Table of Contents

U.S. Senate Date: Wednesday, February 4, 2026

Committee on Environment
and Public Works

Washington, D.C.

STATEMENT OF:	PAGE:
THE HONORABLE SHELLEY MOORE CAPITO, A UNITED STATES SENATOR FROM THE STATE OF WEST VIRGINIA	3
THE HONORABLE SHELDON WHITEHOUSE, A UNITED STATES SENATOR FROM THE STATE OF RHODE ISLAND	8
D. SCOTT SIMONTON, PE, PhD, FELLOW, MARSHALL UNIVERSITY INSTITUTE FOR CYBER SECURITY	13
MATT ODERMANN, EXECUTIVE BOARD MEMBER, NORTH DAKOTA RURAL WATER SYSTEMS ASSOCIATION	20
SCOTT DEWHIRST, DEPUTY GENERAL MANAGER, ENGINEERING AND TECHNOLOGY, FAIRFAX WATER, ON BEHALF OF ASSOCIATION OF METROPOLITAN WATER AGENCIES	25

IDENTIFYING AND ADDRESSING CYBERSECURITY CHALLENGES TO PROTECT AMERICA'S WATER INFRASTRUCTURE

Wednesday, February 4, 2026

United States Senate

Committee on Environment and Public Works

Washington, D.C.

The committee met, pursuant to notice, at 10:00 a.m. in room 562, Dirksen Senate Office Building, the Honorable Shelley Moore Capito [chairman of the committee] presiding.

Present: Senators Capito, Whitehouse, Cramer, Ricketts, Husted, Markey, Schiff, Blunt Rochester.

STATEMENT OF THE HONORABLE SHELLEY MOORE CAPITO, A UNITED STATES SENATOR FROM THE STATE OF WEST VIRGINIA

Senator Capito. Good morning, everyone. It is nice and bright and sunny outside, so that is good. We will check on the snow removal later, and see, and the ice removal. Good morning, and welcome to today's hearing.

Today, we will examine the challenges facing drinking water and wastewater systems to install, implement and maintain adequate cybersecurity, as well as try to identify opportunities to address these challenges through new legislation.

First, I want to thank our excellent panel of witnesses for making the trip to D.C. and to share their perspectives on this important topic. Your work to enhance the resilience of our water and wastewater systems is incredibly important to Americans' health and daily lives.

There are approximately -- this number is stunning, really -- 170,000 water and wastewater utilities across the Country. These utilities fill a vital role in ensuring that communities across the Country have access to safe and reliable water and sanitation services.

I know in the audience we have several of our water system utility folks here. So, I will shout out to my fellow West Virginians.

Accessible and reliable water and wastewater services are

essential to protect public health and provide fundamental services to our constituents. These services can also be a foundational basis for a strong economy and a strong America.

Because of the important role our water systems play in our Country, they are unfortunately a target for bad actors. Over the last several years, we have seen a broad trend of entities linked to our geopolitical adversaries, such as Iran, China, Russia, using cyberattacks to target our critical water infrastructure.

Cyberattacks on water utilities may take various forms. For example, ransomware attacks can compromise business or customer information. Attackers can also gain access and then manipulate a system's operational technology, disrupting the treatment or distribution of water or altering the levels of chemicals to potentially dangerous amounts.

Either way, a successful attack that disrupts safe and reliable water or sanitation services or exposes sensitive customer data could be debilitating for impacted communities. These threats must be acknowledged and challenged, particularly as technological advances, such as AI, increase the speed and efficiency of these attacks.

The rise in cyberattacks is occurring at the same time as our water and wastewater systems deploy new digital control technologies -- I have seen some of them myself, systems that

allow utilities to operate more effectively and effectively.

As we look to upgrade and modernize our water systems in the face of these threats, it is more urgent for our utilities, Federal agencies and water sector and cybersecurity experts to work together to increase that system resiliency.

Increasing water system resiliency requires us to take a clear-eyed look at the many challenges and shortcomings that our utilities are facing. Legacy systems are difficult to maintain and update. Workforce shortages limit in-house expertise, and fulfilling basic cybersecurity hygiene practices requires consistent monitoring and communication.

For instance, in 2024 the Environmental Protection Agency identified instances where some water systems utilized a single login for all their employees, failed to change default passwords, or did not curtail the ability of former employees to access the systems.

While we work to improve the resiliency of our critical infrastructure from cyberattacks, solutions to address cybersecurity must be deliberate and tailored to reflect the challenges faced by utilities of different sizes and locations. A one-size-fits-all mandate from the Federal Government will likely be overly burdensome and unworkable, particularly for our smaller systems, and can hinder utilities' ability to take achievable steps towards meaningful progress.

Water and wastewater systems across our Nation are already grappling with how to prioritize limited resources while meeting Federal and State requirements under the Clean Water Act and Safe Drinking Water Act. Costly requirements can distract from the core mission of providing safe, reliable and affordable services to the American people.

In addressing these cyber challenges, we must strike the right balance between the role of Federal agencies and empowering local utilities to address their challenges and improve their cybersecurity at their own facilities. Due to the constantly evolving technological environment that we live in, addressing this challenge will require innovative solutions that enable utilities to adapt and respond to quickly changing circumstances.

Building and maintaining resilience against cyber threats is not a one-and-done event; it is ongoing and ever-evolving. We should not rely on one specific technological advancement as the silver bullet solution or have blinders on when it comes to envisioning or preparing to address potential threats.

I look forward to the discussion today, learning how we can be better partners with our water utilities to identify cybersecurity threats and provide a flexible toolkit going forward

I now recognize Ranking Member Whitehouse for his opening

statement.

[The prepared statement of Senator Capito follows:]

STATEMENT OF THE HONORABLE SHELDON WHITEHOUSE, A UNITED STATES SENATOR FROM THE STATE OF RHODE ISLAND

Senator Whitehouse. Thank you, Chair Capito, for convening us on another important topic. Thank you to our witnesses for being here.

Cybercrime and cyberwarfare are realities of the 21st century, and have been for quite a while. Back in 2010, I started the Intelligence Committee's Cyber Task Force, where we spent six months investigating cybersecurity threats to our Country.

The water sector has modestly improved information sharing and coordination between the EPA and the Cybersecurity and Infrastructure Security Agency. Non-profits and water sector trade groups have increased public awareness of cyberthreats. This, however, is insufficient.

