America’s Frontline Cyber Readiness:
A View from the Federal, State, and Local Levels

Featuring: Michael D’Ambrosio, Tim Eisler, Dr. Christopher Rodriguez, Timothy Roemer

Moderated by: Dr. Samantha Ravich

MAY: Hello, I’m Cliff May, FDD’s Founder and President. Thank you for joining us today. FDD is a non-partisan institute focused on national security and foreign policy. We are a source of timely research, analysis, and policy options for Congress, the administration, the media, and the wider national security community. We take no foreign government or foreign corporate funding and we never will.

I’m pleased to welcome you to today’s event, *America’s Frontline Cyber Readiness*, which explores the lessons state and local governments have learned – and continue to learn – from the global pandemic, and how these lessons should be applied to better prepare the nation to respond to cyberattacks.

Even as we all adjust to new ways of working in the COVID era, those seeking to do damage to the United States and our allies in cyberspace continue their attacks uninterrupted. And we are at a particularly high risk given our increased reliance on technology – whether teleworking or the demands on our supply chains.

Today’s conversation, hosted by FDD’s Cyber and Technology Innovation, will add important details to how we should think about implementing a key finding of the congressionally mandated Cyberspace Solarium Commission: the creation of a “Continuity of the Economy,” or COTE plan. Similar to COG, “continuity of government” and COP, “continuity of operations,” a Continuity of the Economy plan would ensure the rapid restoration of our nation’s critical functions after a catastrophic cyberattack.

Though it didn’t require a global pandemic to prove the need for such a plan – it is ever more evident how vital COTE is. Governments and industries alike have had to rethink everything from how we do business to how we communicate with our colleagues, customers, and constituents. Imagine trying to do that in the middle of the fog of a cyber war. The stakes aren’t just, how do we restock shelves of toilet paper? But how do we ensure the continuous flow of life-sustaining goods and services to the American people regardless of the cause of the disruption?

We have recently seen firsthand how our citizens turn to state and local officials in times of crisis. These governments and local industries are on the front lines protecting critical functions of our economy. During a cyberattack, they similarly are the decisionmakers that get our systems back online.

I’ll provide brief introductions of our panel here, but please visit our event webpage for their full biographies.

Michael D’Ambrosio is the United States Secret Service’s Assistant Director within the Office of Investigations, where he oversees the planning and coordination of domestic and international criminal investigations involving counterfeiting, financial, electronic and cybercrime.

Tim Eisler is the Information Systems Manager for the City of Dublin, a suburban city in the San Francisco Bay Area. Tim managed the division that thwarted a ransomware attack, and led the effort to find evidence of the attempt, and so we are looking forward to hearing from him some of what he leaned so that we can all benefit without, hopefully, having to endure the same experience.

Tim Roemer is Arizona’s Chief Information Security Officer. Previously, he spent a decade with the CIA. During his tenure there he was a nonpartisan to the White House Situation Room, where he provided critical national security updates to the President, Vice President, and National Security Council.

Dr. Christopher Rodriguez is the Director of the D.C. Homeland Security and Emergency Management Agency. He previously was the Director of New Jersey's Office of Homeland Security and Preparedness, and prior to that spent time with the CIA.

My colleague Dr. Samantha Ravich will moderate today's event. Samantha is the visionary behind FDD's Center on Cyber and Technology Innovation and our Transformative Cyber Innovation Lab. She also serves as vice chair of the President's Intelligence Advisory Board and as a Commissioner of the Cyberspace Solarium Commission. It was her distillation of disparate observations almost two years ago at a Cyber Enabled Economic Warfare, or, CEEW table top exercise that led to the concept of COTE. We are excited that she will continue to lead FDD's efforts to support COTE implementation following the Cyberspace Solarium Commission's adoption of this critical concept.

We hope you enjoy today's conversation. I encourage you to learn more about FDD, and check out our recent events and analysis at fdd.org. You can follow us on Twitter @FDD. I am now pleased to turn the floor over to my esteemed colleague Dr. Samantha Ravich.

RAVICH: Thank you everyone for participating in this really important session. You know, COVID has tested the resiliency of our continuity plans and showed us some of our broad vulnerabilities across the spectrum, but particularly from a cybersecurity and emergency management perspective, what has this crisis revealed about the needs of our states, local, territorial, tribal governments in terms of being really prepared for a disruptive cyber event? Let me just preface by saying the Cyberspace Solarium Commission, we released our findings in March but we released a pandemic annex in the June timeframe where we looked at what COVID was teaching us about how to deal with a disruptive event and the overlay for a cybersecurity large event.

So, let me just start with Tim Roemer. As you apply lessons from COVID, how does that get you thinking about, for the state of Arizona, what that could mean for a disruptive cyber event?

ROEMER: Well, thank you so much for hosting us today. Really important topic, obviously. I became the CISO of the State of Arizona one year ago and fortunately what COVID has taught us is that we should really be doubling down in our state on some of the areas that we put into play one year ago, which the first one was investing in our employees, investing in every end user. We like to refer to this as the human fire wall. The reason why this is more important now than ever is because you've got more vulnerable employees working from home off your networks in a personal, sometimes, environment. They've got a lot of distractions going on. They're going to be more prone to clicking on a link or doing something that's more risky. That's why investing in their education and training, ensuring that they're in a position to protect your state data or any data that anyone has access to, is more important now than ever.

