FDD EVENTS

Hard Water: Increasing the Cyber Resilience of America's Water Supply

Featuring Tom Fanning, Fred Humphries, and Dr. Kevin Morley,
Moderated by Dr. Samantha Ravich
Introductory remarks by RADM (Ret.) Mark Montgomery

MONTGOMERY: Hey, good afternoon, everyone. Thank you for coming to today's event hosted here by the Foundation for Defense of Democracies. It's Wednesday, December 13th.

Today's panel is here to discuss the cyber risks facing the water and wastewater sector and how to improve the cyber resiliency of this critical lifeline infrastructure.

I'm Mark Montgomery. I'm the Director of the FDD Center on Cyber and Technology Innovation and Executive Director of CSC 2.0, an initiative to continue the work of the Cyberspace Solarium Commission. And on behalf of both FDD and CSC 2.0, I want to welcome those of you joining us here in person and on the livestream. In addition to FDD and CSC 2.0, today's event is co-hosted with Microsoft.

As we've seen over the past few years, America's adversaries know just how vulnerable our water utilities are. In fact, just recently, Iranian hackers breached poorly-configured equipment across as many as 10 water utilities. FBI Director Chris Wray recently warned that Iran might target U.S. critical infrastructures as the war between Israel and Hamas continues, and that's exactly what we're seeing.

It really doesn't matter that many water utilities are small, and it certainly doesn't matter that they don't necessarily serve a military infrastructure. Hackers know that if they can stoke fear and cause real damage, affecting the lives of ordinary Americans by corrupting our water systems, America's water infrastructure doesn't have the cyber resilience necessary.

Which is why, over the past year, we've collaborated with Microsoft to host a series of virtual roundtables focusing on understanding the challenges and developing solutions to the cybersecurity problem. We convened experts from across the federal government, across Congress, as well as from the water utilities and technology centers, many of whom are here today.

We've discussed the threats to water sector, the international obligations to protect the sector from cyberattack, best practices to reduce cyber risk, and how to build greater cyber resilience. We're pleased to publish the findings of that roundtable series here today. In fact, there's a book – books in the back of the room with copies of the report that are available, and there's a link on today's event page for those doing this remotely.

Before I turn the conversation over to Samantha Ravich, Chair of FDD's Center on Cyber and Technology Innovation, and herself formerly a Commissioner of the Cyberspace Solarium Commission, let me share with you three of the recommendations from the 13 that were in the Microsoft-CSC report.

First, we need to better resource and direct federal government efforts. The EPA [Environmental Protection Agency] is starting to step up to the plate, but it needs significantly more funding, expertise and authorities. They can look to the Department of Agriculture, who has done some programs for water utilities, working with the National Rural Water Association.

We need to look for better public-private collaboration. This includes things like government industry, joint government industry oversight in a standard setting to develop industry-led standards for application through third-party testing, and more research funding for water security test beds to focus on operational technology and industrial control systems.

Finally, water utilities themselves need to invest in cybersecurity. Many can access federal or state funds to make these investments if they know how. Others needs to take advantage of free cybersecurity resources that are provided by EPA, by water associations like the American Water [Works] Association, and training provided by the – by cybersecurity firms and nonprofit organizations, like the Cyber Readiness Institute.

On that last point, I just wanted to say that CCTI is pleased to partner with the Cyber Readiness Institute – it's led by Karen Evans, in fact, one of our CCTI board directors as well – and by Microsoft to provide free training.

There's a lot that needs to be done from the top down, but we can also improve the water sector cyber resilience from the bottom up.

And now I'll introduce our esteemed panelists.

First, we're pleased to have here with us Tom Fanning, the Executive Chairman of Southern Company for some period of time more, and himself a commissioner on the Cyberspace Solarium Commission.

Fred Humphries, Corporate Vice President at Microsoft – as I said, an organization that helps significantly with these nonprofit efforts – where he oversees strategy and government affairs, outreach and a range of technology policy issues, including cybersecurity and artificial intelligence.

Kevin Morley, Manager of Federal Relations for the American Water Works Association, the largest organization of water experts in the world, representing utilities that provide water to more than 80 percent of all Americans.

Finally, a few words about FDD before I turn over to Samantha. For more than 20 years, FDD has operated as a fiercely independent, nonpartisan research institute focused on national security and foreign policy. As a point of pride and principle, we accept no foreign funding. For more on our work, please visit our website at FDD.org or follow us on Twitter at – or X @FDD.

And now, Samantha, it's over to you.

RAVICH: Well, thank you, Mark. Before we get started, I just want – since Karen Evans missed the shout out because she just walked into the room, I just want to give her an additional shoutout. She's truly fantastic and important in all the work that we do here.

OK, so great. Thank you, Mark. Look, there's over 150,000 public water systems in the country, right? So, we have to cover a lot of ground or a lot of water in the next 50-so minutes. So I really want to jump right into it. So, I'm going to – you know, I'm going just start with Tom.

OK, you're from the energy sector – no offense. You're not from the water sector, you're from the energy sector. So why are you here? Why do you think this is important? How are you involved with this?

FANNING: I get the question, "what are you doing here?", a lot.