Meanwhile, foreign bad actors continue to enhance their capabilities and evolve the nature of their attacks. State-sponsored and state-aligned bad actors linked to countries like Russia, China, Iran and North Korea have been increasingly relentless in their attacks on American facilities. They have stolen sensitive information, scrambled networks, extorted ransoms and disrupted sectors ranging from health care to, as we hear about today, drinking water.

There are nearly 170,000 water systems across our Country.

As these systems modernize, they incorporate technology that is more efficient, yet more vulnerable to cyber-attacks. According to GAO, many of these facilities have already faced digital breaches, but without more incident reports, it is impossible to know the full scale of the threat they face.

Since 2023, Russian, Iranian, and Chinese hackers have successfully attacked small municipal water systems in Texas, Pennsylvania and Massachusetts, and have tested the security capabilities of countless other systems. They are always probing.

Over the past six years, Rhode Island municipal facilities, one of them a large wastewater utility, have experienced at least six cyber-attacks, collectively resulting in hundreds of thousands of dollars in losses.

These are just the incidents that have been reported. All water utilities without adequate security are at risk regardless of size. While none of the previous attacks on the water sector have caused major service disruptions, they all cost time and money. The cyber-attack that incapacitated even one major water facility would not only be disastrous for the people affected, it would spread fear across the Country.

According to an EPA survey, less than 25 percent of our water and wastewater utilities perform annual cyber risk assessments. Less than one in four. Just imagine the

consequences of a coordinated nationwide hit. Clearly, we are not ready.

The Trump administration has forced out thousands of Federal cybersecurity experts, cut funding to research and readiness cyber programs, and crippled our relationships with key international intelligence partners. We need to strengthen our national cybersecurity capabilities, not weaken them. And water utilities need more knowledge sharing, not less.

We can change that. Even when water utilities understand the risk and solutions, updating cybersecurity measures is often deferred in favor of maintaining service levels to their ratepayers. To meet the challenges of the 21st century, we must repair and replace outdated infrastructure, while also updating and maintaining our cybersecurity defenses. This is not either-or.

To start addressing our Nation's massive water infrastructure investment deficit, the Infrastructure Investment and Jobs Act provided more than $50 billion, with some expanded eligibility for cybersecurity projects. This was a good start, but not enough.

I look forward to discussing how this committee can expand EPA's current authority and can help update physical and digital infrastructure across the Country to keep water safe, available, and affordable.

Thank you very much, Madam Chair.

[The prepared statement of Senator Whitehouse follows:]

Senator Capito. Thank you, Senator Whitehouse.

And we will now turn to our witnesses. I am very excited to welcome our first witness this morning. Dr. Scott Simonton is a fellow at Marshall University's Institute for Cybersecurity, and is a Professor at the Department of Mechanical and Industrial Engineering.

Marshall's Institute for Cybersecurity is working on several projects with water utilities in West Virginia. We are so excited to have the Marshall Institute for Cybersecurity at Marshall University. I look forward to learning more about the institute's work today.

With Dr. Simonton is his wife, Molly Simonton. Thank you, Molly, for coming; and his son, Nathanaiel, who is, I just learned, a freshman here at George Washington University. He is on an ROTC scholarship. Thank you for your service now and what it will be in the future.

We also have Alex Donathon with us here, who is the Executive Director of the Marshall Institute for Cybersecurity for Critical Infrastructure. Thank you for being here. And Dr. James Lanham, who is also with the Cyber Institute, and a professor and good friend from Marshall University.

With that, I will turn it over to you, Dr. Simonton, and welcome.

STATEMENT OF D. SCOTT SIMONTON, PE, PhD, FELLOW, MARSHALL UNIVERSITY INSTITUTE FOR CYBER SECURITY

Mr. Simonton. Good morning, and thank you, Chairman Capito, Ranking Member Whitehouse, members of the committee. Thanks for the opportunity to speak with you today.

As Chairman Capito mentioned, I am Scott Simonton. I am a civil and environmental engineer, a professional engineer registered in West Virginia, Kentucky and Mississippi, a veteran and a fellow in the Institute for Cyber Security at Marshall University and a professor in our College of Engineering.

My work places me between cybersecurity professionals and infrastructure operators. So I am helping translate cyber threats into real world engineering and public safety consequences so both sides can act on these risks.

For more than 30 years, I worked with water systems across Idaho, West Virginia, Central Appalachia, on environmental management, infrastructure modernization, and now cybersecurity. I want to offer a practical view from a region where small systems are essential lifelines and very resource-constrained.

West Virginia has several hundred community water systems, and over 75 percent serve fewer than 3,300 people. These are small, rural systems, often with one or two operators who handle everything: treatment, distribution, reporting, and now digital oversight.

But even the smallest systems are now relying on SCADA, PLCs, internet connected monitoring and control systems, but they typically lack dedicated IT or cybersecurity staff. As outlined in our written testimony, the vulnerabilities are common and well documented. These include exposed remote access interfaces, default and shared PLC credentials, flat networks that connect business and operational systems, and legacy vendor-managed equipment that cannot be easily patched.

These issues show up consistently, but not because operators lack commitment, but they lack capacity to deal with some of these issues.

Under the Safe Drinking Water Act as amended by America's Water Infrastructure Act, systems serving more than 3,300 people must completely risk and resilience assessments and emergency response plans that include cybersecurity. But in West Virginia, most of the systems fall below that population threshold. But they face the same cybersecurity threats as the large utilities, but they don't have the mandate, the staffing or the structure that those larger utilities have to deal with cybersecurity risks.

So, we leave or we are left with a very significant gap in that modern monitoring and control systems have reached even the smallest utilities, but these cybersecurity requirements have not.

At Marshall's Institute for Cyber Security, we are working directly with operators, utilities, and State partners to close that gap, turning Federal guidance into real operational improvements. We have three examples that illustrate this. Currently, Marshall ICS has helped prepared 14 National Guard cyber units that have since been deployed on real world cyber missions. This expands the region's ability to assess and secure infrastructure, including water systems. And it provides it where that local expertise is needed.