I like to think that we have a team in Arizona that includes every employee. So, one year ago we got Governor Ducey's support and he mandated statewide annual cybersecurity awareness training for every single state of Arizona employee. What that means is we essentially took a 16-person cybersecurity team at our Department of Administration that I manage. We turned it into a 36,000-person cybersecurity team by making every single employee part of our team. That means annual statewide cybersecurity awareness training, as well as more phishing. We have increased the amount of phishing that we do to our employees, and we've made it much harder as well. So, with the support of our Director Tobin at ADOA and the Governor, we know that we have their approval now more than ever to make sure that every employee knows how important cybersecurity is to the state of Arizona.

RAVICH: That's great. You know, Chris, I'm sure that what Tim just said resonates with you. But a couple of years ago you participated in a tabletop exercise that we at the Center on Cyber and Technology Innovation at FDD hosted on cyber enabled economic warfare. And it was interesting at that point you were the only SLTT official at the table, which says a lot really about some of our assumptions regarding cybersecurity at that point. But one point that was made during that tabletop is the difference between natural disasters, which are localized and finite, and cyberattacks which are not bound by geography or time and can cause breakdowns in supply chains across the board, and how that makes you think about being able to share resources with others in your locality, other states, other officials. Am I more likely, less likely to share equipment, let's say, if there's a major cyber disruption as opposed to there's a fire or a flood a few states over?

So, I just want to get your thoughts on that and also for the audience and for the other panelists, I mean Chris was on the front lines at Hurricane Sandy so he understands Hurricane Sandy, COVID, so what are your thoughts on some of those things, Chris?

RODRIGUEZ: Yes. Thank you, Samantha, and I think Tim Roemer would appreciate this. We at the state level are really on the front lines of defense against cyberattacks and certainly in the immediate responses to emergencies like COVID, or certainly major disasters that are weather related. And the cyber threat does complicate in some respects the response to major disasters because, in the case of COVID, it has a lot of cascading impacts to our community. Washington, DC serves as a kind of quasi city state that provides direct services to residents but also performs a lot of state functions as well.

Take for example, Tim mentioned our employees. 60% of our 35,000-person workforce is now working remotely and a lot of those lot of those frontline workers are providing direct services to our residents and so the cyber threat landscape just expands. In the COVID context, as we expand our testing capacity, our contact tracing capacity, housing that information and taking in and ingesting that information in our state system under the Office of the Chief Technology Officer also becomes a challenge because we are ingesting so much more information and have to protect that information.

And so, that does kind of, as I said, create new challenges. Here in the District we are also providing laptops and tablets to all of our students who are going to be attending classes virtually. Again, that does expand the cyber threat landscape and each of those tablets and equipment has to be scanned and protected against any types of attacks that might inadvertently occur in the use of a child. And so that does – again, the cybersecurity element of this is so central to our response, even as you're dealing with an unprecedented global pandemic.

RAVICH: So, Mike, I want to turn to you for a moment. And one of the problems that arises again during COVID, during other natural disasters, is that the bad guys prey on the populous, right? As Tim and Chris were talking about, they're trying to get out useful, important, critical information to their citizens during times like COVID and the bad guys know this and so they put out bad information. Fraud really ticks up, and so it's bad information. It's bad information on how to use your device. So, talk a little bit about the Cyber Fraud Task Force, because I know that you're really focusing your efforts on that. And if you want to start now, or I was going to ask you a little bit later about US Secret Service, people don't think about you in this context so if you want to start with that as well, I think the audience would really be interested in hearing that.

D'AMBROSIO: Yeah, no, that's great. I appreciate, Samantha, having this conversation. It's a real well-respected group and I look forward to the discussion. Listen, here's the mission of the Secret Service, right? Most people see the Secret Service primarily in our protective role, especially this is a campaign year, a different campaign year but a campaign year nonetheless. And the Secret Service mission really focuses on the protection of our nation's leaders. What most people don't know is that we started in 1865 with the protection of our financial and payment system. That really continues to this day and the two missions are really integrated.

I will tell you in 1995 we created what we call the Electronic Crimes Task Force, and the reason that was created was the Secret Service, pretty innovative at the time, decided that, hey, technology is really being embedded in our financial infrastructure. Financial industry really took the lead on utilizing technology within their operations and traditionally that then created some exposure that most people weren't prepared for. So, we created this Electronic Crimes Task Force. In essence it was a collaboration between state and locals, all our federal partners, and the private sector, as well, to come together, form subject matter experts and collaborate on how to solve complex problems.

Innovative at the time. We see a lot more of that really today. The Cyber Fraud Task Force for us is really just an evolution of that. We really focus on protecting the financial and critical infrastructure. What I will tell you is most cyber breaches, about 75% of them, if you look at the Verizon data breach report, are all financially motivated. So, there is the nation state activity that's out there that's looking to exploit data, but most of this is really sort of financially motivated. What we try and do with the task force is this. We're really focused on a couple of things. We want to identify all of the crime and all of the fraud. We're going to investigate it, we're going to prosecute it.