(LAUGHTER)

It's very clear to me. And I want to go back to the mission of the original Solarium Commission under President Eisenhower. It was on the aftermath of World War II and we had, looking at a map, the Soviet Union on the right and the emergence of NATO on your left. And the imagination was a conflict on the plains of Poland, the tank battle.

And what we see now in this digital world that we all live in, that the battle is not on somebody else's beach, it's right here.

I guess I'm still Executive Chairman of Southern, and that will end at the end of the year. But we get attacked three million times a day. And I know a whole lot of other companies do as well. And so, the battle is not protected by an ocean on the right and the left and friendly neighbors on the north and the south, it is here.

And so, I think one of the big ideas of Solarium was that we had to reimagine the notion of national security. The private sector cannot rely upon the federal government to do our work for us. We have to collaborate.

If you look in the Cyberspace Solarium Commission, we intentionally did not use the word “cooperate.” It is collaborate. We have a joint obligation to protect America.

OK, now, as I started now over a decade ago, leading the electricity sector, very quickly, like, within a matter of months, I realized that living in a silo, worrying about electricity on its own is completely ineffective. And so, we started an effort to find likeminded souls around the United States. And son of a gun, we did. Electricity is absolutely dependent upon communications. Finance is absolutely dependent upon electricity, and so on and so on.

So, when you consider your silo obligation, your silo risk register, if you will, you very quickly understand we are absolutely interdependent with each other. We can’t live within our own reality. Our reality has a first, second, and third derivative that involves everybody else, especially water.

And so, we need for water to be successful. Otherwise, we will not be successful. Otherwise, the national security of the United States will not be looked after as it should be.

RAVICH: That’s just brilliant. And, you know, we are so thankful for Tom’s leadership, again, not just on energy and on cyber and its connectivity to it, but really understanding that this all links together, right? If we are going to have a prosperous economy going forward, we have to understand this interconnectedness and the attacks that are upon it.

Which brings to me to talk to Microsoft, the man from Microsoft, Fred. And so, over the past year – because this also shows – showcases just how important this subject is – Microsoft partnered with CSC 2.0 to host a series of discussions, as Mark mentioned in his introduction.

Why was this a priority for Microsoft? And why were you concerned enough about this effort on water to launch this effort?

HUMPHRIES: Well, first of all, I got to do just a – please make sure you get the report. It's out there, I saw it. That’s great. All you have to do is read what’s on Page 4. It’s got the executive summary for you all that do a lot of reading, but it’s only 20 pages. So, please do that.

I think there’s multiple reasons why Microsoft engaged on this in this partnership, and I think it was four different discussions that took place.

One, from a customer perspective, I mean, when you think about just the importance of cybersecurity and cyber resiliency, it’s so, so important to us from the customer piece.

Another aspect is that, you know, water is like a part of the critical infrastructure. It’s a critical, critical piece. It’s important when you think about the downstream dependencies that take place as well.

And then I think the key – you know, it’s interesting – and it’s always hard to follow an executive chairman, because Tom really captured a lot of the different things in his – remarks – is that from the multi-stakeholder perspective, that it’s a very, very important, as well, as you look to solve, right, the different aspects that can take place.

In my 23 – yesterday was my 23rd year at Microsoft, and got to work – I get to work on a lot of different things, this new thing called AI aspect. But it’s evolved on different aspects. But when you think about cybersecurity, the cyber issues that we have in front of us and the nation state attacks that are – that are taking place, and what are they focused on? Water aspect is real.

And so, between customers, the dependencies on water, the – just the aspect of candidly the vulnerabilities that you have to deal with from the small, I’ll call them – correct me if I’m wrong because I’m not Mr. I have all the language right to describe, you know, water entities or utilities, the –

(CROSSTALK)

Thank you, sir. I like your socks too.

(LAUGHTER)

And so, those are – you know, that's a – we're – a lot of exposure.

And so, for that reason, hey, we want to be out there and as well as other companies, just not do this Microsoft commercial. Others are very focused on this.

RAVICH: So Kevin, I was going to say, you know, like they say on TV, ripped from the headlines. But I think that totally dates me, because if you're not reading your paper, an actually paper …

FANNING: Right.

RAVICH: … you can't, you know, rip it from the headlines, I think.

But in all seriousness, Iranian cyberattacks have been targeting small U.S. water systems. And I've seen some reports kind of downplaying these attacks – and you know, and it struck me – yeah, if someone throws a brick through my window and it didn't happen to hit my child and it just lay on the floor, I don't kind of, you know, brush it off, like oh well, whatever.

But there's this kind of – like, it didn't cause damage, so, you know, maybe we shouldn't be worried about it as much. I'm not so sure about that. I don't think you're so sure about that.

But as our water represent – industry representative, you know, shed some light on what the sector is seeing these particular attacks, what you're most concerned about, you know, not in these attacks but also what it could signal what might be coming down the pike. And, you know, what else you can talk about on this subject.

MORLEY: Sure.

RAVICH: Thank you.

MORLEY: I have great socks.

RAVICH: You do …

(LAUGHTER)

(CROSS-TALK)

MORLEY: No, I think that, more seriously, it is not something to be dismissed …

RAVICH: Yeah.