In the town of Ansted, West Virginia, ICS is guiding the town through its transition from paper-based processes to modern digital systems that support billing, payroll, and a new wastewater treatment facility. Our work includes vendor governance, IT/OT separation, secure remote access, and staff training. This provides a scalable model to rural communities, we feel.

In the Huntington water system, ICS is conducting on-site OT assessments in advance of a major upgrade to a digitally-controlled ultraviolet treatment system. Working alongside operators and National Guard cyber units, we help ensure cybersecurity is integrated into the system design, not added after the fact.

These engagements demonstrate what works: practical, repeatable assistance delivered where operators actually work.

Long-term resilience is going to depend on people. Marshall has developed and is developing stackable micro-credentials in the water sector for cybersecurity designed specifically for working operators that cannot leave their systems to attend extended training.

These programs teach secure remote access, segmentation, vendor oversight, and incident response. These are skills that reduce risk immediately.

From our field work, what we think is needed is pretty clear. One, we need targeted support for basic cyber hygiene. That includes multi-factor authentication, segmentation, secure remote access, and logging.

Number two would be a circuit rider style cybersecurity program for rural utilities, modeled after USDA's technical assistance program.

Number three would be incentives for small systems to adopt those Safe Drinking Water Act requirements, even though they fall below the population threshold. And, support from more university partnerships. Convert Federal guidance into applied improvements, and it is exactly what Marshall is currently doing statewide.

The operators who run America's small water systems are dedicated professionals who keep communities safe every day. With the right partnerships between utilities, National Guard

cyber units, Federal agencies, and universities like Marshall, we can make small and rural systems some of the most cyber-resilient in the Nation.

Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Mr. Simonton follows:]

Senator Capito. Thank you.

Before we go to the next witness, let me just ask you, OT stands for?

Mr. Simonton. Operational technology.

Senator Capito. Okay.

Mr. Simonton. Versus information technology.

Senator Capito. Right. Okay. Thank you.

I am going to turn to Senator Cramer to introduce our next witness.

Senator Cramer. Thank you, Chairman Capito, Ranking Member Whitehouse, for holding this very important and timely hearing.

It is a pleasure for me to introduce a fellow North Dakotan, Matt Odermann. He is here today in his capacity as an executive board member of the North Dakota Rural Water Systems Association. He has a big fan base there in the back, I noticed. They are all here for the same reason as the West Virginians are here.

Matt brings more than a decade of experience in cybersecurity and critical infrastructure protection, with a strong understanding of the unique challenges facing rural water systems. Matt serves as a cybersecurity supervisor at Minnkota Power Cooperative. Minnkota is a regional generation and transmission co-op with a number of distribution co-ops in the upper midwest, where he leads efforts to secure that IT and OT

environment across a multi-State utility footprint.

He has extensive experience in the rural water sector, serving as a board member of the All Seasons Rural Water Users District, and as past president of the North Dakota Rural Water Association.

I am not sure what you do in your spare time, Matt, and I am not sure who all pays you. It is impressive; you are a great servant. He is also a member of the Cybersecurity and Infrastructure Security Agency Water and Wastewater Sector Coordinating Council.

He will provide valuable insight for today's discussion on cybersecurity challenges facing water systems, and importantly, offer the rural system perspective on these challenges.

Thank you for sharing your knowledge with us today, Matt.

Senator Capito. Thank you. Mr. Odermann, you are recognized.

STATEMENT OF MATT ODERMANN, EXECUTIVE BOARD MEMBER, NORTH DAKOTA RURAL WATER SYSTEMS ASSOCIATION

Mr. Odermann. Good morning, Chairman Capito, Ranking Member Whitehouse, Senator Cramer, and members of the committee. Thank you for the opportunity to testify on this important issue.

My name is Matt Odermann, and I hail from the great State of North Dakota, where I do serve as past president of the North Dakota Rural Water Systems Association. North Dakota's rural water system has 282 members, serving 97 percent of the State's population.

I am especially proud to be a long-term board member of a small water system, All Seasons Rural Water District. And I am here today on behalf of National Rural Water Association, which represents 31,000 small and rural water utilities across the Country.

NRWA provides a diverse range of services to its members, including training, disaster planning, and relief in several affected technical assistance programs. Additionally, I represent the NRWA on CISA's Water and Wastewater Sector Coordinating Council. In that role, I participated in a cybersecurity task force focused on developing a practical plan of action to help the sector advance its cybersecurity posture.

For more than 20 years, I have worked in IT and

cybersecurity roles across critical infrastructure sectors. I currently serve as a cybersecurity supervisor for an electric generation and transmission cooperative. I have seen first-hand the cybersecurity challenges that play out in a converged IT/OT environment.

The vast majority of water and wastewater systems in this Country serve communities of 10,000 people or less. We have the same responsibility as large water utilities to deliver safe drinking water every second of every day.

The difference for us, though, is scale. Small systems operate with limited staff, limited revenue and limited technical capacity. Most do not have in-house cybersecurity personnel.

In rural America, cybersecurity is not a question of indifference, it is a question of capacity. The threats are real, but so is the progress. Cybersecurity awareness in the water sector is growing, largely through trusted, non-regulatory partners like NRWA, State rural water associations and the WaterISAC group.

Through these efforts, we are seeing a cultural shift. More and more rural water systems are moving to an understanding that cyber risk is part of operating a modern utility. At the same time, how Federal security efforts are delivered matters just as much as what is required.

From the sector's perspective, the EPA is first and foremost a regulator. When cybersecurity became part of the sanitary surveys, many utilities felt that they were being asked to self-report cyber weaknesses to an enforcement agency. That created confusion and concern.

For example, water system operators reporting an outdated firewall in an effort to be transparent worried it might lead to some sort of enforcement action. Even when intentions were not meant to be punitive, the regulatory power dynamic shapes how those actions are received.

Long-term improvements are built on collaboration and trusted technical assistance, not fear of violations.

There is also a cultural gap. When cybersecurity is framed as compliance or abstract IT risk, it feels disconnected. However, when it is framed as protecting pumps, SCADA systems, and the ability to keep water flowing 24-7, operators understand that.

That translation layer is critical. And organizations like NRWA, State rural water associations and others play a key role in bridging that gap.

Based on my experience, I offer the five following principles. First, lead with assistance, not enforcement. Adoption is stronger when cybersecurity is delivered as support, not primarily as a compliance obligation.