But how are we going to do that, right? One, you've got to be able to share information with your state and local counterparts, whether it be the victims, whether it be private sector organizations. Doesn't matter necessarily who it is. By sharing information you end up building trust. A lot of times there's this divide between the private sector, whether it be municipalities – "Hey, federal government has all these answers. We know who's doing it. We're just not sharing it." It's not really true. Like in any crime, we need the collaboration of the victim and in order to do so we've got to share information and build that.

And then we want to enable operations. One of the things that we did in 2008 is we partnered with Hoover, Alabama for the National Cyber Forensic Institute. We really noticed a gap in the capabilities in state and locals. I think it was Chris who said, "Hey, state and locals were really on the forefront of these pandemics and all of these different type of disasters." Well, that's correct, and so from a force multiplier standpoint, the federal government really needs to enable state and locals to support these particular operations. That's what the National Cyber Forensic Institute does. It's again, partnership with state and locals, built by state and locals with federal government support. We trained over 12,000 state and local investigators, prosecutors and judges, going after digital technology involved in every aspect of life can include crimes. We need them to be able to exploit that particular data. They're right now doing about 300,000 forensic exams have been done with the examiners who have gone through the NCFI. Right? The other thing we're doing is we want to build a resiliency of state and locals. You've probably seen some of Tim's neighbors, Texas, state of Louisiana, even prior to COVID were targets of cyber criminals. Well with ransomware attacks, right?

So, we're trying to build the capabilities involved in that. The NCFI was critical in the response in Louisiana. I will tell you something else we're doing. We're working with the McChrystal Group. We instituted a cyber incident response seminar, right? To really work the resiliency piece, the preparation piece for municipalities. We're focused on primarily ransomware. Our healthcare sector. Again, they're not investing necessarily in cybersecurity. Their job is to save people. We need to make sure that we can prevent them. So those are some of the things that we're trying to focus on and the goal of the Cyber Fraud Taskforce.

RAVICH: That's great. Thanks. Thanks Mike. So, Tim Eisler, it's a perfect segue to what you can talk about in terms of it is a more than safe assumption to say it is not if it is when and one is going to be hit by a cyber breach or a ransomware attack. So, as you are comfortable, take us through what it's like on the other side of such an attack.

EISLER: Sure. Thanks for having me here. This is a great group to be a part of. Really appreciate it. So yeah, it's not a matter of if, it's a matter of when. And when it's going to happen again. So, we were hit by a ransomware attack this year. Thankfully our endpoint protection did a good job of keeping that from spreading and losing any data. But they did have control of our environment for a while. Basically, shut us out of the system.

Thankfully, I have good consulting company that can help remediate that. They did try to encrypt everything. It was a ransomware attack. They left note without any dollars attached, but basically "Contact us to get your data back." Thankfully, the endpoint protection did its job and prevented it from going any further. But there was a lot of forensics to do after the fact and seeing how they were able to gain access to environment. An interesting piece is they were able to gain access in the beginning of the year. So, they actually in our environment undetected for many, many months, but then waited to we were all working at home, when our guard was down to actually unleash the attack. So, pretty good insight to how we were working and when to strike.

So, we were able to handle that and we put in more security pieces in play to kind of prevent that from happening again. But it's a constant barrage of attacks against us. We do the cybersecurity training. We're due for another one, I think in a couple of weeks. Constant phishing attempts, testing our user base. And we still get people that click through. The phishing attempts that we run are pretty sophisticated and try to target people with something like – It'll know when the reviews are coming up.

So, they'll say, "Hey, review is ready here, click on this." Or "You got caught by a speeding camera." And there's always a few clues in there, but just people react instinctively. And they're like, "Oh yeah, I'm expecting review, it sounds logical." So, they click on it. So, constant training is important and then constantly hardening the environment.

One of the pieces that we're looking at is a managed service. We're a small group of IT folks for the city. There's four of us running the whole department. So, we don't have the manpower to be there on the weekend and watching the environment 24/7. So, looking at a managed service company to engage that will have insight to our network constantly through the end points.

And if they see something going wrong, they can take action. Either notify us or take action on the weekend. So that kind of support, I think is essential for local governments who don't have the deep pockets or the deep staff to kind of keep an eye on things all the time. So that is certainly a piece of technology we wish we'd had before this happened. And they would have spotted elevated privileges back in December, raised some flags, started investigating, let us know, and we could have prevented the attack from even really occurring have we had some pieces like that in place.

So, I don't know that a lot of municipalities have these managed services or have the depth to basically run a security operation center. But I think that's something that more and more municipalities will be taking a look at.

RAVICH: Yeah, that's really important. It is something also, we looked down on the solarium, IT modernization at the local level, for sure. Well, one thing I just wanted to follow up on when you and I were talking, and everyone's like, patch, patch, patch. Yes, absolutely patch, patch, patch. But you patch in a way when it is business normal, but these are abnormal times. And what you had said, and kind of stuck in my mind is, yeah, it's not as simple as click a button and a patch downloads, and then you can kind of set it, forget it. And if you're not in the office while these things are running, they get stuck in the pinwheel of death. And you may not have an actual patch. So, did I a state that correctly?

EISLER: A lot of people are working at home and we've either sent laptops home with them with the VPN. But in most cases, people are working on their own hardware at home using a virtual desktop interface. That gives some disadvantages because when they connect they're coming through a firewall, so they're behind our walled garden basically, but it's their computer that could be an issue. So how to keep their home personal computer patched.