MORLEY: … and I think it's important to recognize that it is a – an –interesting tactic that was taking place. Very unsophisticated but it is alarming, in the capability that it –could have propagated. And, you know – and it's not an issue that is unique to the water sector. There was a brewery that they started messing around with too. So they're messing with the beer.

But again, it's – the issue and the fundamental functionality that was targeted is a – is an issue that can be propagated in any sector against any PLC [Programmable Logic Controller]. They all have default passwords, right? And so how do you manage access to these things becomes very important, which comes back to a point that myself and my colleagues and the sector have been advocating, on the need for directed resources, such as the one that you were talking about, to facilitate for these smaller systems that may not – that – you know, they don't have an in-house IT [Informational Technology] or operational control department. They have some folks that are doing things. How do we facilitate and enable them to implement these best practices?

So, there is a resource and capability issue, and we've been very proactive in providing those resources and trying to get that out. Like you said, there's 150,000 water systems. That's a lot of boots on the ground. You know, myself and my colleagues, we can't talk to everybody all at once.

So I think it's a shared effort. I'm glad to hear the program that Microsoft's been sponsoring with you all to provide some of those basic services, but it comes back to some of the really good services that are available from CISA [Cybersecurity and Infrastructure Security Agency], right, like the Vulnerability Scanning Service. That's a huge benefit. So how do we get that – how do we have a shared message to get those resources out and implemented in the field, right?

We have lots of checklists. They've been around for a long time. Implementing those checklists is where there's a little bit of friction in – you know, necessarily in some of these smaller entities. They're not cybersecurity experts. They're water utility operators and they're very good at what they do. We need to work collectively to get them into a place where they can actually implement these things in a way that they know is not going to compromise continuity of service.

RAVICH: But before – I want to tease that out a little bit more, but before we get to it, let me just again go back into doom and gloom for one moment. How serious do you think these attacks could become if we don't do something?

MORLEY: I think it – to – you know, what Tom was talking about, I think these are – it's a very interesting and new direction of a directed attack on a supply chain target, and it could have huge implications across multiple sectors. It is not to be taken lightly.

Thankfully, many of these systems, because they are older systems, actually are able to switch over to manual control. This is cyber-informed engineering, some of the things that we've been talking about with Idaho National Labs, which is great.

And there is a weird, interesting kind of inflection point of technology transformation where some of the things that we're putting into systems, whether it's electric or water or what have you, there is no manual capability.

So we're setting ourselves up for a potential continuity of operations issue that – if we don't think through secure by design on a go forward basis.

HUMPHRIES: Can - can I – can I jump …

(CROSSTALK)

FANNING: No, go ahead – go ahead.

HUMPHRIES: You know, as I think about some of the things regarding AI and as we look at it, you know, we have a Microsoft cybersecurity co-pilot. I had the pleasure, oh, to see 27 different demonstrations of what we have in the pipeline – we have that now, that's not in the pipeline – on different AI solutions.

One of the things, as I hear you, that you always worry about on these autonomous systems or whatever you might have in place what we call our cybersecurity co-pilot, is that there still needs to be a human engaged, even with – you might have more efficiency and other things that AI can detect from, you know, the – that threat aspect, that's something that's actually real important, that you're highlighting that needs to be a part of the design to be able to detect.

FANNING: Yeah, but I think he also said that one of the defenses you have is to go manual. The electricity system in the fifties was running a manual way. And one of our layers of defense, the big kind of crown jewels of electricity, is not nuclear plants or any of that stuff, it's the electricity management system. Southern Company is about the size of the nation of Australia from an energy production standpoint, whether it's electricity or natural gas.

We control the flow of electrons all across the southeast. If they could get that – so we have a system, we have a – we have a place called – well, it's – can theoretically survive big bomb attacks, all kinds of things. We have another undisclosed location in Georgia that – you know, EMPs [Electromagnetic Pulse] and all that other stuff.

The third thing we have is called Spare Tire, which can get you from the blow out on the highway to a gas station. Wouldn't want to run a power market on it, but son of a gun, it worked for five or six days. And then we have finally MacGyver, and MacGyver is our way, if we can't trust communications, that we could unplug and run manually.

And so we have all that stuff, OK? So you've got to be able to do that. It – that's not, in my view, kind of this interesting option. That is an obligation that you have, to be able to think through, not just prevent. Remember, your cyber defense is all about your human body. You've got a lot of stuff about your body that's – keeps stuff out. Your body also had – handles bad stuff when it gets in. So do you have those measures? Do you have a way to completely obviate the connection to the digital world?

The – one more thing I just want to say – some – we get trapped. And as I was listening to you – and I'm going to – I'm certainly not criticizing – but it sounds like cyber sounds like it's something that is out here and I'm not responsible for it, and then it comes in and a – oh, I have to think about cyber now.

In the Cyberspace Solarium Commission, I remember [Fmr. Rep.] Langevin and I went back and forth a lot about this is an obligation of every management team that exists and every board that exists. It is 100 percent an undivided obligation of management. It is a legal obligation. And we were saying oh, this should be part of Sarbanes-Oxley [Act] in your evaluation of an effective control environment, for heaven's sake.

These are cultural changes we're going to have to make in the private sector.

