FDD EVENTS

Strengthening the Cybersecurity of American Water Utilities

Featuring Ken Kopocis, Dr. Kevin Morley, and RADM (Ret.) Mark Montgomery
Moderated by Dr. Samantha Ravich
Keynote remarks by Representative Jim Langevin (D-RI)

RAVICH: Hello, I am Samantha Ravich, chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. Thank you so much for joining us. America's critical infrastructure is only as strong as its weakest link. And in the United States, water may be the greatest vulnerability. The United States has approximately 52,000 drinking water and 16,000 wastewater systems, most of which service small- to medium-size communities of less than 50,000 residents. Each of these systems operates in a unique threat environment, often with limited budgets and even more limited cybersecurity personnel to respond to these threats.

Conducting federal oversight of, and providing sufficient federal assistance to, such a distributed network of utilities is inherently difficult. Water infrastructure is critical to U.S. national security, economic stability, and public health and safety. Building on the work of the congressionally mandated Cyberspace Solarium Commission, FDD published a research memo highlighting the current state of cybersecurity in the water sector, the role of the Environmental Protection Agency, the EPA, in supporting the sector, and offered recommendations to address policy gaps to support water organizations.

The report really has opened up people's eyes to how this most vital of resources can be put into jeopardy by our adversaries. The CSC 2.0 Project, which was established by Cyberspace Solarium Commissioners and is continuing the work of the Commission, has recently published model legislative text for implementing some of the report's recommendations into law. We are fortunate to have three experts with a mix of industry, government, and congressional expertise to discuss these issues.

A few quick words about FDD before we get started. FDD is a nonpartisan research institute, exclusively focused on national security and foreign policy. FDD houses three centers on American power and produces actionable research and develops policy options to strengthen U.S. national security. FDD proudly accepts no funds from foreign governments or corporations. For more information on our work, we encourage you to visit our website, fdd.org. You can also follow us at @FDD on Twitter.

With that though, I am pleased to virtually welcome Representative Jim Langevin to give some opening remarks. Congressman Langevin is a senior member of the House Armed Services Committee, where he serves as chairman of the Cyber Innovative Technologies and Information Systems Subcommittee. A national leader on securing our nation's infrastructure against cyber threats, I had the distinct honor of serving alongside him on the Cyberspace Solarium Commission, and to call him a friend. His commitment to public service over the past two decades, especially on the issues of cybersecurity and critical infrastructure protection is unequaled. Welcome, Congressman Langevin.

LANGEVIN: Hello everyone. I'm Jim Langevin. And for the past 22 years, I've proudly represented the 2nd Congressional District of Rhode Island in the United States House of Representatives. I'm sorry I can't be with you in person with everyone today, but I'm grateful with the opportunity to say a few words on the cybersecurity of our water sector. The water sector provides some of our society's most core essential services. Access safe drinking water, and properly treated wastewater are baseline functions a society must fulfill to support modern life and public health.

The water sector also supports the functionality of many of the other 15 critical infrastructure sectors in this country. It's for these reasons that cyber threats to our water sector should generate serious concern. Yet we know that from CISA, the FBI, NSA, and EPA, that known and unknown cyber actors are attempting to compromise both information technology and operational technology assets at water treatment facilities.

Now, we've seen what cyberattacks against our water sector can do. Last year in Oldsmar, Florida, a hacker tried to poison the city's water supply by increasing its sodium hydroxide content to extremely dangerous levels. Fortunately, quick action by an operator at the facility thwarted the attack, but it demonstrated that under investments in water sector cybersecurity could lead to disaster.

Unfortunately, we've been flirting with such a disaster for years. In the Cyberspace Solarium Commission's final report, we looked at cybersecurity of the water sector and noted that, and I quote, "Water utilities remain largely ill-prepared to defend their networks from cyber enabled disruptions." Adherence to existing cybersecurity guidance has been inconsistent with many utilities, lacking the resources they need to fully meet recommendations from the water sector associations and the EPA, the water sector to sector risk management agency, or SRMA.

Yet the EPA itself also faces challenges in meeting its responsibilities when it comes to the day-to-day relationship between the federal government and their water sector. While the EPA is not only the SRMA that faces such challenges, we further noted in the Solarium Commission's final report that there remains, and I quote, "Insufficient coordination between the EPA and other stakeholders in water utilities security."

Knowing what we know about the cyber threats facing the water sector, this status quo simply cannot continue. The risks are too great. So we need to raise the bar among water utilities across the country, build a capacity and strengthen adherence to industry-wide standards. And we need to ensure that the EPA is appropriately resourced and empowered to fulfill its critical mission as a sector risk management agency for water. CSC 2.0 has taken a hard look at how we can accomplish these goals and carry out the commission's work forward. Today's event is an important step forward in turning ideas into actions. And we've successfully done so many times before.

As we move forward, I invite you all to engage with my office on this issue. Finding legislative solutions to difficult cybersecurity problems is not always easy. So we need to make sure that we get them right. But I'm optimistic about our prospects for success if we work together. So thank you, and enjoy the rest of today's event.