One of the things we did early on before we even knew we were under attack just as a matter of precaution our endpoint protection company gave us licenses for free personal use. So, we pushed that out to our users, "Look for using a computer at home, you don't have antiviral protection or endpoint protection. Here it is. It's covered for three years. City's paid for it. It's a personal end point protection."

So, we pushed that out. And most of our users adopted that. Some had another brand and they ditched it and took ours on. It doesn't let us see their computer, but it protects their computer. So, if they're using their own computer to connect to us, we want them to be as protected as possible. But certainly patches, updates. They're difficult. And if they take our own equipment home, if they're not connected to VPN, they're not going to get the automatic pushes for updates. So, it does create some difficulties.

RAVICH: Yep. Yeah. Thank you. I want to get back to sharing information lines of communication. Chris, as you're communicating down the pipe to your citizenry, but also, I mean, look in District of Columbia I understand, obviously you have deep connective tissue for preparedness with Northern Virginia and parts of Maryland. Talk a little bit about and obviously the federal government, where do you see the bottlenecks are in terms of lines of communication and sharing information so that as we're taking the experiences of COVID and overlaying them on cybersecurity, where do we need to get better so that we can be more resilient with the possibility of a major cyber disruption?

RODRIGUEZ: Yeah. Thank you. Thanks Samantha for the question, even before COVID the region, the national capital region has its CISOs and CTOs have formed alliances of information sharing. In some jurisdictions it's harder to get that buy in than in others. But we have seen, broadly speaking and generally speaking, good coordination and information flows between the 24 jurisdictions that make up the national capital region in Northern Virginia, and then in Prince George's County and Montgomery County in Maryland.

And the way that that information sharing flows, it's not automated. So, I don't want to say that the systems are linked to share automated threat indicators. But it mostly happens face to face and exchanges between the CISOs and the CIOs or the CTOs, depending on how the different jurisdictions structure their information security organizations.

The thing we've seen a lot of cooperation coordination on isn't on the COVID response. We haven't seen, or at least the jurisdictions have not shared, and we haven't seen in the District any abnormal activity on our networks related to COVID.

But what we have seen though is coordination operationally on the ground with our response. For example, as the different states move into different phases of the pandemic for reopening, we have been very cognizant of coordinating with, for example, Arlington County and Fairfax County, which surround the District and Montgomery and Prince George's in Maryland. We have seen in those instances where those counties have actually broken from the states and what Annapolis and Richmond actually wanted to do in order for them to remain in lock step with the District, which has been a little bit more for lack of a better term conservative in terms of our reopening posture.

So, on the cyber front, we do have those lines of communication open to share information it's not done without the involvement of humans. But on the COVID response, we have seen a lot of coordination in our reopening strategies and our plans. Just two days ago, I was on the phone with Arlington County and they were looking at potentially restricting some of their restaurant activities and wanted to know what the District thought of that and whether we were planning to move in a similar direction.

So that type of coordination is really critical for us because the District has very porous borders with the surrounding jurisdictions. And so, remaining in lockstep with them is really critical to making sure we keep our cases down here.

RAVICH: Mike, so when Chris was talking about the flow of information, obviously between District of Columbia, Maryland, Virginia, on COVID but it kind of calls to mind okay from the federal perspective and on cybersecurity best practices, I mean, we're still kind of learning what is allowed to be shared, how it is shared. Of course, which agency in the federal government, is it U.S. Secret Service? When is it the Bureau? When is it DHS? So, when you look at Tim Roemer, Eisler, or Rodriguez, can you give us some color in terms of where you see kind of the bottlenecks as the federal response with what the folks on this panel really need to look to for answers from the federal government. Especially on the cybersecurity, not the COVID side, but on cybersecurity, best practices and mitigation and all that.

D'AMBROSIO: Yeah, no, absolutely Samantha. I mean, I think as Chris pointed out right in there, there are ways that people are sharing and they're getting through. But a lot of it really is human based. It still is who you know, how do I get involved in the different ISACs and the different type of fusion centers. Most people here, have spent some point in federal government and you see it's a large bureaucracy and it can get challenging. Who do I, when do I call them? Is this a regulatory issue? How does this all get sorted out? And I think the federal government it's really incumbent upon us to get out there and make it clear how the federal government can support and what are some of those clear lines of communication.

And then there is something on the victim side as well, which I'll get to in a minute. So, one of the things is we've been doing a lot of work with both CISA, Cyber Information Security Agency, and the FBI in trying to clarify what really is the role between CISA, between the FBI, between the secret service. The FBI has their task forces. We have our task forces. The CISA has their PSAs out there, right? We look at it and we look at CISA and we say, "Hey, their role is they're reporting in a fusion agency that's getting this information out. It's up to law enforcement to share what we can that doesn't interfere sort of with ongoing investigations with that." The FBI and the Secret Service have been working very hard. We're sort of making a big play that the National Cyber Investigative Joint Taskforce should be the place to deconflict on cybersecurity investigations. CISA should be the place where we provide best practices, trends, intel that comes out to help state and local municipalities.

The other key piece of this though too then is understanding from a victim standpoint, that what is the information that you can share? What are the protections that you can share? And that the federal government does have a capability to come out and help. But you are the victim. Just like in a street crime. If you don't report, who did it to you, then the federal government has a hard time coming out and helping you.