Second, fund any mandate. Cybersecurity requires hardware, software, training, and staff time. For small systems, even a few thousand dollars can be a barrier.

Third, focus on foundational controls. Many systems struggle more with phishing, weak passwords, and legacy equipment rather than nation-state threats.

Fourth, rely on established, trusted partners. Guidance delivered through organizations utilities already rely on is more likely to be implemented.

And fifth, recognize diversity. A system serving 800 people and 2 employees cannot be treated the same as a large utility.

In conclusion, protecting small systems must be a national security priority. With the right balance of partnership, practical guidance, and resources, we can strengthen cybersecurity across America's water infrastructure, not through fear, but through collaboration and resilience.

Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Obermann follows:]

Senator Capito. Thank you very much.

Finally, we are going to hear from Scott Dewhirst. Thank you for coming. Mr. Dewhirst is the Deputy General Manager of Engineering and Technology for Fairfax Water. He is testifying on behalf of the Association of Metropolitan Water Agencies this morning.

He has held various leadership roles for utilities in Tacoma, Washington and Newport News, Virginia. You have been all over the place there, that is good.

Mr. Dewhirst, welcome. You are recognized for five minutes. Thank you for coming.

STATEMENT OF SCOTT DEWHIRST, DEPUTY GENERAL MANAGER, ENGINEERING AND TECHNOLOGY, FAIRFAX WATER, ON BEHALF OF ASSOCIATION OF METROPOLITAN WATER AGENCIES

Mr. Dewhirst. Thank you. Chairman Capito, Ranking Member Whitehouse, Senator Cramer, and members of the committee, thank you for the opportunity to testify before you today to testify. My name is Scott Dewhirst, and I am the Deputy General Manager of Engineering and Technology at Fairfax Water, over engineering and technology.

I am here today on behalf of the Association of Metropolitan Water Agencies, otherwise known as AMWA, an organization that represents the large publicly owned drinking water systems across the Country.

I also serve on the board of managers of WaterISAC, the water information sharing and analysis center, which is the water sector's dedicated information sharing hub for cyber, physical, and natural threats.

Cybersecurity in the water sector is a growing issue that grows more urgent by the day. Drinking water systems represent an attractive target for cyber adversaries. There have been insufficient Federal resources dedicated to this topic.

A successful cyberattack on a water utility would not only threaten water quality and public health, but would also undermine public confidence in the safety and reliability of

drinking water. Cyberthreats have become more frequent, more sophisticated, and more damaging. Addressing them requires sustained investment in people, technology and planning.

According to WaterISAC's most recent cyber incident survey, about 14 percent of responding water systems reported experiencing at least one cyber incident during the quarter, up from 11.5 percent during the same period in the last year. As a large public water system, Fairfax Water employs a dedicated cybersecurity staff. Incident response plans and the ability to leverage resources offered by Federal and sector sponsors, including the EPA, the Cybersecurity and Infrastructure Security Agency, otherwise known as CISA, and WaterISAC.

However, Fairfax Water is not typical in terms of its robust cyber capabilities. Of the Nation's roughly 50,000 community water systems, many lack the personnel or financial resources needed to utilize Federal guidance, assess risks, or implement recommended actions.

There are many ways to meaningfully strengthen cybersecurity across the water sector, including by increasing resources for risk mitigation response, authorizing targeted grant funding for cyber resilience, ensuring that State and local governments are well resourced, and mapping out implementable minimum Federal cybersecurity standards.

It is critical that existing resources like WaterISAC are

well funded and being utilized across the industry. WaterISAC lays a unique role in the sector's cybersecurity preparedness by actively monitoring cyber threats and vulnerabilities affecting water utilities. It also provides guidance on risk mitigation tools, best practices, and response actions that contribute to an all hazards resiliency posture.

Despite its critical role, WaterISAC receives no State or Federal grant funding and faces challenges in connecting with the thousands of water systems across the Country. My written testimony cites legislation that could help expand access to this wonderful resource.

Congress should also recognize that cybersecurity must compete for water systems' attention with more high profile needs, like infrastructure upkeep, compliance with regulatory mandates, and keeping bills affordable for ratepayers.

To help water systems invest in cyber defenses, in 2021 Congress authorized EPA's Mid-Size and Large Drinking Water System Infrastructure Resilience and Sustainability program, and a compatible program for clean water agencies. The programs offer grant funding for cybersecurity enhancements.

However, these programs have received minimal funding. Congress should commit to providing adequate funding to help water systems meaningfully invest in the software upgrades, security personnel and enhanced threat detection and monitoring

procedures.

Finally, while guidance and tools provided by EPA and CISA are valuable, there are currently no statutory Federal cybersecurity requirements for water systems, making these best practices optional and leaving less resourced utilities wholly unprepared for a cyber incident.

AMWA recognizes the danger in making Federal regulations overly burdensome, complicated or prescriptive, especially in a rapidly evolving threat environment. At the same time, some level of Federal guidance would help ensure that all water systems are taking appropriate steps to protect against cyber threats.

One proposal I believe warrants further consideration is establishment of a water risk and resiliency organization, or WRRO, that would be comprised of cyber experts and drinking water and wastewater system operators. This WRRO would develop, recommend and oversee cybersecurity guidelines for drinking and wastewater systems, tailored to their size and risk profiles.

Based on the model of the North American Electric Reliability Corporation, otherwise known as NERC, and the energy sector, this organization would work in partnership with the EPA to ensure that water systems of all sizes secure themselves against cyber threats while avoiding the unworkable one-size-fits-all mandates.

While it is clear there is much more work to be done to strengthen our water systems' cyber posture, AMWA stands ready to work with you toward meaningful solutions.

On behalf of AMWA, thank you for the opportunity to testify today. I look forward to your questions.

[The prepared statement of Mr. Dewhirst follows:]

Senator Capito. Thank you. Very good.

You came right in at the zero zero mark. That is very precise, I will tell you.

So we are going to start the question portion. I will begin with Dr. Simonton.

You highlighted, obviously, what Marshall University's Institute for Cyber Security is presently partnership with Ansted, which is just to frame it for the audience, a very small area. And the Huntington water system, which, I don't even know if it would be a medium size, but I would put it in that category, not large large like Fairfax, but large, larger.