RAVICH: Thank you, Congressman Langevin, again for your remarks and your service. I'm now pleased to bring in today's panelists. Joining us, we have Kevin Morley, who is manager of federal relations for the American Water Works Association. We also have Ken Kopocis, former deputy assistant administrator for the Office of Water in the Environmental Protection Agency. And finally, my colleague, retired Rear Admiral Mark Montgomery, who serves as senior director of FDD's Center on Cyber and Technology Innovation, and he previously served as executive director of the Cyberspace Solarium Commission.

Mark, I'm going to begin with you. FDD recently completed a report that highlighted the water sector as the weakest link in our national critical infrastructure. Could you take a moment to describe the challenges we are facing in the sector and why it concerns you?

MONTGOMERY: Thank you, Samantha and thanks to Representative Langevin, as well. As you, me and Representative Langevin remember when we were on the Cyberspace Solarium Commission, we did indicate in our final report that there were a number of critical infrastructures that concerned us. Pipelines was on this, this is pre Colonial [Pipeline], water was another. The commissioners had us take a deep dive on this, and I do think it's fair that our conclusion that America's critical infrastructures are only as strong as their weakest link, and water infrastructure could be the greatest vulnerability in these infrastructures.

Really, the significant cybersecurity deficiencies that we observed in the drinking water and wastewater sectors resulted really from structural challenges. There wasn't a specific human or person that caused these. The United States has literally 52,000 drinking water systems, 16,000 wastewater and a lot of these just service small- and medium-sized communities, less than 50,000 citizens. I think 88% of the water is delivered by public sector utilities. These systems operate with limited budgets and even more so, limited number of cybersecurity personnel and expertise. Conducting effective federal oversight in the best of times is really difficult and providing sufficient federal assistance to such a distributed network is also inherently difficult.

What we had found is that really driving or compounding this challenge was something we experienced about 20 years ago, maybe even 30 years ago, which was the increasing automation of the water sector. The removal of linemen who walked and operated valves and pumps and manually inserted the chemicals to purify the water properly, they have been replaced by electronically controlled systems, IT and OT systems. This was done at a time when there was realistically, no perceivable adversarial threat, either nation state or criminal, to these water systems. As a result, cybersecurity, wasn't baked in. I think all of us who work in cybersecurity know that the hardest way to fix a cybersecurity problem is when you have to reverse engineer back into systems. That's going to be the most expensive, painful, difficult solution.

This automation though, did reduce costs and it did facilitate better regulatory compliance in a lot of areas. But I think because of what I said about not having a threat, the utilities did not invest the savings from the automation into the cybersecurity of the new systems that relied so much on cyber, on IT, OT and ICS and SCADA. All acronyms that have to do with the maneuvering of water for the system.

Listen, this also then gave the adversary an expanded attack surface. Before where he probably could have only attacked the billing system of a water utility, they can now go after the field operations, and it can also lead to disruptive and cascading effects if you have similar software management systems at multiple utilities. You could have multiple attacks conducted simultaneously. This really is a challenge, and that is the challenge that faces the utilities. I think compounding this further is that the federal government agency, the Environmental Protection Agency — which was originally called sector specific agency, but is now called the sector risk management agency, that's the agency that bears the responsibility for supporting the water utilities — it has not historically been resourced or organized to support the cybersecurity needs of the water sector, particularly when you think about the scope and the scale of the challenges the sector faces.

This is a perfect storm. You have the private sector really challenged, and the conditions getting significantly harder and worse over the last 20 to 25 years, and owned and operated by public utilities, which don't have the ease of raising capital or the ability to change rates with the same speed and agility of a private sector company. And it's married to a sector risk management agency that has a lot of number one challenges and has not put the appropriate investments into this. What I'd say is, does it matter? Of course, it matters. Water, particularly the drinking water portion, but all water infrastructure is critical to national security, economic stability, and probably most importantly, public health and safety. So, we really do need to tackle this and that was the challenge that we envisioned up front.

RAVICH: Yeah, that's great. Certainly, attacking an adversary's water system is as old as the Bible. But what you talk about Mark, brings it into the 21st century.

Ken, you headed the Office of Water in the EPA several administrations ago. Why is the cybersecurity threat such a challenge for the agency to tackle?

KOPOCIS: Well, there's a couple of reasons for that. One of course, is just trying to identify the nature of the threat. A second one is the fact that these 52,000 water providers that have been identified are scattered all across the country and they operate independent of each other. As Mark said, some 80 plus percent is provided by a small number of those providers, but there's a large number of them out there. Then the there's also another cause and that's the perpetual reason at EPA, is that they're under resourced for the activities that they're tasked to undertake. There's no doubt that EPA recognizes the threat and has taken some steps to address it. But it's within a universe where EPA's workforce is some 3000 individuals fewer than it was 20 years ago. Their budget is $3 billion dollars less than their budget was 20 years ago and the needs for the agency to undertake these kinds of activities have only increased.