HUMPHRIES: Pick – picking up on your point, I mean, one of the things we've been advocating when we talk about just AI in – generally and AI in cybersecurity as well is the notion of safety breaks or you know, that you can go in and just say hey, we're – manually, we're shutting this down, you know, aspects. So I think the things that you outline prescriptively there, I think you're spot on.

MORLEY: Just to add to Tom's point, you know, about – we've been very vocal about, even in the absence of a – an explicit federal statutory mandate in the sector, there is a fiduciary responsibility for the utility, as part of their general business practice of managing the cyber risk.

FANNING: Yes.

MORLEY: So totally agree with you.

HUMPHRIES: Yeah, but – agree, but pragmatically, as you were talking earlier – we were talking on the small and mid-size, right? You know, they're running into just the economics of…

MORLEY: Oh yeah, there are lots of stresses on our …

(CROSSTALK)

(LAUGHTER)

(CROSSTALK)

RAVICH: … and I love the exchange and I don't want to shut it down. I …

HUMPHRIES: Nothing like something going organic.

(LAUGHTER)

RAVICH: … but I want to – I want to follow up on something that Kevin – he did call out cyber-informed engineering, Idaho National Lab, on – it and for those in the audience or those listening livestream, it does get to really changing a mentality about how you build these things, how you design these things, how people in an organization at every level have to take this into consideration. It is cyber-informed engineering. So it is not hanging out there and then it only comes – pokes its head up, you know, when something bad happens.

But it – Kevin, AWWA [American Water Works Association], where you work, has been thinking though about an industry-led standards body. What does that entail? And tell us a little bit about that.

MORLEY: Yeah, the devil's always in the details, but functionally, looking at our peers in the electric sector, right, back in 2005, they've moved forward with a process of normalizing or standardizing cybersecurity best practices, right?

And so from a governance perspective, that same – that co-regulatory model seemed to be a reasonable way to move forward and use the expertise within the sector for the people that manage these types of assets to contribute to defining "the what" on a tiered risk-based approach, given the scale and diversity of the sector, working with – and under oversight from EPA, as the SRMA [Sector Risk Management Agency], to move forward with a – on a reasonable path to institutionalize cybersecurity best practices across the sector with some baseline minimum controls to address some of these things, working with the small systems, such as what Representative Davis has introduced for the circuit riders, to help bring along utilities instead of just having a top-down punitive process, right?

FANNING: In fact, it can't be a top-down punitive process. If you live by regulation, regulation by its nature is always backward-looking. It is something that is already old, that was based on something that happened some time ago. We know – now to Samantha, to pull back on your age joke…

RAVICH: Your age joke.

(LAUGHTER)

FANNING: You did the – rip the headline.

RAVICH: Thank you.

FANNING: …was the idea of a lava lamp from the 1960s and '70s.

RAVICH: Oh, you're quite old, yeah.

(LAUGHTER)

FANNING: Yeah. But if you just kind of watch those things, for the hours that you will from time to time, depending on your condition …

(LAUGHTER)

… the thing is always moving and changing and you just kind of get transfixed by it. I mean, that really is the notion of changing attack vectors and changing attack surfaces of those things that we're trying to defend.

They're always changing. Regulation can in no way prevent an effective attack from hitting. And now go to AI. We know that new cyberattacks will come with a learning capability, and so if I throw a right cross, you throw a left jab, oh, I'm understanding now that you're going to throw a left jab, I'm going to do something different.

It's always going to change. And who has the best AI from an offense/defense standpoint? It's going to be really cool to see. This is fascinating stuff.

RAVICH: And there's a – let me follow up on that – there's certainly – you know, government is trying to figure out its proper place in this and alongside – you know, with the private sector, Tom, your tenure on CISA's Cybersecurity Advisory Committee just ended, but CISA's Joint Cyber Defense Collaborative has efforts on water.

So what kind of role do you see for CISA and other interagency partners supporting industry-led initiatives, like what Kevin was talking about, but also more broadly, so – in water – but also more broadly on cyber risk management?

FANNING: Yeah, so I chaired the CISA Advisory Board for 2 years, and just giving that up this year. It – it's fascinating. So this reimagination of national security, with the collaboration of the private sector with government, requires completely reimagined operational systems.

We have to train the private sector as to how to govern itself from a cyber standpoint. We generally believe that associations are not the place to do that, that it's got to be asset owners, people that have the asset at their disposal.

Failing that, associations are absolutely the right way to do it, especially if you've got 150,000, you know? And we've got to train government as to how to work with the private sector. The government does not know – I can remember GridEx. That's our – every 2 years, we do this giant war game across America. Just finished this last one. And I can remember, you know, you start with a small problem, and you grow the problem until you break the system. And at one point, the system broke, and this guy that I love, Tom Bossert, terrific guy – he was the cybersecurity guy on the National Security Council, and he is wonderful. He invoked the FAST [Fixing America's Surface Transportation] Act, where the government could take over the operation of the electricity grid.

Well, he invoked the FAST Act, and I said, "Tom, so what do you do now?" And you know, like, I don't know. Who you going to call?

The government doesn't know how to run the water system. They don't know how to run electricity. They don't know. The private sector must lean in and inform government. Government moves from being a regulator, oversight to being an enabler, to enable a fast response.