I was interested to hear, and I heard this from the rural water utilities folks that came in to see me yesterday from West Virginia, the circuit rider, cybersecurity circuit rider idea through the Department of Ag. So if you could frame out just briefly how valuable circuit riders are in general for physical infrastructure for the smaller systems, and then how somebody dedicated fully to cyber, would you see it as a dedicated cyber, would that be the best, or somebody who has that enhanced credentialing that could do both on the existing program?

Mr. Simonton. Thank you for that question.

As far as the circuit rider is concerned, the university is already able or we are moving toward supplying both students to do these things for the utilities or others that don't have that

in-house capacity. And of course also with our National Guard units that we are training, not just in water cyber, but in infrastructure security in general.

So I would see or we would see these circuit riders as dedicated certainly to cybersecurity, because that is the need within the utilities.

Senator Capito. They could fill a day with that.

Mr. Simonton. They could fill a day with that, absolutely. And they provide that expertise. They basically become consultants to the various utilities that provide the expertise that they don't already have. So that is how we would see those circuit riders or that ability to provide that capability that the utilities don't currently have.

Senator Capito. So let's say at Marshall, since you are dealing with this, cybersecurity for critical infrastructure as a general rule, would it be, and I said in my statement it can't be a one-size-fits-all. So would it be a parameters thing where you could then have, technical assistance is what all three of you have said would really need, you are not expecting the one and two and three person utility to be able to meet this challenge on their own, they have to have assistance.

Would it be like a framework for smaller systems that could then sort of be a plug-and-play type of thing?

Mr. Simonton. That is what we are trying to develop, is

this scalable plug-and-play framework. Every system, of course, is going to be different. But the needs are going to be very similar. They are going to have similar systems, they are going to have very similar threats, they are going to have very similar needs.

So we are developing this framework that can apply not just to water utilities, but across infrastructure. And so, again, it is providing that in-house expertise.

Senator Capito. All right, good, thank you.

Mr. Odermann, we are talking about rural water systems here, and the unique challenges of the systems in rural areas. We all know that if you can get into one system, a lot of times that can lead you to another system. So there are vulnerabilities.

You said how many different systems do you have in North Dakota?

Mr. Odermann. There are 282 members of the Association.

Senator Capito. Yes, that is a lot of people.

Mr. Odermann. It is 97 percent of the State, so it is significant.

Senator Capito. So, how do you see that in terms of being able to serve where you are in North Dakota?

Mr. Odermann. The circuit rider program?

Senator Capito. Yes.

Mr. Odermann. The circuit rider program is single-handedly the most successful built-up program that I see in our State. It is mature, it is well-documented, the deliverables and administrative stuff is set up already. Those trusted relationships between those systems and the State association are built.

So if we were able to spin up a technical circuit rider for cybersecurity, I imagine the uptake on that would be significant.

Senator Capito. Thank you.

I want to talk about the workforce challenges. This is something I have been interested in, and several bills in the past have put in some availabilities for workforce development as our aging, as I see in West Virginia when I visit utilities, our general managers, who are all utility kind of, they do everything, from fixing the leaky pipes to running the system to doing the billing, everything, trying to get young people interested in this as a career is, I think, difficult.

I think the cyber aspect of it might have a little bit of a bump of more of the modernization of the systems, and you would be using all kinds of skill sets here.

I know one of our water systems in the audience has used like an apprenticeship type thing, where you would start in high school, coming to the utility, not even really thinking it is

something you want to do, but make a little bit of money. And the next thing you know, they are full-time employees working.

Have you had any experience with that, Mr. Dewhirst?

Mr. Dewhirst. At Fairfax Water, we do take a pretty aggressive approach with summer internships. I think what people don't understand, it takes many different types of skill sets and different types of jobs to run a water utility.

So this gives students a chance to really see what is involved, even in the cyber space, even in the technology space.

Senator Capito. Yes.

Mr. Dewhirst. Laboratory, whatever it may be.

So we think that is a great approach to getting people introduced to the industry and to have a long term career.

Senator Capito. Okay. Senator Whitehouse?

Senator Whitehouse. Dr. Simonton, I am pretty sure I remember driving West Virginia Supreme Court Justice Richard Neely to Marshall University to give a speech when I clerked for him years ago. So if memory serves, I have actually been on your campus. He was a very distinguished and lively person. Fair description?

Senator Capito. That is an understatement.

[Laughter.]

Senator Whitehouse. So, welcome, and thank you to Marshall University for your work on climate change. Your research,

Sustainability Day, or Awareness Day in the sustainability department, the climate change advocacy work you have done with Citizens Climate Lobby, the Armstead Lab's work on Appalachian Climate Resilience, Dr. Cartwright's work on young people's understanding of climate, you guys have done a lot of good work, and I am grateful to you.

Mr. Dewhirst, you mentioned the NERC model. What is the NERC model, and why might it work for water utilities as opposed to electric utilities?

Mr. Dewhirst. From my former experience in Tacoma, where we were a shared utility, water and power utility, I got to see NERC somewhat in action.

Senator Whitehouse. I was a utility regulator back in the day, so I am interested.

Mr. Dewhirst. Okay. NERC is set up to where, my experience has been where you have a mix of operators of the system as well as cyber experts that collaborate to develop standards and levels of compliance for different risks associated with each utility. So I think a model like that is worth a conversation to understand how we can make that work for all the different sized systems across the Country.

I think what it does, it allows not, it doesn't prescribe things, it is more of an outcome-based approach. It also gives risk-based challenges, risk-based requirements, so a system that

has more impact or more connectivity, if you will, across the space would have higher standards and expectations that one that is a little bit more isolated.

But yet it is very important to establish baseline standards for everyone. It also will work its way across the entire sector, no matter what the size would be. So I think that is an important concept that we need to think, so we are not leaving anybody behind, but we are growing together and collaborating on what is the best approach.

One more aspect I will bring up is it gives us a chance to be nimble. So as you have heard in all your comments this morning, your opening statements, these threats are evolving, they change quickly. We have AI, which just came out three years ago and now we are talking about it all the time.

So it allows us to move quickly and not have to wait up on another Congressional action to change a law or a standard, we can actually move more nimbly into other ways to address threats as they are coming up.