So, we need sort of the information flow to go both ways. The federal government needs to be a little bit clearer, work more together as a whole, and we're trying to do that. And then we need the victims to understand that they are victims. And that there is a benefit in contacting law enforcement in order to share information.

There's also a couple of things that need to obviously be looked at. There's always challenges with classifications of data. Getting that particular information out. And even just investigative sensitivities that need to be worked through as well. But all of those, generally speaking, with building relationships with some trust can be overcome.

RAVICH: Chris, you had a comment.

RODRIGUEZ: I think those comments are spot on what Michael is saying, and I'd be interested in what Tim has to say. I think what my experience in being in the federal level and now at the state and local level in two – or one and a half states – is really that the federal government can help us more by sort of building up our indigenous local capacity. And I was sort of a little bit heartbroken that in the latest round of Homeland Security funding, the FEMA, in particular, had a requirement that 5% of the grant of the FEMA UASI grant has to be spent on cybersecurity without giving States more. So, you're basically – and I know I'm speaking for my state hat and not from a federal hat – but CISA is a great resource, I think for training and for information sharing and for best practices. But the challenge I think is that each state has different structures and different requirements, different challenges. And so, I think the more resources the federal government, yes, mostly in terms of money, but also information sharing can really help build up that capacity because as I mentioned, we are on the front lines, and that type of assistance is really critical as, look, we're dealing with governors or mayors that are now in the midst of a global pandemic and cybersecurity, it's a tough sell. You're basically trying to convince a politician, a policymaker to plan for something that might not happen with money they don't have.

And so emergency management is the same way. It's a very difficult tradeoff for some of our local authorities and elected officials. So, anything the federal government can do to sort of buildup indigenous capacity within the local jurisdictions is very helpful.

RAVICH: Yeah. Tim Eisler, then we can go to Tim Roemer because I'm sure you have something as well.

EISLER: Yeah. I was just going to say, for us, the regional information center was a key asset when we learned that we were under attack. And so, they coordinate with the Sheriff's office and the federal – so that was a great resource that we leaned on immediately. The Sheriff's office actually helped us make that connection. And that was a great team, really kind of helped us liaison to the FBI. We actually just had a discussion with them and they shared some information about the tack and where its origination came from and ways to mitigate it.

So, that was a really helpful resource. And I don't know that all municipalities know who their RICs are or how to get ahold of them. But I think that's an important liaison piece that really connects them to the municipalities to the federal resources. So that was a big piece, big colorful piece in our situation. The other piece that I find useful is getting on the Secret Service, I think it's the SSTF or FT LISTSERV. So, getting information bulletins from them as they come out, I get those almost weekly, it depends on the activity, but I get them periodically. And I find those really, really helpful. That was kind of a chance encounter by meeting someone who happened to be connected and said, "Oh, you should be on the LISTSERV."

So, it's a useful tool and it's good information coming from the federal side, but the way I got to it was just complete randomness. So maybe a national registry for municipality IT managers where they can say, "I want to sign up and get this." Because it's good information. It's just a lot of people don't know what's out there.

RAVICH: Yeah. Good idea, Tim Roemer.

ROEMER: Well, I'm in complete agreement with my colleagues on this one, but just to reiterate what Chris was saying, it's really about helping those smaller municipalities and those locals underneath that state perspective because when you're the state CISO where Chris gets to do it for the District, you have a decent amount of resources at your disposal, but when you go into a state and you go to the more rural counties and the smaller cities, they don't have cybersecurity teams, they barely have an IT staff. And so, where the federal government can really help is with those locals and helping give them the resources that they need. We've done a lot within the last year in Arizona to get more grant funding from our Department of Administration to the smaller rural counties, especially the school districts. We're seeing school districts are a huge vulnerability and criminals are going after them.

And I'd love to see more ways to get funding and resources to the locals that really affect all of us to be able to help them would be huge. And so, yeah, I know from the state of Arizona, look, we don't have it all figured out. Sure, everyone could use more resources, but the smaller you are, obviously the worst situation that you're in for sure.

RAVICH: Yeah. And I think the point that Chris brought up which is like when you're facing down the barrel of COVID to hive off money for cybersecurity, it's a tough sell. Well, partly, it's tough sell because there's too many people that don't understand the knock-on effects of how hard our life will be, would be, if we had a major cyber disruption, with COVID or without COVID. In the dark, not able to get your medicines, not able to get food from Wal-Mart, not able to get money from an ATM, all of these things. So, it's one of the things I know everyone on this panel tries to do is to get that understanding, that kind of mindset of, we don't have to be helpless. This is how bad it could look. We can do things to mitigate and prevent it, hopefully, mitigate it if it does happen.

So that's one of the reasons why we have panels like this to really draw that out for the viewer to understand what needs to be done. Another aspect of communication I want to also go back to Tim Eisler, a conversation that you and I had last year in the midst of rolling blackouts from that fire season, and our hearts go out to the folks in Northern California that are suffering from this fire season. And you had mentioned that during that last fire season blackout, from PG&E, that you had to activate your amateur radio connections from your city and others. And it was something that I had never focused on, that amateur radio was a way to be able to communicate and that there are these active networks. Could you take a moment to kind of explain what that is and how that worked?