When I think about CISA, they have two great, big functions that are so helpful to this nation's national security. One is what we call the NRMC, the National Risk Management Center, that evaluates all the different risks within the silo of a sector and then evaluates the first, second, and third derivative risks. What are the interdependencies, and if that breaks, this breaks also, that kind of thing.

The second one is this idea from Solarium, the joint collaborative environment they call the JCDC [Joint Cyber Defense Collaborative], but this is where we have the Intelligence Community, sector risk management agencies, private sector, and then the guys that will hold the bad guys accountable – DoD, FBI, Secret Service, U.S. Cyber Command, you name it. And these guys all collaborate, aspirationally, in real time. Aspirational behavior is not done by regulation, right? Aspirationally in real time, so that we can illuminate the battlefield. That's the most important thing we can do.

Second, as we see the lava lamp of attacks come in, we start to get a sense of things we can do in the private sector to kind of get ahead, skate to where the puck will be, and take action before an event happens.

Thirdly, to the extent an event happens and we have that bad day in America, we now have a way to have an integrated response to get America off the ground and back on its feet.

RAVICH: But there are different size private companies, right? So – and so, on this panel we're talking about water. And, you know, as Kevin talked about, there's a lot – tens of thousands –

MORLEY: 80 percent in this. I mean, we're, like, the complete opposite of electric.

RAVICH: … and I'm going to get there - of small water utilities. I live in very rural Virginia, so I'm actually quite interested in this idea that Representative Davis is helping to jumpstart on a Circuit Riders for cybersecurity, for rural water utilities.

And so, I want to get to Kevin, but Fred, let me ask you a question on this. As you know, like, these small water utilities, they don't have support teams, right?

And so, in addition to programs like, we hope, the Cybersecurity Circuit Riders and a program we'll get to in a minute, Microsoft and FDD are working on with CRI [Cyber Readiness Institute], one solution, of course, is for the utilities to rely on technology providers, right, including cloud service providers, to provide them with the cybersecurity that they need, because they're the little guys. They – again, they don't have the teams.

So, what roles do cloud providers and other technology companies have? What does this say about the role of cloud as a critical technology for critical infrastructure? Microsoft President Brad Smith actually indicated that, you know, cloud itself should be considered a critical infrastructure.

HUMPHRIES: Let me start off on one thing that Tom was kind of talking about that ties into this …

RAVICH: Yeah.

HUMPHRIES: … to this question that, you know, you have so many leading technology companies in the world that – gathering a lot of information. We, the Microsoft Threat Intelligence Group – Council, MSTIC, 65 trillion signals a day – 65 trillion signals a day, monitoring, processing aspects, 125 million devices managed on our platform.

MSTIC is this small but powerful part of our company that collects a lot of information to be able to analyze on the threat piece, which would include water and aspects, as you were talking about the back and forth and the AI. So this is where, like, companies and knowledge that we have and working together, where there's some public-private. This could be a warning system aspect. And there's others who can do this as well. So, that's one.

Two, on a cloud piece, one of the things that the cloud can do is respond really quickly compared to on-prem. Can't do a whole lecture on that right now, but just on the abilities to do that is real important. And then when you take AI and what it allows you to be able to do as well is real helpful.

We have been advancing that this should be – particularly when you're thinking about cloud and AI, this should be a - what some like, some don't like, there should be a licensing aspect when it comes to critical infrastructure. Know what one is doing, as they are going to be that provider on the cloud. And there's competition alive and well in that space from an infrastructure perspective.

But, you know, when you're doing AI with a large language model, there's a lot of promise but there's some things that you need to make sure, right, someone has line of sight in. So, that's how we kind of look at it.

RAVICH: So, Kevin, when you listen to this – and you were shaking your head before when I was, you know, giving out the numbers, the large numbers of small water utilities. And, you know, this panel and the work that we're all doing is what capabilities can be used to help these small water utilities …

HUMPHRIES: Cyber readiness.

RAVICH: … well, that we're going to get to – we're going to get to that, but the – you know, the unique challenges, again, of these small water utilities and the numbers. I mean, I just want to underscore the point for – again, for the audience and those listening, live-streaming, how many there are.

How many of – American citizens, you know, reside in places with these very small water utilities?

MORLEY: Sure. Yeah. Not an unchallenging situation. And I think it's one of the challenges, right, and something to kind of keep in mind, is that in these smaller communities, right, it's a – these are primarily municipally operated systems. Not always. There's plenty of investor-owners too.

You know, they're part of a city network. So it's the utility, it's the county clerk's office or the city clerk, it's the school system, right? And so, there's a unified effort here to that overall best practice of how they manage those assets and how they're segmented and separated.

And I get – I come back to, you know, that's the reason why – so providing support for actual boots on the ground to go and help facilitate implementation of the things that we've been talking about for almost a decade or more – I mean, I'm pushing this stuff since 2008 – you know, we're not – in the water sector, we, as a federal government, have not invested in that capability, right?

And I'm not being critical but, you know, the electric sector is having some – has had some great success in getting direct support into smaller rural electric utilities. We have not done that in the water sector, right?

So, we're – I'll just remind you, you know, 93 percent of the 150,000 serve less than 3,000 people, right? That's a lot of systems. Now, some of those systems, because I've just been out in the field, they don't have any of this stuff. They're literally a manual operation, right?

