can be a part of it and leverage it and take...

Carlos Kizzee:

Chris, one more thing on that one. One more note. Netta mentioned something that I think is really, really significant, and not many jurisdictions have done it the way that Maryland has, and I think it's a best practice that's worthy of note. Requirements are not going to be homogenous, they're not going to be uniform. So doing some type of an assessment, even if it is a little long, doing some type of an assessment where individual entities get to identify their unique virtues and areas where they may need some additional help, but doing that in a safe space. Nobody likes to give a bad report card on themselves. There are some cultural issues that have to be overcome in that context. But having an environment where you can do a self-assessment, third party assessments if possible, and think about the results of those holistically, that gives the opportunity for a state like Maryland to then look at, we can acquire this capability at a state level, make it available across all of our municipalities. So some jurisdictions that didn't even recognize they had that problem, would never be able to afford to resource that problem, can now be benefited against that. And perhaps recognizing that over time, maybe what the state provides doesn't quite meet my local needs, but I at least have a starting point that I can build on now.

Chris Teale:

That's great. You both have mentioned the grants that are coming down the pike from the federal government, and I want to ask this next question, and through that lens if you like, which is, what does the future hold for this whole-of-state approach? Especially as there's a billion dollars, which I know is a drop in the proverbial bucket. What does the future hold, Carlos?

Carlos Kizzee:

From my perspective, I think that by the federal government doing what they have not done before in this particular area, in cybersecurity granting funds to states, but leveraging the states to ensure that those funds get to local and rural entities and agencies in the grant program. And there's actually a hard requirement for 80% of the funding to benefit local entities in the state, and 25% of that for rural entities. I think that creates a culture of cooperation and collaboration. It creates an incentive, an environment where there's an incentive not just for states to participate, but also for states and local municipalities to work together. We've seen in the last several years more and more states are doing more holistic statewide approaches. And these are states where, again, IT is not centrally managed or centrally budgeted for, and security is not centrally managed. But we're seeing more and more whole-of-state.

I think that while we might see a slight decrease, as Sandra was saying in ransomware in some areas, in our state and local government environments, these are data rich and capability poor environments. Threat actors are targeting K-12, for example, they're targeting public health. Why are they doing that? Because it's lucrative. They make money from the data that they get and from the ransomware attacks that they charge. They're going to continue to do that as long as it's going to continue to be profitable. So I believe that in the future, we're going to see more and more whole-of-state simply because we have to. It makes sense.

Chris Teale:

Absolutely. And Netta, same question for you. What does the future look like in Maryland?

Netta Squires:

Yeah, I think, and not just for Maryland, but I think really heading towards collective defense has been something that I think the value has been shown and seen everywhere, and it's something that these kinds of grants, but also just this sort of forward-thinking as a whole of state and really a whole of nation at the end of the day is going to move us towards is that collective defense, is being able to understand that in having organizations like the MSISEC that have their [inaudible 00:28:32] program, but I think run through you or the MSISEC and being able to do vulnerability and attack surface management at a national level, at the state level, that is huge. And that's where I think we need to move. That's where I think we are moving towards, and that's what these kinds of efforts are going to help us move towards.

It's also, we hear all these terms like defense and depth. We want to make sure that we have multiple layers of defense. And so if we have organizations that are signed up also to the MDISEC and also to the MSISEC and also have their own vulnerability and exploit management, then that is defense and depth.

And then personally I think coming from an emergency management background, working on mitigation prevention. Let's just not let them through the door. If we can stop it there, then we don't have to do all the rest. So really kind of increasing those resources that we have collectively and individually to focus on detection and eradication initially so that they can't even get into the perimeter, I think, is going to be kind of where things head with these collaborative approaches.

Chris Teale:

Sounds good. All right. A last one from me, since we're almost out of time. We could keep going and going for a full 90-minute soccer match if that's what we were inclined towards. I want to leave our guests with a bit of a call to action. Carlos, what advice would you have for state or local governments that look at this whole-of-state approach? They want to do it, they have no idea where to start. What advice would you have for them?

Carlos Kizzee:

I would say for state and local governments, job one is to join the multi-state ISAC. And the multi-state ISAC is nonprofit activity. It is free. Nothing's free. It's subsidized by a partnership, a cooperative agreement in partnership with CISA, the cyber and infrastructure security agency within DHS. But join the multi-state ISAC. If your local government agency is not a part of the multi-state ISAC, you should be. There are services that are available to you that are already paid for by the federal government and subsidized. We have a 24 by seven security operations center, and we have other services and capabilities that help you block malicious threat activity that's coming towards your network, that provide you some response-type of capabilities and some awareness capabilities, whether you have no SOC or whether you have a security operation center or a large operation center.

I would say get involved with your peers by joining the multi-state ISAC so that you can collaborate with other states and local jurisdictions that are going through the same thing that you're going through so that you can share lessons, learn things like that. And please, within the context of the whole-of-state topic, understand that there are authorities and resources that you have already. You may have to design new ones, you may have to leverage more effectively the ones that you have, but view cybersecurity as a collective defense matter. Don't view it as something that everybody who has a protected laptop or some capability has to fight on their own.

Chris Teale:

Okay. And Netta, I'm going to ask you the same question, but you're not allowed to answer, "Come and work for the state of Maryland." That's cheating.

Netta Squires:

Yeah. I also want to actually mention one more tool that I would recommend working with the Center for Internet Security, and that's their NCSR, National Cyber Security Review self assessment for the maturity assessment. And so, we were talking a little bit about understanding where your vulnerabilities are. That's something we use and something that we're going to try and make mandatory if we're allowed to, at least for grant recipients, because it's huge, being able to use. So there are so many free tools out there that have been put together by our federal agencies. It can collaboration with the Center for Internet Security and your taxes are paying for it, so we should leverage them. But I think just starting to really get educated on the resources that are out there would be a first good step, in my opinion, to just really understand what is already done and available.

I don't want to reinvent the wheel. Nobody needs to reinvent the wheel. On [inaudible 00:32:52] website, there's templates for everything. One of the things we're doing for the locals is we've created templates for incident response, disaster recovery, business continuity, cyber [inaudible 00:33:05]. So being able to have a streamline. But a lot of those resources also exist. So being able to understand what we already have, and then augmenting and supplementing with what we don't have, really working. And government doesn't need to reinvent everything. Industry has done it really, really well. We don't have to build up our resources internally on everything to be able to carry it out. We can partner with industry. So partnering with industry to leverage their tools, their resources, their development, and then being able to really just have forums. Create those forums for open conversations, for collaboration, to hear what other people are saying, to see how it pertains to you.

And then I think the only last thing I would say is break down the silos. I feel like so much about cybersecurity is hush, hush. We don't talk about incidents, everything, but like why? You don't not talk about a terrorist attack. It's all over the news. We want to know. We want to learn. We want to grow. So

breaking down those silos and connecting with your partners so that we can learn and ultimately all be more resilient for it.

Carlos Kizzee:

Well said.

Chris Teale:

Absolutely. All right. Well that was, as they say, a buzzer beater, right at the final thing. But that's it. Please thank our panelists for their insight. Thank you.

Netta Squires:

Thank you. Thank you.