What I see is EPA, as I said, because of resources, isn't really equipped as they try to balance how to undertake these responsibilities. It's just something that they need to do. I do think that there are opportunities for the agency out there. I think some of the work that you all are doing helps lay the groundwork for undertaking those kinds of activities. Perhaps we can get into a bit more of that later.

RAVICH: That's great. Yesterday, Mark and I were on a panel on the cyber workforce in the federal government and the need for new ways to bring in new talent. Ken, you touched upon those needs at EPA. There's certainly cross fertilization from the report that we talked about yesterday, to this topic at hand today.

Mark, let me just go back to you for a second before I get to Kevin. Recently, the team at CSC 2.0, rolled out some model legislative text to address the issues raised in the original Cyberspace Solarium and our FDD report, but one of the most challenging was a call for establishing a water risk and resilience organization, a WRRO. Can you explain a little bit about what that is and what you were trying to achieve?

MONTGOMERY: Yeah. Samantha, thanks. Broadly, in the overall framing the, I think, six recommendations we had, the idea was that we'd layer an approach, which would combine strengthening the EPA, improving government financial support and oversight, and then a strong partnership between government and utilities to result in a more secure, reliable and resilient sector. Very specifically to get at that third element, was the idea of establishing a water risk and resilience organization. Our vision here is a sector-led organization. That's because at this time, without getting to all the nitty gritty, the EPA's water cybersecurity team, you can count the total number of people on one hand. Three Finger Brown might have been able to count them all on one hand.

The idea is that because of that lack of capacity right now in EPA, we need a sector-led organization to manage the development of mandatory cybersecurity standards and oversee compliance with them. But because you have to have federal oversight — this approach does account for federal oversight by that limited EPA team, which separately we recommend growing significantly — but that federal oversight and it would be focused on defining requirements for the standard so the EPA would be very specifically working with NIST, the National Institute for Standards and Technology at the Department of Commerce on defining the requirements and standards and getting approval for their use for implementation by the sector-led organization. So the EPA would be the federal oversight agency, you'd also have technical support in this from CISA. CISA is the Cybersecurity Infrastructure Security Agency at the Department of Homeland Security. Again, EPA's the lead, but CISA does provide routine support to all sector risk management agencies. This wouldn't be any different.

Then I do think Department of Energy could also provide some cybersecurity expertise in this because they have been running similar utilities-based sector-led organizations in what's called the North American Electric Reliability Corporation, the NERC. I think DOE could help there, but I do think the water sector would manage the standards

development process, the implementation. We can use the expertise that reside in organizations like Kevin's, and like the various associations that are in the WaterISAC, and the other organizations like AMWA. There's a good number of six or seven water sector organizations. But the idea here clearly is a sector-led organization with EPA oversight that manages and develops mandatory cybersecurity standards.

RAVICH: All right, Kevin, I'm not just going to let you rest on your laurels with the great work that you do at the American Water Works Association. Now I'm turning to you. This water risk and resilience organization that Mark was just talking about seems very similar to something that your organization has been working with, with a friend of mine, Paul Stockton. What do you think of the WRRO recommendation and how might it be improved?

MORLEY: Yeah, thanks. I appreciate the opportunity to talk with you all today. AWWA, amongst the various organizations, has worked for a number of years to elevate the visibility and awareness of the cybersecurity threat to the sector. That includes one of the things that we have done is developed some guidance and approach to how a utility could use in this cybersecurity framework. As we move forward here in the last couple years with some statutory obligations, but also especially on the heels of this last year with SolarWinds, the Oldsmar incident in the water sector, and Colonial [Pipeline], it became very clear that something more was necessary. So we worked with our leadership to evaluate what are the options? Status quo, direct implementation from a federal agency, or what we've likened in the work that we did with Paul Stockton, we would call a co-regulatory model. It's a shared responsibility. There's important elements from our federal partners and there's important elements from the asset owner operators and taking initiative.

We came to the conclusion, Samantha, that this was not something that could be wholly done strictly with the federal family or strictly within the sector and it required this co-regulatory approach. We very much like the idea of the framework or the model from the electric sector. We think there's a lot of value in that shared burden, if you will. Recognizing the capacity issues that Mark noted with EPA, but unlike the electric sector, we're not starting with a blank sheet of paper. There's a lot of knowledge that has been developed on what best practices would be. We think we would be in a position to move rather expediently to establish some baseline minimum cybersecurity practices.

But as Ken noted, there's a huge scale in the size and complexity of utility operations that necessitates a tiered risk-based approach. What's good for the small town I grew up in upstate New York is not necessarily what's appropriate for say a DC or Chicago, just because of the complexity. Half the stuff wouldn't apply where I was from, perhaps. That requires more subject matter expertise from the sector, and we think that something like the water risk and resilience organization can provide the forum by which that knowledge can be collected and organized in a manner that is most productive in advancing cybersecurity in the sector.