But, we're moving forward and there's a lot of great efficiencies that come with, you know, advanced metering systems and things of that nature that utilities are moving towards. So their footprint is moving along, beyond the fence line, to becoming global.

And so, how do we best prepare them? And that means we've got to put boots on the ground to go help them do this. If it's a – if it is a key priority, how are we going to do that, right? And there's some mutual aid that can happen between big systems and small systems, things of that nature, but we've not fully resourced it yet, in my opinion.

RAVICH: Well – and that gets to – oh, and let me just say – but that gets to, you know, the issue of, look, the energy sector looks to the Department of Energy as their sector risk management agency. The water utilities look to EPA. And I think we'd all agree that EPA is not yet there, in terms of providing the support that it must to this critical infrastructure.

And, I mean, you can challenge that if you would like to. I mean, you know, hopefully they'll get there. They're moving in potentially the right direction, but water utilities can't wait for the EPA to become a mature sector risk management agency, right?

So Fred – but all of you jump in – we need to improve the sector's cyber resilience now, and it's becoming more and more obvious, which is why we are so pleased to – that Microsoft has asked us to join with an effort with the non-profit Cyber Readiness Institute to provide free training for small utilities.

Fred, Microsoft seems to really be putting its money where its mouth is on this, yes?

HUMPHRIES: We're trying to do our part in – with that Cyber Readiness Institute and focusing on the small and mid-sized entities, utilities on coaching and, you know, giving advice on what you need to do to be prepared on the cyber front and cyber, you know, resiliency aspect.

And one of the things that – and it's in the report, that talks about cyber hygiene, hygiene, hygiene, hygiene, multi-factor authentication, multi-factor authentication, zero trust – are just a couple of things, right?

Boy, does it make a difference. And you come to find out, like, where are these vulnerabilities? It's something really simple to do that we don't do. And so, just on that front – and so the – and then on the EPA front, they need help. We need to do some advocacy on just some resources and if that's the right place – I think it is – on the security risk management aspect, because it's real. But those are a few thoughts on that.

RAVICH: Kevin, you want to?

MORLEY: Yeah, so I would say I agree with the development and maturity of the agency, and there – there's been some activities that they've been – put in place to try to begin to build that capacity.

I think the question is how do we do it, and what is the most effective way? And, you know, we've been, along with our sector colleagues, have been trying to work with the agency to help guide the "how" part and what we feel is most effective in getting some of these things done.

I would say just a quick note. You know, one of the other challenges in our sector that I think the electric sector's had some of this, too, right, we have these – some of these legacy systems that, unfortunately, can't read into Microsoft 11 – Windows 11.

And so, how do we – how do we work to bring these legacy systems forward, right? It's not that they don't want to update to the newest versions of…

(CROSSTALK)

That backend system won't work.

HUMPHRIES: That's right.

MORLEY: So how do we deal with that, right, so they're not stuck on a – on support of Windows 7 platform on the back…

(CROSSTALK)

So, I mean, there's some of these technical operational challenges that aren't a quick fix. It's a rip and replace kind of functionality that we need to really get a hold of across many, many systems.

FANNING: You know, the point I would make here – this is a very tough issue. We crossed this bridge in electricity early on, where someone like Southern Company, we can spend all the money…

MORLEY: Right.

FANNING: … in the world and everything else. That's easy. It's the co-ops and small munis and everything else that's more of an analog to the water system.

MORLEY: Right.

FANNING: We do things like mutual assistance and we put in programs – CRISP [Cybersecurity Risk Information Sharing Program]. We found out special ways to apply data sharing and analytics framework to help those folks.

At the end of the day, you can't rely on EPA. The right mental model is that it is your obligation. And so, therefore, failing the advancement of a capability at EPA, you've got to take responsibility to fix it yourself in advance. So it's not one then the other.

I think private sector – I'm speaking very broadly here – the private sector must take the accountability. If you are part of a framework that is integral into national security, it is your job, all stop. You better find a way to fix it, at least tactically, if not strategically, in a big system and everything else.

We can't say that's EPA's job. That's our job.

RAVICH: Yeah, I'm - oh, I'm sorry.

FANNING: And I know that's a little provocative cause …

(CROSSTALK)

… that's what we must do.

HUMPHRIES: It's not. You know, as I just advocated for – there's a role for EPA, I think that's – when you talk about the multi-stake stakeholder aspect, you're talking about there's a private, there's a public, it's a community in some ways, but yes, the private's got to do its accountability piece. But I do think that there still is a – there's potentially – I like how you phrased it of how you're trying to shape with the EPA, but I think that there's some potentially opportunity here…

RAVICH: But look, this is what, you know, the American private sector excels at. There's a problem. We need to step in and try to fix it because, as we like to say here quite a lot when we're talking about cybersecurity of the broader economy and the national security platforms that rely on it, we either hang together or we hang separately, right?

And what the three gentlemen up on this stage have talked about for the last 45 minutes is we need to find a way to hang separately, and those that have the capabilities helping those that don't because it benefits all of us.

MORLEY: That's right.