EISLER: Certainly. So, it's actually a pretty cool thing. Our emergency operation center has a dedicated citizen who has a ham radio license. And there's a couple of backups to that. And we keep their equipment, they actually own the radios, but we provide the infrastructure to run those. So, they have their own room in our emergency operation center. And when we do drills, they come in. We've got a couple antennas for them and a nice radio. So, they're the backup communications between us, the county and the state or between other municipalities. So, if all else fails, the phones go down and the cell phones go down, the internet goes down, we've always got the ham radio operators. So, they're an integral part to the OC. They show up for all the drills and they'll show up in the actual activation. And there's, I think at least three of them dedicated to us so they can run in shifts.

So, it's a very cool technology because it's old and it works. And it's a way to communicate when all else fails. I don't think we've ever had to rely on them, but they're always there and at the ready, and they test and they communicate with their counterpart at the county or at the higher organizations when we need assistance. So, it's pretty cool thing. The downside, I think is that that's a hobby for a lot of people and that generation is getting older and there aren't as many new people coming into that. So, I know they've made the licensing a little bit easier, you don't have to pass Morse Code anymore to get your ham license and they have workshops where you can get your license and a radio all on the same day. But I think that needs to be encouraged a little bit more. And I see some of the younger generation kind of going back to analog hobbies with analog photography, so maybe we just need to encourage more people to get into this. So, we always have that backup.

RAVICH: I think it's a fantastic suggestion. After we talked, it became on my list, get my amateur radio license. And after you and I talked, I looked it up. It was a critical part of FEMA delivering aid in Puerto Rico after Hurricane Maria, when again, no power, no telecoms, the cell towers were down, that amateur radio was the technology that was relied on for that emergency. And again, at the Cyberspace Solarium Commission, one of our recommendations on Continuity of the Economy looks at what do we have to have as backup analog systems in the event of a major cyber disruption so that we can get our economy back up and running as quickly as possible.

So, the question I want to ask Tim Roemer, when we also look at cyber disruptions, we of course, look at the resiliency of our supply chains. And how do we go about getting what we need back up and running when there are disruptions in the supply chain? Clearly everyone on this call kind of understands the supply chain disruptions with PPEs and others for COVID. Tim, an announcement recently that Taiwan Semiconductors is going to build a very large fab, a world-class fab in Arizona. And as you kind of put the pieces together, the supply chain resiliency for this new endeavor, but also recognizing that a potentially an outside state such as China may not want this to be the success that we all want. So how do you kind of put those thoughts together in your head and what kind of reliance would you look to for the federal government to help you as you think through this from your seat in Arizona?

ROEMER: Thank you for bringing that up, Samantha, because this TSMC announcement of a nearly or at least an estimated $12 billion investment into this facility is not only huge for the state of Arizona from an economic perspective, but also as an American, it makes me really happy that the United States of America will get this facility as opposed to going to someplace like China. So, you mentioned the supply chain and how important that is. Well, these microchips are essentially used in our most important pieces of technology, including our smartphones. If all of those manufacturing facilities are located in a certain region in the world or a certain nation that can either directly decide not to share those products with you anymore, or during a pandemic, for example, what if your human workforce, we're talking about the human element a lot in this call, which I think is great.

What if the human side of producing those microchips goes down in a pandemic or a natural disaster? Or what if it goes down due to national security concerns and tensions with another state? In order to have the resiliency of the supply chain for something like micro chips that are so essential to all of our technology companies including Apple, we need those facilities to be in the United States. And Arizona's thrilled to be getting that investment. Now, the real hard work comes in though, because now we need to partner really closely with our federal partners, including the FBI, and we've begun having these conversations with them. We need to start talking with our universities and even our community colleges, anybody who's pushing through degree programs for the talent pipeline in the workforce development, if you will, because when that facility gets up and running and let's say three to four years, they're going to need to hire those human beings.

They're going to need the staff to come in and operate them. You're going to need to make sure that you've already put in place processes and procedures to protect not only the individuals, the overall organization and the products that are coming out of it. So, I mentioned that you want the facility to be in the United States and all the different reasons why, well, the supply chain could be manipulated by somebody in another country, but we can't think that just because it's in the United States, it can't be manipulated here as well. Nation state actors or terrorist organizations are always trying to find ways to infiltrate our organizations to get a leg up. We know China is stealing our intellectual property and we've been working closely with our universities here, especially on COVID related research to make sure they're aware of that and how to protect it.

But when it comes to a facility that's got a $12 billion investment, you're going to need that human investment. You're going to need to start keeping in mind the counter intelligence perspective, making sure that who you are hiring to be part of these facilities, to be part of the programs are cleared and vetted, and that you've got those good policies and procedures in place. And we've also talked a lot in this call about information sharing. We're thrilled in Arizona that we just started partnering with our state fusion center to build a cybersecurity team and build that information sharing up. It's going to need to really go through the roof with a facility like this coming to Arizona, because we're going to need to make sure that there is constant communication. So, when the federal government, when Secret Service or FBI, or CISA is warning something about a vulnerability that we get that information to those involved in this project, but also again, it's that human side of it.