Again, as Mark noted, with oversight from EPA on the approval process and if push comes to shove, having some enforcement oversight for those entities that opt to not implement the appropriate protocols. I mean, again, this is again, not getting down to the details, but I think we see this as a shared approach and AWWA and some of the other organizations have recognized that a sector-led effort in partnership with EPA is really essential to advancing in an expedient manner.

RAVICH: I'm going to go back to Ken in a second, but before I do, Kevin, you have your finger on the pulse and talk obviously, throughout the various water organizations and utilities. Are they familiar with this idea yet? What are you hearing back as this is starting to bubble up?

MORLEY: Yeah, I think it's usually odd, as Mark and I have chatted before, for a sector to advocate for regulation. But when you lay out the options on the table and the business case for why this is important, folks, as I've gone around the country and talked about this process, they recognize the value of this type of approach and have been reasonably accepting of that provision. Granted, we haven't worked out the details of the what and the how, but they recognize the need to raise the bar on cybersecurity and our board and leadership have embraced that process and are seeking to continue support for that. So, [I] appreciate this opportunity to talk about it further.

RAVICH: Great. Ken, again, for the audience, just making it clear, you are not now at the EPA, you had been at the EPA. But knowing the agency, how do you think that they would respond to this recommendation in particular?

KOPOCIS: Well, I think that my experience over the long time of working at EPA and with the EPA, is a level of receptivity, I really do. I think that EPA has long worked with its regulating partners out in the water sector. Sometimes the relationship gets a little stormy because EPA has certain things by law they're required to do. But this is an area where they don't necessarily have a legal standard that Congress has told them that they have to meet. So if it were me, my counsel to EPA would be, the first thing I'd want to do is follow up to what Kevin was suggesting. And that is to sit down with the utilities and jointly identify what are the needs, what are the threats, what are the vulnerabilities?

As Kevin rightly says, the vulnerabilities in New York City are not the same as some small town in upstate New York. If you tried to come up with a single set of answers, it simply wouldn't work, particularly for the smaller communities and it'd be way inadequate for the larger ones. There would be a process to work with the utilities and recognize what everybody's talents are. I think initially a lot of the utilities are going to be asking, "How can I get some help?" and EPA's going to be asking, "How can we help?" That's going to be the key question, rather than EPA saying, "This is how we're going to help you and trust us, it will."

Then I think that there's going to be some needs to identify technologies related to security vulnerabilities, et cetera, as Mark was talking about. EPA working, again with the utilities, can help advance where they could offer expertise. It doesn't have to be solely within the EPA. As Mark identified there's a lot of expertise across the federal government. EPA's probably never going to have the internal capability to handle all those needs, but only an agency like EPA can bring the other agencies in.

I think once the needs and vulnerabilities are recognized, once some answers are developed, then I think that my world, I would have EPA support these solutions financially. They're not going to be in a position to pay 100% of the cost, but I do think that one way that's proven to be successful over the years is a joint-partnership and investment in carrying out these responsibilities. That's my three-pronged stool, if you will. But I think that's going to be a path to at least open up the opportunity for success.

RAVICH: I think that sets the stage very well for the next question that I'm going to ask Mark, because he had some very strong recommendations for strengthening EPA, especially in its role as a sector risk management agency. It goes to what EPA can and should be tasked legislatively and otherwise to do. Mark, maybe you could walk us through some of these recommendations.

MONTGOMERY: Thanks, sure. That was a delicate way of putting it. I'm probably not on EPA's Christmas card list right now, but I'm okay with that. Because I think these recommendations are things that EPA's leadership and future leadership are going to appreciate if we can get them into law. Very – I'll do the conclusion first. The conclusion is we have to change [increase] the budget of the Office of the Division of Water Cybersecurity within the Office of Water.

From what I can tell, it's hard to pin it all down, but it looked like they have a portion, probably $6 or $7 million dollars of a $15 million dollar budget for cybersecurity. The $6 or $7 million's for cybersecurity. That might be a tiny bit high. What we're recommending is that you grow that. Now look, the final number needs to probably be around $45 million. It does not work in the federal government to go from $6 or $7 million to $45 million. That's called putting money in a 55-gallon barrel and burning it. You have to grow gradually and so we recommend a gradual grow to $15 million a year dedicated to this, to eventually $30 million a year and then $45 million.

But what are they doing? What they're doing is something that is called out for all the sector risk management agencies, and that's the concept of you have to support the sector's risk management effort. You have to run programs that assist owners and operators in ID'ing and understanding and mitigating threats and vulnerabilities. You don't have to do it yourself. Sometimes you can hire or secund other organizations, if you had a water risk and resilience organization, could do that. In the absence of that, you can use associations like AWWA or AMWA, or the WaterISAC.

But you have to have guidance. If you go on the EPA website now, it's very disconcerting to read the language around assessments where it says, "We don't provide a standard." I mean, it proactively says, "Not us," and it needs to be proactively "us." When you look at other sector risk management agencies that are succeeding, they have an opposite approach. But they also have to help with very specific risk identification assessments and that's what I was getting at. They have to actually help provide the templates for these assessments. This is important, and I think eventually they need to get these back because one of their requirements is they're supposed to tell the Department of Homeland Security what's the national risk that we face in the water industry. I don't know how EPA could do that right now without getting some kind of acknowledgement from the utilities.