RAVICH: And so – OK, so I want to take the next 15 minutes or so to open up the Q&A to the audience. Please introduce yourself. There's probably a microphone hanging out. I know everyone has a question on water. Yes?

DEROSA: Oh yeah, sure. I'm Anthony DeRosa with the Association of State Drinking Water Administrators, so I get to work with Kevin a lot on this issue. I appreciate all the comments here.

One of the things that I think gets missed, and I'm curious, maybe even the electricity sector experienced this. We're focused a lot on the assessment. Right? We don't know what the problem is so we're trying to get out, we want the utilities to understand what the threats are. Those threats are very different depending on the type of utilities. They have various implementations, various levels of cyber maturity, regardless of system size. You have very well positioned small systems, and well-positioned large systems as well.

I think where things kind of fall off for me are on the corrective actions component. And I think that feeds into the culture of reluctance to even find out what's wrong. You know, if you were to go to the doctor and he told you something terrible was wrong with you, if you can't do anything if you can't afford a surgery, you don't know what to do for next steps, that's useless knowledge.

How do we take that next step so that we're actually moving the needle by ensuring corrective actions and supporting corrective actions? And I think, not just providing, to Kevin's point, boots on the ground technical assistance, but, you know, funding incentives and things like that.

FANNING: I'll do aspirational behaviors. Look, when I talk about this joint collaborative environment, the government can't know how to protect us if they don't know what's going on in our systems. The private sector is extraordinarily reluctant to open the kimono to the intervention of the government, except that is the only way we can assess the battlefield in as much real time as possible.

I can remember, there was an old program I worked on with – at NSA – how do you run your electricity system, and let us kind of look at it and see it in real time? That gave them the knowledge of how to attack a system if they wanted to, but by the same token, it gave them a sense as to the priorities in order to triage a problem on our own.

There is a huge mutual benefit, and one of the challenges I have had in this reimagination of national security, whether it's the business round table or the U.S. chamber with the private sector is to say, that if you are engaged - our - old acronym was SICI, right? Wasn't that unfortunate? Systemically Important Critical Infrastructure. Now, they use SIE, Systemically Important Entity. You need to get to the asset level, though, it's not at the entity level.

But the idea here is to really understand what we can do during a time of crisis and how to fix it, and then get ahead of the curve. The private sector doesn't want to do that, and yet we must. To stick your head in the sand, if you were involved in a national security activity like energy, like water, like other things, you have an obligation to do it.

I would argue that if we can demonstrate to the private sector a fair equation of benefits and burdens, then I think the private sector will run to the altar and hopefully engender the kind of collaboration we need.

RAVICH: Kevin? And …

(LAUGHTER)

Mark?

MONTGOMERY: I have a question. This is for Tom. The - recently, it looks like the federal government, the Executive Branch passed on - on kind of updating and embracing Continuity of the Economy planning. What do you think about this? And what do you think the risk is in not updating that planning?

FANNING: Yeah, I think it's enormous. I think it's a miss. And I think it's - you know, as a CEO of a private sector company or whatever it is, every day you should wake up thinking today's going to be better than yesterday, tomorrow's going to be better than today, and I'm not going to rely on what I did then, I'm going to work relentlessly to get better, every day.

I don't seek my successes. I want to celebrate them, but I'm really after the deltas, the problems, the things that we can do to get better. OK, we know that in a Continuity of the Economy posture, that we already have a significant amount of regulation and executive orders, perhaps laws that create somewhat of a patchwork, some quilt, if you will, that is outdated in many cases, imperfectly sized in others, generally ineffective to be able to handle a problem.

The other idea that I take significant issue is – look, if a problem arises, I have the power to convene, yet America just got knocked down, let's imagine, and now I'm going to start calling people. And knowing that there is enormous interdependency in the private sector, do I just call banking, or do I call electricity, or do I call communications? And how do we know how they work together?

In my view, the COTE Paper, Continuity of the Economy, fails to leverage the notion of collaboration with the private sector. It is written as if the government can do it on its own, and they can't, all stop.

One of the most important features of the CSC 2.0 COTE Paper is the notion that we should have, at least, exercise of the private sector in working with the federal government to solve problems during a time of crisis. I think we owe it to America to take that step and not just rely on what exists and what we did last year or 20 years ago.

RAVICH: And we will get there, we will absolutely get there. We just need to get there before it's...

FANNING: Before a problem hits...

RAVICH: I think we have time for one more quick question. Otherwise, I'm going to turn it back to the folks on the panel to kind of - you know, again, wrap up but think - just say to the audience, what really is going to keep you up at night about this issue on water cybersecurity and, you know, where we need to go quickly, so that we can all kind of have a more restful night? Fred?

Oh wait, before I - before I turn to you, I actually wanted to ask you another question, you know, and which is, you know, back to the cloud – and you can answer this as part of your wrap-up.

It seems to me that one of the things when you were talking that struck me is that if we don't understand the indicators of compromise, if we don't understand where the attacks are coming from on all of these 120,000 small water utilities, you know, we won't be able to see it as a system where, you know, an adversary might be able to exploit.

And if that fits into any of your answers, so be it. Otherwise, Kevin or Tom will take it.

HUMPHRIES: OK. Thank you.

RAVICH: You're welcome.