Senator Whitehouse. When I was first working on cyber, and we were trying to do a big bipartisan cyber reform bill, which actually got pretty close, Senators Kyle and Graham and McCain and Thune were all working with me on that, we nearly got it done. We were trying to figure out what were the best ways to have American businesses step up their cyber defenses in this

continually evolving environment, where if you set up our, if you have to go back and re-legislate that bar when things have changed, you have wasted everybody's time.

One of the things that we were looking at was to require cyber insurance, so that if you had sort of general liability insurance, you would have to carve out a cyber insurance defined sort of rider or element, so it didn't get buried in the overall thing. That would then focus the insurance industry, year by year as policies were renewed, in trying to look at how vulnerable you were, and in particular with respect to liability, whether you had met the prevailing standard of adequate defense, so that even if something did go wrong, you at least had the defense that you had done every reasonable thing that could be expected of you.

And it is a lot to ask of all of you in one minute and 30 seconds, but I would be grateful if you would take a moment after the hearing is over and think about what role requiring insurance, requiring a rider, requiring some specific aspect of the policy might have in terms of being that spur that continually drives forward and requires both the insurance side and the utility side to take a look at where they are on all of this.

Is the question clear enough? Okay, my time is up, so I will let that go. But I do look forward to hearing your written

responses about that and figuring out whether there is an insurance element to this that can help solve the problem. Thanks.

Senator Capito. All right. Senator Cramer?

Senator Cramer. Well, given Senator Whitehouse's time running out, I am intrigued. I think, Mr. Odermann, in your statement, your five points, by the way, were great. I couldn't get past the first one because it struck me. It made so much sense, as a former regulator recovering, myself.

You said provide assistance, not enforcement. And then I hear Senator Whitehouse talk about insurance. As I am listening to him for the first time talk about this, I am thinking to myself, okay, that is maybe a better regulatory system than a government agency, right? There is a market aspect to that.

Maybe, since he didn't have the time to listen, if you could start maybe to chime in on his point, and this point of not enforcement, but assistance.

Senator Whitehouse. And you can add Senator Cramer to your QFR response to me. Thank you.

[Laughter.]

Mr. Odermann. I think Senator Whitehouse was listening in to some of my conversations yesterday.

Senator Whitehouse. I am not that good.

[Laughter.]

Mr. Odermann. The fiduciary responsibility of being on a board, you typically look at, how do we cover our risks? Cyber insurance definitely is part of that. That is definitely driving some organizations to strengthen their cyber defenses.

Because if you are a higher risk, you pay higher insurance premiums. If you desire more coverage, they are going to investigate you a little bit more or make sure that, hey, is this somebody we can actually cover or not.

So the point about cyber insurance driving some of the changes is happening already. As far as dictating that in law or regulation, I am not sure how that would play out. But it is definitely moving the ball on the front lines.

Senator Cramer. So you all have alluded to, obviously, or been rather emphatic about the ability to collaborate, coordinate, particularly in rural, probably some of the big municipalities provide a little assistance. We have heard this, in all my years in Congress, when it comes to rural water systems, probably more than any other thing, please just, even technical support.

But this is a little bit different, because when you think about 282, as Senator Capito sort of gasped about, 282 members, that is a lot of members. One thing I know about your members, like most North Dakotans, is while they like to collaborate and partner, they also protect their sovereignty and autonomy,

maybe, even in some cases. Maybe give me a best practice that has worked for each of you as a way to just give us a little guidance. We will start with Mr. Dewhirst.

Mr. Dewhirst. I think that we as a large system example, we want to work together with everyone. I think we engage with our colleagues across the State in Virginia, for instance, and share ideas and share best practices.

I think the WaterISAC, I think that is a great example where we can all collaborate together. I think if we can bring awareness to incidents as they occur and that becomes a central clearinghouse for everyone in the Country, it gives us a way to manage those threats and make sure people, large, small, it doesn't matter where you are in the Country, is aware of those threats, and they can take mitigation steps to correct that.

So I think WaterISAC is a great tool to kind of weave through all of us to give us those standards and protections. Thanks.

Mr. Obermann. Definitely using trusted partners that already have those relationships built out. That is State primacy agencies, and State associations have a footprint in every community in North Dakota, for example. They know those circuit riders by name, probably have their cell phone. They probably know their kids' names and things like that. So that is a very trusted relationship.

What doesn't work is a 15-page bulletin information disclosure. That doesn't land with an operator in a small system. But definitely the trusted partners is where it works the best.

Mr. Simonton. I would add, first of all, Senator Whitehouse, I knew Richard Neely personally and have very cherished memories of spending time in his office.

I could also address it as a former regulator in West Virginia and in Idaho, as a consulting engineer that dealt with regulatory agencies. For the most part, especially at the State level, I have found the agencies to be really valuable partners and very helpful in trying to, regardless of the regulated community, help them comply with regulations and not always wielding the stick, but actually providing what can become a very trusted resource for these utilities, for example, in this space.

So that can be part of it, and not just the punitive part of the regulatory agencies, but I find them to be actually very helpful most of the time.

Senator Capito. Senator Blunt Rochester?

Senator Blunt Rochester. Thank you, Chair Capito, and Ranking Member Whitehouse. And thank you so much to the panelists for being here today.

For me, this hearing on cybersecurity and our Nation's

water and wastewater infrastructure is both critical and timely. According to reports, and these are public reports, one is even from my region, the Delaware Currents, there is a quote that, once a hacker gets into a water system, they could potentially turn pumps and motors on and off, alter chemical levels in drinking water to dangerous levels, and even plant software bombs that could disrupt the water system later.

That same report went on to say that there are risks associated with poor cyber hygiene, as you mentioned, to States and also that cyber attackers come in many forms, from disgruntled former employees to nation states like China, Iran, South Korea and Russia.

So to be clear, this is the kind of stuff that could keep you up at night. I don't know if it keeps you all up at night, you are all shaking your heads. But one of the things that I thought about, when you add onto it in this moment, is extreme weather. That is another whole risk.

So I want to start with you, Dr. Simonton. I come from a State that is urban, suburban, rural and coastal. We also have many small towns.

I am curious, do water utilities account for extreme weather events when thinking about cyberattacks? And what additional steps are needed?

Mr. Simonton. Thank you for that question, Senator. I

think that we have been blessed in this Country with infrastructure that works. So people don't give it a whole lot of thought, because when they turn their tap on, they get clean water.