Again, if you had a centralized resilience, WRRO, you could reach into somebody to get that answer. In the absence of that, it's going to be a lot of work. I think they have to do coordination to be that day-to-day federal interface. Again, I think they try to do that. They're really undermanned to do it. But they also have to serve as the government coordinating council chair, something they do, and they have to participate in cross-sector coordinating councils with energy and others, which they do. I think that takes up a lot of their day-to-day workload for the limited number of people they have. Then that worries me because that coordination's important. But if you're not doing any of the ligature work with the sector,[it] really doesn't matter if you're running an excellent meeting.

They have to be a participant in the threat and vulnerability information sharing. Now here's a place where the director of national intelligence plays a role, CISA, as we mentioned earlier, plays a role. I think EPA is more of a facilitator here, making sure you make the connections between the utilities, the private sector so to speak, or utilities and the federal government's information. I think Ken mentioned it, that these are critical roles played by other federal agencies. They have to do the incident management for water and wastewater sector. I think that's something they do now, probably the workload's going to increase. This is why they're put with disaster management, they're co-located with disaster management.

Same way in energy, a big organization, energy that is the equivalent to the water organization that we're envisioning. It's got 20-fold the budget and tenfold the people of the current water organization, but it handles cybersecurity and emergency response. I think, similarly, you do that in water. Then supporting emergency preparedness, helping people develop the plans they need for resiliency, for response and recovery from issues. This is really important. It goes beyond cyber, it is about creating an overall lowered national risk management. To me, this is critical and there's no way around it, this takes money. Look, a lot of this is a new mission. In fairness to EPA, we should

not be saying, "Hey, tell us what lead abatement program are you taking that money from?" Because nothing went away as you brought in these cyber requirements.

They really need in my mind, this plus up from $5 million or $6 million, whatever it is now, to $15 million, to $30 million, to eventually $45 million. This is large numbers, it's not large compared to the overall cost of lead abatement programs, for example. But it's large in terms of the administrative management of EPA and those numbers are sometimes really, really tightly managed by the appropriators. But I think there is an excellent argument for this. We're trying to make it from the outside. We hope EPA embraces this. I don't have optimism about that, but I think that this is a reasonable approach to get EPA in a better position to provide the oversight that's required either for the WRRO or if it's in some longer-term vision, an EPA-led sector standard management.

RAVICH: Oh, I think you'll get more than a Christmas card. I'm hoping for a gift basket for you. I think your recommendations are going to go over that well. They're good, they're obviously incredibly important recommendations. Ken, we all understand that agencies and departments have their own culture, so what are your thoughts, advice, guidance on helping the agency to open up? Well, how will they receive this? Are there ways to get them to realize as Mark said, this is not a bash EPA, and this is also a recognition that EPA is going to need more resources to be able to do these things? But what are your thoughts on that?

KOPOCIS: Well, I would expect that the agency would be receptive to looking at the recommendations and advice of people from the outside. Certainly, in my time at the agency, I spent an enormous amount of time meeting with outside experts who helped inform the agency in its decision-making process. I think that it's going to be important for Congress to recognize that this is a need. I think that one of the things that I've talked about in the past, we discussed it a bit in the transition, of cybersecurity and its relationship to physical security. Nobody expects that people are going to be able to defend this country through armies, air forces and navies. We have a structure in place to do that. I think that so many of the instances that we've seen lately have demonstrated that cybersecurity is as much a threat to the U.S. health and safety and the economy as an outside military force. It may not be as destructive, but it can certainly be as threatening and as disruptive to everyday life and including the loss of life.

So EPA clearly will need resources to do this. It's no secret that there are a substantial number of members of the Congress who don't think very highly of EPA in its regulatory function, but this isn't about a regulatory function. This is about taking care of people in their communities, and it has to be sold that way to justify those kinds of monetary increases. Congress can give EPA a plus up in its budget and can be very specific on what it can be spent on so it doesn't fold into the regulatory program that so many people seem to dislike, but it would instead be a direct benefit to the communities.

From the bottom up, it would also be very helpful for these elected members of Congress to hear from the water utilities of, "Hey, we want you to fund this program at EPA. We need you to fund this program at EPA," because if it's just the president's budget asking for the money, all some people will see is, "oh, there's EPA asking for more money and we're not going to give it to them." It's not an easy task, but I think the criticality of the task is what has to be explained to people. Once that is, then I think there's a way to generate support.

RAVICH: Kevin, you've worked with EPA, alongside EPA for a number of years. I mean, what do you think about these recommendations to strengthen the agency? And as a second part of that, and keying off of what Ken said, we had a question from Suzanne Smalley, asking if industry has actually asked the EPA for a more aggressive or involved, let's say, regulatory structure.