There's going to need to be a lot of education taking place for people that may not have ever worked in this field before. We're lucky to be on such a great call with so many great colleagues and I'm so impressed by this panel. I know Chris Rodriguez and I both come from a human intelligence agency background. So, I think in these types of situations, we're going to need to tap into those leaders at the local levels that have some experience there and be able to facilitate as a liaison with the law enforcement agencies because if you've never done it before, my colleagues have hit the nail on the head today.

It's about building the trust, but if you don't know who your special agent in charge is of your Arizona office or whatever state you're in, you're not going to have the trust to immediately hit the ground running and say, "Sure Tim, I want to start telling you about all the threats coming into this facility or you trust me to share back with me." So fortunately, in Arizona, we've got a great relationship with our federal partners and intelligence sharing, but it needs to be improved. It needs to be increased always. A facility like this is too important, not just to the state of Arizona, but to the United States and a lot of our allies as well.

RAVICH: I think those are fantastically important points. Tim, the U.S. taxpayer, the population of Arizona are going to be critical to making this a success, but understanding the wraparounds for cybersecurity and counter-intelligence purposes right from the get-go so that we don't build a facility for the benefit of our adversary is absolutely critical. Mike, I think you wanted to jump in also to talk about the importance of the local populations in helping our security and in this perspective or in the last conversation.

D'AMBROSIO: No, what I think Samantha and Tim just talked a lot about it, is Tim and Chris, the federal government's got to support the state and locals. One of the things that I go back to sort of the NCFI when Louisiana had the attack, the ransomware attack, the response was the state response of an individual that recently graduated from the NCFI. He was empowered with the equipment and the knowledge from attending that to actually prevent the spread of that attack. They were able to start school on time, because he was able to get in there because he was given, by the federal government, but to a state and local who was able to respond right to that attack.

The other piece that we haven't mentioned yet is the importance of the state National Guard. You're starting to see state National Guard agencies take a lead role, sort of in the preparation and the response to cybersecurity type of incidents within the states. They're building that capacity. And then that's a natural link back to the federal DOD space in order to tie together all of the things that we're talking about today.

So, I just think it's important that, to Tim and Chris's point, the federal government does have to empower state and locals. And we have to do it with training and education, but also the equipment and the capabilities and the capacity.

RAVICH: Yeah. Because, so we have about five minutes left, and what I want to focus these last five minutes and hear thoughts from each one of you, is kind of keying off of what Mike just said, but if we titled this panel SLTT, state, local, tribal, territorial, but it's missing something on the front end, two on the backend. So, it's actually, the continuum with the federal on the one side of that continuum, and then also corporate and citizens. So, it's not, SLTT is fine, and it captures a lot. But where does federal fit in? And then of course, where do the corporations and the citizens themselves? Because this is a continuum when we're talking about cybersecurity.

So, let me start with you, Chris. In that notion, you can go back to what Mike's point on the Guard, and you and I have had discussions about that, but in so many hats that, of course, you wear, you have to get the word out to have the citizens of the District of Columbia, and also in your AOR for Virginia and Maryland, the corporations. There's a lot still to be done. So just give us some thoughts on where attention should most be focused.

RODRIGUEZ: Thanks for the question. And I'll be brief because I know others are going to want to join in, but I think on the, we've spoken a lot about the federal government. I see the federal government as enablers, as force multipliers in this fight for the states, in particular, and the local jurisdictions. For the private sector, I think that there is a lot that, and I know, Mike, I know that Secret Service has done a lot of outreach to the financial sector in particular.

And I think. From a state and local perspective, we do have to leverage those relationships. Again, I think it is more of building that trust with the private sector. And in my experience, I've found some to be more willing to share than others. And I think, again, that is just developing trust over, not months, but years, and making sure that you can get access to information, even if it's just the brief.

So, because if the state or the local jurisdictions have an idea of the types of challenges that the private sector is facing, there's a lot that we can learn. And I've found the private sector to be very cooperative on things like training and just information sharing exchanges, rather than sort of more of the behind the curtain aspects of their facility. They've also been very helpful to us in the District about how to organize our cyber response and sort of taking lessons learned from how they do that from an incident management standpoint and a consequence management standpoint. So that's been very helpful.

RAVICH: Thank you. Tim Eisler, I want to continue that conversation that Chris just started on the corporate side, I think you can see Silicon Valley with binoculars maybe from where you stand.

EISLER: Certainly, there are plenty people work there that live in Dublin.

RAVICH: Right. But am I correct in saying that they have to be kind of maybe more part of the conversation when we're talking about cybersecurity infrastructure across the board and how it would affect you in your city and protecting your population?

EISLER: Absolutely. And working with some of our vendors to look at hardening our environment or increasing capacity to enable work from home without difficulty, looking at grants. One of our vendors suggested there could be some grants for hardware purchases that would certainly help out the municipalities. Grants for a security operations center, managed service environment. I don't know that a lot of municipalities can have – a lot of this stuff is unbudgeted. Things that we're doing this year are just emergency funding. They were not part of the natural budget. So, we're having to scrape money to do the things that we wouldn't have expected to do otherwise.