So we are seeing, whether it is chemical spills, extreme weather events, that our infrastructure is fragile. And so we get these messages on occasion, when there are these disruptions.

So I think across the industry, and certainly, I can speak just across civil and environmental engineering in general, we are certainly starting to take extreme weather events into account in design and maintenance and certainly that is going to apply to cyber systems within these utilities and therefore cybersecurity becomes an issue.

Senator Blunt Rochester. Thank you for that answer.

The Midsize and Large Drinking Water Systems infrastructure program, which is run by EPA, is one of the few Federal grant programs that helps water systems reduce cybersecurity threats. Unfortunately, the program has never been funded near its authorized level of $50 million, and is set to expire in Fiscal Year 2026.

Last month, my Republican colleague, Senator Curtis, and I introduced the Water Infrastructure Resilience and Sustainability Act to reauthorize this critical program.

Mr. Dewhirst, thank you for mentioning our bill in your written testimony. Why is reauthorizing this program so important right now and how utilities use the program's resources to strengthen cybersecurity protections?

Mr. Dewhirst. First of all, thank you for the question, and thank you for your sponsorship, and Senator Curtis, of that bill. I would just alert; that bill has such a wide range of uses it can be used for. Cyber is one of them for sure.

So it allows a lot of the basic stuff that needs to be done on the cyber front to be done, whether it is doing a simple assessment about where your vulnerabilities are located, employing some software tactics, multi-factor authentication, segmenting your network, other types of things, like firewall additions, those sorts of things. It is there for everyone to partake in.

I will echo your comments that it has not been funded to the level that it should. Even thought it is authorized, it has not been appropriated. So I think any improvement in that front would be appreciated by all of us sitting at this table here, because I think it also does touch all the systems of all sizes in various ways.

We would very much strongly echo your sentiments to fund it appropriately.

Senator Blunt Rochester. Thank you.

Mr. Odermann, you are shaking your head. I want to give you an opportunity to respond.

Mr. Odermann. He nailed it. But the only thing with some grant applications for smaller systems is it can be an administrative workload that they just simply don't have the capability to --

Senator Blunt Rochester. It is back to the capacity.

Mr. Odermann. Yes. Again, that is where a circuit rider concept could assist in those types of applications and management.

Senator Blunt Rochester. Thank you. Also, Dr. Simonton, when you talked about the stackable water credentials, I think that is so important too. As a former personnel director for the State of Delaware, understanding that when you don't have that capacity, it might be only two people or three people that are working in these small places. So making sure that we have those.

The other question -- my time has expired, but I will submit for the record questions on the use of AI tools and AI agents. This is something that is really important to me. I have a couple of other questions for the record as well.

Thank you, Madam Chairman, for this incredibly important and timely hearing. I yield back.

Senator Capito. Thank you.

Senator Ricketts?

Senator Ricketts. Thank you, Chairman Capito, and Ranking Member Whitehouse, for holding this important hearing today, and thank you to our witnesses for coming and sharing your perspective on what we can do to better secure our water systems against the cybersecurity challenges that we face in our world.

In Nebraska, our water and wastewater utilities manage and protect our State's groundwater, they provide critical services to Nebraskans, and we have talked about how it impacts the States where you are from.

The security is increasingly at risk from foreign adversaries seeking to undermine critical infrastructure, and threaten public safety through cyber attacks on our water systems.

Communist China has actively been involved in targeting wastewater systems, critical infrastructure in every community across the U.S. And in 2024, the EPA OIG found that nearly 100 drinking water systems serving 26.6 million people had critical or high risk cybersecurity vulnerabilities.

This includes open internet portals, default passwords, unpatched systems. These vulnerabilities leave utilities exposed to cyber criminals and foreign adversaries.

It is important that rural water systems have the tools, resources, and technical support necessary to defend against

these cyber and foreign threats. Yet many small and rural communities face significant barriers in accessing these tools and resources.

Just yesterday I met with the Nebraska Rural Water Association who shared some of these challenges, such as the staffing shortages we have discussed and reduced technical capacity. To protect our water systems, our food supply, and ultimately our national security, we must ensure rural communities are equipped to build and maintain resilient water infrastructure.

In West Point, Nebraska, they are doing just that. They have upgraded their system to a cloud-based management platform. These platforms allow water utilities to monitor and manage infrastructure for many locations and house data in a secure location.

Mr. Odermann, what do you think the relative advantages of moving water operations to a more advanced automated program, like the cloud, versus what they have historically been at?

Mr. Odermann. There are definitive advantages to that model. Scalability, there is long-term cost savings. Typically you are not having to house as much technology equipment in-house.

You get baked in security practices. They are not going to let you do certain things on the cloud platform without

following certain guidelines and standards.

And then to speak to the weather thing, it is geolocation diversity with where your data is stored, so you have some disaster recovery advantages as well.

The one negative would be, it takes a different technical setup and configuration to manage cloud services. So that is a little less limited than the traditional client-server setup.

And then also you are dependent on an internet connection. So if you are somewhere without an internet connection, you are stuck.

But there is definitely a model that would work there.

Senator Ricketts. One of the other things we have heard is that with modern systems, you have to upgrade them more often. Is that what your experience is in North Dakota as well?

Mr. Obermann. Yes, updates are all-consuming of my life right now. That is what keeps me up at night.

[Laughter.]

Mr. Obermann. Yes, it is a challenge, and again, that is where these smaller systems just don't have the capacity to manage all those IT and OT assets. Giving them technical assistance to align with a trust vendor that meets standards would be an avenue for them.

Senator Ricketts. Great. Thank you.

Dr. Simonton, I was mentioning some of the cyber-attacks,

some of the things that can leave us open and vulnerable. What documentation do we have on attempted attacks against water infrastructure? What do we know about the sources or the actors behind these attacks?

Mr. Simonton. I don't know that I can really speak to that, Senator, because so much of what happens, I mean, as you probably well know, the United States suffers a mind-boggling number of attacks every day. So how many of those are directed specifically at the water sector, I couldn't answer that.

Senator Ricketts. So, would it be helpful then if we were trying to do more documentation specifically on our water systems and wastewater systems to be able to know how much is that being targeted versus, say, hospitals, which have typically been very high profile when they get attacks, and they have a ransomware attack, you know, because everybody at the hospital can't get treatment, right?