MORLEY: Yeah, some good points there. I guess I think overall, the elements of what Mark was talking about, I think provide a little bit more structure to how EPA is involved as a sector risk management agency and provides some important resources and direction as to how that's allocated and directed. As I said before, AWWA amongst other things, is a standards development organization. We have developed standards within this realm of all hazards risk and resilience and emergency response that EPA has often participated in and supported. We believe that approach provides some more substance to that activity.

In terms of resourcing, I think to Ken's point, it's nice to have things on paper here in Washington, but at the end of the day, what is most effective in supporting change in behavior, i.e., implementation and that's a little bit of capacity development. I think through some of the points that Mark made and some of the elements in that provision, supporting capacity development, as Ken well knows, there was a number of programs that focused on small, medium systems and getting them that knowledge transfer. Just yelling at people and saying, "Do multi-factor authentication," without really demonstrating how that goes about, is a piece of the puzzle that's really important to bring everybody along.

We have had conversations with the agency, and they are aware of our interests. I think there perhaps is a little bit of difficulty in seeing outside the box. It is a very different approach than what it's traditionally been in the water sector. I don't think that they are unreceptive to it, but I think the devil's in the details, and they certainly have some other actions that they're looking at within their current regulatory construct that I'll just put it on the table. None of the associations are supportive of this would be integrating cybersecurity into the sanitary survey program. Which a little bit of a burden transfer on the state primacy agencies who also have limited capacity.

Part of the model that we're talking about here with the WRRO is recognizing those resource constraints. It really comes down to this collaborative trust in who is doing the what. We believe this more distributed approach through a third-party organization that can provide that audit function and valuation evaluation, if you will, of how utilities are implementing the standards that we talk about, the output of that is what's really important. That information can be shared with the state and can be shared with the agency to address those interests of what is the status of the sector and how are things going.

Then ideally, the majority of the sector typically moves along pretty well in terms of compliance on these things. I think there's an opportunity here with some of the resources Mark talked about that if a utility is having difficulty getting there, there's opportunity for technical support to help bring them along and not just hit them with a sledgehammer for an enforcement action, which isn't necessarily in the general interest. What we're really trying to do is support implementation of change in cybersecurity so that ultimately the public health of the community served is protected as best as possible.

RAVICH: Well, it's important to underscore that you were talking about bringing the capacity to the states and down to where the utilities are operating, because obviously people aren't going to die of thirst at the federal level. Or God forbid, in any other way. It's at the local level. It is where they drink their water, it is where they need their water. Mark's team did recommend some changes that would direct state revolving funds to spend more on cybersecurity. What do you think of that in particular, any other means to achieve this type of support to utilities that haven't yet been mentioned?

MORLEY: Yeah, I think the important thing with that particular provision of the model legislation that's important is the recognition that this isn't a no cost option. If we want utilities to move along with some degree of expedience, then some resources are going to need to be provided to facilitate implementation. I'm not 100% certain that an explicit carve

out within the SRF program is the most prudent approach. But that aside, the mechanics of that are really important and there are certainly other programs that Ken can probably speak to with more expertise than I, but the like STAG Grant program. One of the limiting factors in the SRF program, not to get too down into the weeds, is that if that can really support what we would traditionally call CapEx funding, it is not supportive of OpEx.

If I, as a small or medium utility am transitioning to some sort of security as a service like cloud, or I want to use AWS, or some other service to support the security of the IT or OT infrastructure, that's now considered a subscription, if you will, and is operations and maintenance. That's not eligible under the SRF program. Now, that doesn't mean that there aren't nuts and bolts kind of things that can be funded through the SRF program. But that is one concerning constraint that I would have with that particular funding mechanism.

But certainly I think the important thing is the recognition that some additional funding support because comparatively, as Mark wrote in the report, the funding allocated to cybersecurity in the water sector compared to say, our colleagues in the electric sector, is de minimus. I forget Mark, but it's $250 million in grants for roughly 3000 utilities. We've got nothing for 52,000 utilities plus 16,000 wastewater systems. So if we're serious about the issue, then we're going to need to put some muscle behind it to make the changes that we think are important.

MONTGOMERY: Samantha, that's a great point Kevin had there that, you know you're right when it's the solution that was used for the most similar infrastructure, energy. In the infrastructure bill, this is the bipartisan infrastructure act last year. We 100% addressed the cybersecurity issue with the energy utilities with a $250 million program. Then when you move over to the water side, their cybersecurity competes with drought, climate change, natural disasters, rising sea levels, the four signs of the apocalypse. Or you can invest a little bit in cybersecurity. Obviously, the big four get taken care of and to prevent that kind of thinking, which is human, the Congress took care of energy, did not take care of water. Sorry to jump in, but Kevin mentioned it and he's absolutely right.

RAVICH: Yeah, yeah, no. Ken, I want you to jump in here on the DRF [SRF] or other ways that you think that increased funding or assistance is best gotten for cybersecurity efforts to the utilities. Again, you're just saying, again, you are no longer at EPA, so you can think broadly and don't have to clear anything with anyone.