HUMPHRIES: As I look to wrap up, I'm always kind of a glass half full type of person. I feel that what's in the report, it discusses so many things such as – from an opportunity side at – if we do cyber hygiene, we do some partnerships, we - there's things that we can harden and strengthen, things when it comes to being protected on the cybersecurity - security front. It's going to take a little bit of everybody.

We, in Microsoft, through partnerships on the Cyber Readiness Institute and things of that nature, we're trying to do our part to be a part of the solution aspect.

I will just say on – one of the things that was talked about as well that is important, you constantly – on the cyber front, we're constantly - when something doesn't go like it's supposed to go on the cyber front, you got to assess it, you got to learn from it, you know?

We have a secured first initiative that's as – a result of a learning - because on some of these nation state attacks, it's very - it's not about authentication, it's - a little bit more sophisticated than that. And so, you've got to always stay on top of things. And that's where the cloud, I think, can be helpful on responding fast. But you – and you can't mess around in this space.

And on this water piece, which I enjoyed to be a part of, this is - this is not something I do every day, is talk about water, but...

MORLEY: But you use it...

HUMPHRIES: I...

MORLEY: ... I hope - I hope you use it.

(LAUGHTER)

HUMPHRIES: ... no, no , but it - but no, not really - no - yes. It is critical infrastructure. It is a real topic that, as we go in – into 2024 - a lot going on in the world - a lot going on in the world that we need to be prepared for, and that's not just to give a false alarm, but a - but a real thing that we need to be thinking about.

RAVICH: Thank you.

Kevin?

MORLEY: Yeah, you know, it's - it - this - the last couple of years as the cyber issue has evolved, you know, the water sector is the unseen sector, right? The only time we touch it is when it comes out of your faucet or something, but otherwise, I mean, you know, it's not - you know, it's not as apparent.

And so it has been interesting for us to be suddenly put to the front of the class, with the attention that we typically didn't get in the preceding 20 years that I did this work. So, that is a good thing, I think.

I do think that there are - there is a collective opportunity. It's a shared responsibility, as Tom said. And you know, that is indeed why AWWA, amongst others, has tried to lean forward in setting up a process where we can address the accountability question, but also really importantly, to get past Anthony's point, of – yes, so there's the assessment, but we need to enable these systems to take ownership of the risk, right?

And that doesn't have to be a punitive process, right? And I think we're at a point where we're shifting towards, you know, more than – not just the what, right - Mike – as I say to utilities, I'm, like, just think of this like a hurricane, but instead of a hurricane, Mike Tyson is in this room with us. He wants to punch you in the face. What are you willing to do to avoid that? That's how you need to think about cybersecurity. I mean, that kind of changes it a little bit, if you're like oh, OK, I can get that.

But you know - and there are resources available to help support that...

RAVICH: Yeah.

MORLEY: ... so, how do we get to there, enable them with the how part, which is – I think there's a number of different paths we can get there. And certainly as it comes to, you know, A.I. and things of that, you know, the water sector is very thankful for all these great datacenters because they use our water. So that's...

(LAUGHTER)

… that's a good thing too. So...

RAVICH: Yes, it is.

MORLEY: ... but, you know, more seriously, right, I think it requires a different approach, that, you know, it's not just the federal government and it's not just the private sector, it's - it - there is a collaborative opportunity here. The question is are we going to take it, right?

RAVICH: Yeah.

Tom, last thoughts on this?

FANNING: I actually want to have two sets of comments. One, real quick, scale is sometimes really good and sometimes it's really bad. If they can infiltrate the cloud, then all this protection you talk about, that becomes target one for the bad guys...

MORLEY: True.

FANNING: ... and so now, you're competing against Russia and China's best people. So, that becomes target number one.

Being so diffused, as the way water is, there's some protection there in that if they take out the water system of Sandy Springs, Georgia, OK, I mean it's not good for Sandy Springs, Georgia, but we could bring in truck loads of Evian or something - I don't know, we'll work our way around it, it won't be a systemically problem kind of thing.

But the problem is, with so many small players, do they have the resources in mind?

And here's what I would say, guys, and now I'm to my second point, and that is I don't care. Your obligation, our obligation, nobody here is doing the job that they can do, me included. We've always got to find a way to do better. And given the urgency of the problem, I think what we've got to do is move as fast as we can and get to the 80 percent answer and adapt from there.

So, waiting for anybody, the EPA or CISA or anything else, there are tools out there right now that we can adopt in short measure and just get there.

Listen, we got into this in electricity. Some guys wanted to use CRISP and some guys wanted to use something else, Neighborhood Keeper versus this and that. It's all garbage. Do something, move quickly, move with a sense of urgency, and we'll adapt from there.

RAVICH: Right. So, on those words, you heard it – I mean, there is a real sense of urgency because, no offense, you can live without the lights on for a few days if you must – of course, everything depends on it, I get it – but try living without water, you know, for more than a day, more than two days. It's not good.

Look, we look forward to updating you very soon on the positive impact that the pilot project we're doing with Microsoft and the Cyber Readiness Institute as it continues because it will absolutely help make our critical infrastructure that much more secure.

So, for that - with that, I want to thank the panelists. I want to thank the audience. And I wish you a good day. Thank you.

(APPLAUSE)

END