Interesting, working for a local government, we're the direct line to the citizens, to the community. So, one of the things I think is interesting that Dublin is doing is providing Wi-Fi spots to school children. So, using our parks and rec facilities that are now closed because of COVID, but setting up spaced areas so that parents can drop their kids off. So, they're still distant learning, but now they have a dedicated place they can go with a strong Wi-Fi and do their classwork. The parents can go to work. There's a supervisor there to make sure the kids are okay. So, I think that's a great outreach that municipalities can do. And by using our Wi-Fi, that's protected behind firewalls. So, we're actually providing a service to the citizens that's probably more secure than they would have at home. So, I think programs like that, especially during this COVID, are a helpful piece to the citizens.

RAVICH: Thank you. Tim Roemer. The Governor Ducey has really been a thought leader on a lot of what we were talking about today. What else do you want to highlight from your experience in state of Arizona?

ROEMER: Well, thank you, Dr. Ravich, and all my colleagues, and FDD events for hosting this. This is a huge part of success moving forward on this topic. We can't stop having these meetings and conferences just because of COVID. We can do it virtually because this information sharing that we've talked about today. The perfect example of it is on this call today and getting this information to as many people in power, or just typical citizens that are out there, and they're interested in the topic. I think after 9/11, the nation responded with a lot of funding from the federal government to help state and locals.

And I just hope that we don't wait for a cyber 9/11 before doing that on cyber. I think COVID can be the wakeup call on cyber because we're starting to realize that when it comes to critical infrastructure, we always thought, in Arizona, for example, okay, let's protect our critical infrastructure. And we thought, okay, well that's our Palo Verde nuclear facility. Okay, yeah. That's pretty obvious. But we weren't thinking that it was the grocery stores and the CVS. But when you start thinking about it, that means virtually, because how are people getting their groceries? Well, a lot of them are getting it through Instacart or Amazon and other ways. Okay, so how do you secure that critical infrastructure? Well, you do it with cybersecurity. And cybersecurity needs to start being as just a high of a priority as overall technology is.

And so, in Arizona, a specific example that I'm so proud, and I'm so fortunate to be in Arizona under Governor Ducey's leadership, and director, Andy Tobin of the Department of Administration, my boss. When I first came into my role, one year ago, he immediately made me an Assistant Director of the Agency, took me out of the organizational chart that reported to the CIO. And he said, "Cybersecurity is too important. You don't report to the CIO anymore. You report to me. I'm the head of the agency."

Now, that was amazing because not only did it allow me, from an org chart perspective, to take security issues directly to the head of the cabinet, if you will, for my agency. But it sent a symbolic gesture to every single state of Arizona agency and all their information security officers that we take cybersecurity seriously. We will listen to you. We will invest in this topic, and that we will give the needed resources into this. So, I think one of the things we're starting to see now nationwide, and even in the private sector, is private sector companies saying, nope, security shouldn't be under technology. Security should be its own stand alone, and security should report directly to the governor or directly to the head of the agency. So, I thought that was an innovative way to prioritize cybersecurity. And in 2020, in a post-coronavirus world, I think this is going to be an area that I'd like to see government organizations and private sector organizations learn from and use that as a best practice.

RAVICH: That's great. I think it really does kind of open our eyes to it is an enterprise wide risk. It cannot be hived off. It has to be fully baked in.

Mike, kind of last words on the conversation today, and how you want the audience to leave this conversation, thinking about Secret Service in this regard?

D'AMBROSIO: Listen, I think one of the things that Tim said there is something that everybody has to understand. When we think about cybersecurity or critical infrastructure, we're generally thinking about those large-scale organizations, but everything today is connected. Most of your organizations become vulnerable through a connection that they may have with some third party, or third-party vendor that they're dealing with. And so, cybercriminals have learned, we're not going to go after the large financial institutions. They actually have robust infrastructure when it comes to cybersecurity. You heard Tim Eisler talk about municipalities. Why have municipalities and hospitals been targeted lately? Well, generally speaking, they're not putting in because they don't have the funding and the resources to put into their infrastructure. And so, I think understanding that is key.

And understand this too. Most of the cybersecurity incidents are not zero-day vulnerabilities. They're due to basic cyber hygiene sort of vulnerabilities that have been created. So, to Tim's credit there, they're really doing some things when it comes to phishing and trying to close down those vulnerabilities.

I will tell you this, here's where the service priority is going forward as it comes to cybersecurity. We want to increase the resiliency of those that are out there doing so. And so, one, it's sharing of information. Tim Eisler talked about some of the alerts by joining the task force. I think there needs to be more holistic efforts so that everybody's getting sort of the same information that's going out there. We're doing a lot with training and education, because if we can get out there, and we can do the training and education, it does a couple of things. It builds trust. So, people were facilitating the sharing of information. We're doing training and education. And at the end of the day, we want to do proactive law enforcement. Somebody, at the end of the day, for conducting these activities has to go to jail or has to be prevented from doing so.

And so, all of these things that help us strategically target those transnational groups that really targeting the U.S. infrastructure. And so that's where the services is focused. We're doing it in conjunction with our state and local counterparts. We're doing it in conjunction with our other federal agencies, really trying to bring a holistic approach to it. So again, thank you, Samantha, for hosting this particular group. It was a pleasure.

RAVICH: Well, it was my pleasure as well. It was really a terrific and important conversation. And I'm not sure how many of these conversations are being had with this breadth of experience that you all brought to this. So, I thank you very much.

And with that, we will conclude. But I'm sure we will all be in touch. So, thank you. Thank you very much. All right, bye.