KOPOCIS: Well, I think that because of the resource constraints that have been placed on the agency over these many years, I think that trying to take money from an existing program and move it into a new purpose, I think as Kevin was saying, you're starving one program for the benefit of another. Now that doesn't mean that you might figure that's a higher and better use for that money than investing in an operating cost versus a capital cost. Although, there will be some capital costs associated with cyber as well, obviously. I'd like to think that we can have a rational conversation with the Congress and the administration and recognize that this is a need that has to be treated as the serious need that it is. That means it's a call for new investment and new investment is new money.

I also think new money will help alleviate some of the concerns at the agency. I can tell you, they always feel pressed. Every time somebody says, "Oh, you need to do this new thing," then the first thing that the office directors have to say is, "Where am I going to get the money? Where am I going to take it from, because I don't have a new pot of money to go spend." While I'm not saying that it's going to be a snap to go ahead and create a new funding for the agency to undertake these steps, I think that it's most likely to be successful if there is a way to find some new resources for the agency. They will then be more comfortable in committing their own resources because you're not taking it away from an activity that they've currently identified as important to them and/or a responsibility that Congress gave

them that's non-discretionary and some group is out there waiting just to sue them as soon as they don't do it and put them on a schedule.

I think that's the way to try to convince people to market it, to let people understand that this is really serious. I said a little earlier, I think that people have underestimated this risk for way too long, because the risk is so diverse out there in the 52,000 water utilities. In the post 9/11 world, we spent considerable amount of time looking at the vulnerability of water systems. It wasn't cybersecurity then, it was concern about water systems being poisoned. Well, Blue Plains, right outside of Washington had tank cars, railroad tank cars with chlorine that you could have shot with a rifle from 295. Chlorine is highly deadly, and it doesn't go up. It stays along the ground.

These kinds of vulnerabilities have been identified and the agency can work with intelligence officials and with the utilities. I'll go back to the point. I think it's going to be critical for the agency to understand what the utilities' needs are because they're going to be so diverse and what the risks are and then you start addressing them in a much more collaborative way.

RAVICH: Yeah. Mark, you had one recommendation unique to the smaller rural water utilities. Can you explain what the cybersecurity circuit rider program is and what it's intended to do?

MONTGOMERY: Thanks. Yeah, absolutely and this is a fun one. It's actually in the Department of Agriculture, so we'll take it easy on EPA for a moment here. The National Rural Water Association Circuit Rider program, it's made up of about 150 circuit riders that work with 50 states. I think it happens to be 49 state associations and Puerto Rico. There's a handful of people addressing each one, and they provide hands on training in technical systems to small rural systems that's defined as 10,000 people or less on an everyday basis, 24/7. They do about 70,000 interactions, training, and assistance interactions a year with these small utilities. That's a lot of onsite help, it's delivered where it's needed in a rural community.

I envision these guys, they don't ride horses anymore, the circuit riders. They're probably driving F-150s, they got a little bit of extra pipe in the back of the bed, and they're driving around a lot of tools and they're helping these guys. They're like, "Hey, you got to put that pipe a little farther away from that pipe," kind of stuff. What I don't imagine they're doing is giving any advice on cybersecurity and that's been verified. What we did was suggest, "Hey, let's augment this with a cybersecurity circuit rider program." I think it's $5 million dollars, that won't quite get us to 50. We'd have to adjust the money or adjust the number. But I would suggest around 50 cybersecurity circuit riders. Now these guys are driving around in Prius's, not F-150s and they're coming in and they're saying, "Hey, you're running Windows 7 and you haven't done any patches in four years. Let me explain to you how to get yourself healthy."

So, they provide technical assistance, they can probably provide some minimum support, some limited support in there. I think it's an easy program and keep it in the Department of Agriculture, just because the circuit rider program's there, and I don't want to create extra overhead. You just want to pay for bodies to be thrown up against this and I guess, rent some Prius's. But that, to me, is the idea with this. I think of all the things we've mentioned, for several reasons it's the most likely to happen. Number one is that it's in the Department of Agriculture, not EPA, and that removes some angst. But number two is it's working on an existing program and it's just providing an added capability or capacity.

RAVICH: Speaking from a small rural area, I thank you for that recommendation as does Ken, I think. Okay, final question. But let me start with a quote from a very smart man named Kevin Morley, who said that, "Crisis begs bad policy," it has stuck in a number of our heads. Yeah, so crisis. We've discussed a number of pretty dire challenges, a

number of proposed recommendations, but what are your thoughts on what may happen in this space over the next 12 months? See crisis on the horizon, or are we going to not have to wait for the crisis to get that bad policy that Kevin warned us about? Let me take Kevin first and then Ken, and then Mark, you can wrap it up.

MORLEY: Well, thanks for that, Samantha. I think you always wonder if anybody's listening. I think part of the reason that we took action and did the paper that you mentioned with Paul Stockton, was to move preemptively prior to a crisis, to have an approach that we felt was reasonable to move the ball down the field. Is that going to prevent every possible thing? Absolutely not. I'm not making that claim, but it moves us in the right direction. I think organizationally, ourselves and some of the organizations are moving forward to seek Congressional support for something very similar to the WRRO that Mark and his team have proposed. I think it's very close to what we were talking about. That's very encouraging and hopeful to see something like that be introduced and move the ball down the field.

I think we're prepared to move ahead, even in the absence of that and try to articulate some minimum practices with our colleagues in the sector. Some of that obviously needs to align with pending revisions to the NIST cybersecurity framework and the performance goals that the White House put together. But I think all those things can reasonably be included together and build on the body of knowledge that we've already created in the sector between ourselves and some of our partner organizations and be in a better place in a year from now. But from a structural governance perspective, that's going to require a little help from our friends on the other side of the fence line, so to speak. In the federal government, whether be it directly through EPA or ideally with Congressional support, that would be ideal.

RAVICH: Thank you, Kevin. Ken?

KOPOCIS: Well, I agree with that last one. I think some Congressional involvement is going to be critical because that's going to be where the resources come from. Whether it's augmentation to USDA's circuit rider, which I think is an excellent idea because nobody ever wanted to hear, "Hi, I'm from EPA and I'm here to help you." But we're very good as a nation reacting to disasters instead of anticipating and avoiding them, if particularly you look at natural disasters. But I think if something terrible happened in the water sector, that's what you would see. You would see this huge ramp up and it would be in a crisis response rather than in anticipating it.

One of the things I think of in this sector for example, is if you recall all the work and effort that went into the concerns about the Y2K transition and all of our computers were going to revert to 1900, and people looked back at that and said, "Well, it was a nothing burger. We didn't have a problem." Well, of course we didn't have a problem because we anticipated it, we invested it in it, and we made sure that it didn't happen. Now we're going to have a situation where we have state actors out there who are probing ways to disrupt the U.S. economy. They don't really care, I don't believe, how they do it in the sense that they want to do is create disruption in the U.S. economy, whether it's through the electric grid, the power sector we saw with the oil pipeline.

These opportunities are just out there, and I think that we have to tell people that there's an obligation to address these. We need to be addressed preemptively following on both what Kevin and Mark are saying, and that case needs to be made. We can use some of these prior efforts of the government as ways to work with the public sector, the non-federal sector to achieve those successes.

RAVICH: Thank you. Mark?

MONTGOMERY: Thanks. I think the first and most important thing to say is, look, there's clearly a problem. Some people have trouble saying that out loud, there is clearly a problem. Nobody on this panel has that, but in both the executive branch and Congress, there is a sense of, "well, we'll get to it." And as Ken said, we're probably going to get to it in a crisis management mode if we're not careful here. We need to make the investments now. Many of us on here watched us build DHS on the fly, the Department of Homeland Security, and now we have it warts and all. I mean, there are a lot of things that if we'd been able to build that deliberately and proactively, it'd been a much different type of organization. I really feel there's some opportunity here to take action left of boom.

Ken reminds me, one of the reasons we have trouble here is there is an inherent distrust between elements of Congress and the executive and the EPA. Much more so than you see in the other sector specific agencies. There's usually one off or two off senators who are currently mad at that agency, but that's not the same as a fairly persistent distrust of the agency that you feel. We have to work our way around that with good governance arguments.

Then there's also a sense of encroachment between committees and agencies, that the committees that are responsible for water feel that the committees are responsible for homeland security have poached in the past and they're on the lookout for it. It creates a sense of "not sure we want to open up a can of worms of an authorization here" and something else gets in. So we got to work around that. These are bureaucratic challenges and barriers that can be overcome because there is a problem.

I'd say finally, I do think yesterday or last week, you and I, Samantha, talked with Chris Inglis in an event. I think the national cyber director can play a leadership role here as one of the national risk managers, particularly for the cyber end of this, in ensuring that we highlight, identify the challenge in the water and wastewater sectors and bring the executive and legislative branches together for a solution. I think he has the kind of deliberate, persistent leadership that's going to be necessary to tackle this. A lot of barriers, but I think in the end, the challenge is too significant to be ignored for another two, three, four years.

RAVICH: Yeah, let me just say personally, the Center for Cyber and Technology Innovation, where Mark and I are both at, at FDD, have been writing about issues of importance in cyber and technology for over five years. This report that Mark wrote, I have to say is one of the most important, if not the most important piece of work that we have put out. It is something that people's eyes have just not been open to. I thank you personally, Mark.

But look, everyone on this panel, Kevin Morley, Ken Kopocis, again, Rear Admiral Mark Montgomery, thank you for your service to our country, for helping us highlight and for dealing with these issues in your own capacity for taking time out today to talk with us.

For more information on FDD and our latest analysis, this and others, we encourage you to visit us at fdd.org. And you can find out more information on the Cyberspace Solarium 2.0 project at cybersolarium.org. With that, we hope to see you again soon and thank you very much. Take care, bye-bye.