Mr. Simonton. Absolutely. And what we are seeing across the board in infrastructure, and what we are doing at Marshall University, is not just focused on water cybersecurity, which is what we are talking about today, and really where we started to build the framework, but we are already working in health care, finance, transportation, specifically aviation, because all of these areas of infrastructure are coming under more and more attack. And with automation, of course, more and more

vulnerabilities.

Senator Ricketts. And I will note that there are members of the Nebraska Rural Water Association in the audience today. Thank you very much for your help.

With that, Chairman, I will turn it back over to you.

Senator Capito. Senator Husted?

Senator Husted. Thank you, Chairman Capito, and a lot of great questions and comments. I appreciate it.

Actually, when I was Lieutenant Governor in Ohio, worked in cybersecurity issues with local governments all the time. They were quite common, attempts at local government. I am just curious if any of you would just like to put in context how common a rural water system, how often a rural water system will receive an attempted cyberattack?

Mr. Obermann. Everybody is looking at me.

[Laughter.]

Senator Husted. I was going to let you choose.

Mr. Obermann. I would say that it happens probably daily. Whether there is impact from these cyber attacks --

Senator Husted. You mean attempted attacks?

Mr. Obermann. Attempted attacks, it could be just a phishing email or a port scan of their device and nothing really occurs. I do know that we have had some in North Dakota that have risen to where it has been passed on to the State and local

information center to investigate and provide some technical assistance on investigating what happened there.

But a true number --

Senator Husted. It happens daily?

Mr. Obermann. I would say daily, yes.

Senator Husted. And Senator Ricketts made a very good point about migrating your systems to a cloud-based system, because that, in almost every case I know of, is a preferable way to manage it. Would you agree with that?

Mr. Obermann. There are definite advantages, like I said. Personally, what I like the most about that --

Senator Husted. But that is the advice you would give somebody?

Mr. Obermann. Yes.

Senator Husted. It is just general advice. But I also have learned in the past that it is, despite the training, despite the systems and all that, it is usually a human error that leads to this. So that is the training, that is the awareness. I see all your heads nodding. Please feel free to speak up on that, if any of you want to make a point about the importance of that.

Mr. Simonton. In developing our micro credentials, we have worked closely with water utilities, especially small water utilities. They do kind of throw their hands up on when it

comes to the cybersecurity aspect, they know that they are vulnerable, but they know what they don't know. And they know that they need the training, they need the expertise to help at least from an awareness standpoint.

So the industry is quite aware of the need for training, and I think that is what is important.

Mr. Dewhirst. I would just echo that again. I think the phishing campaigns that are out there are becoming more sophisticated. And that is a simple email. And we all get a thousand emails a day, sometimes. And you are scrolling through, and you can actually hit the wrong button and automatically go to a link that could cause a lot of problems, a lot of harm.

Senator Husted. Don't click on links.

Mr. Dewhirst. But again, it takes that culture, it takes that awareness, it takes people to take a minute to think about it before they do it, and oftentimes you are in such a hurry to get things done you don't do that.

Senator Husted. And where are rural water systems, I mean, do you think they know that? Do you think they are aware of that? And then I want to add, and then what should they do if there is a breach? What is it that they are supposed to do? What is the first thing that they are supposed to do?

Mr. Obermann. First, yes, I think generally they are aware

that there is phishing attacks and things of that nature. The first thing they should do if they are under attack is reach out to that trusted resource. For most people in North Dakota, that would be probably their membership's or their system's IT group that they work with.

And after that would be North Dakota SLIC, which is State and Local Information Center and so on and so forth. Hopefully, that State and Local Information Center can direct them into the resources that they need.

Mr. Dewhirst. And I think one thing, if I could, the utilities really pride ourselves on being prepared and having a plan. I think one of the most important things for every utility, whatever size, is to have a cyber response plan, so you know what to do, you know what to do if and when it happens. When you are ill-prepared, to think clearly in that moment, so to know what you need to do and address that is something we should all be aware of and have on our ready.

Senator Husted. Yes. And is there a Federal agency that you would inform, and if so, who?

Mr. Dewhirst. CISA would be the obvious choice. I again want to echo my comments earlier about WaterISAC and how I think it could play a critical role in connecting utilities, so that when incidents occur, no matter where they are, they can be brought to light and shared with others across the Country in a

very expeditious way, so we can guard against that happening somewhere else for the same vulnerability.

Senator Husted. Yes. Well, I will just close, I know my time is running out. From my research, most of the attacks come from North Korea, Iran, Russia, and China. They don't come from Ukraine or Israel. And I just want to note that.

Thank you, Madam Chair.

Senator Capito. Thank you. Senator Schiff?

Senator Schiff. Thank you, Madam Chair, for calling this hearing on such an important but often overlooked topic. I share many of the concerns I think you have about making sure our water and wastewater systems are protected from cyberattacks. This is a critical issue at the nexus of water affordability, environmental quality and national security.

I have been working on a bill to provide EPA with more tools to address the issue and provide water systems with the resources they need to properly fortify their cyber systems, without impacting the water and sewage bills paid by American households. I am hopeful that this committee can work together to work on addressing this problem.

I have a couple of questions, and I offer to anyone on the panel who would like to weigh in, how prevalent do we believe the ransomware attacks are? I know that particularly in corporate America, there is reluctance to notify the Bureau or

anyone else when there is a cyberattack, for fear of it becoming public and reputational harm.

Do we have any sense of how often water systems are under ransomware attacks?

Mr. Obermann. I don't think we have a clear understanding of what it is, but ransomware attacks are definitely more prevalent than nation-state attacks. Nation-state, or nation sponsored threats tend to just lie in wait. They try and exfiltrate data. Where ransomware is more of a criminal mindset, where we are going to try to leverage and get some money out of these people.

It is devastating to members. I know in North Dakota, there have been a few hospital systems that have suffered ransomware attacks. It has been particularly hard for them. They have had to get short-term financing just to bridge through, to get their billing reenabled.

It is a very serious thing.

Senator Schiff. I remember a hospital in my district, this was probably eight or ten years ago, and this was quiet compared to today, locked up all the hospitals data. The hospital went to the FBI and said, what do we do?

And they were demanding, I think, $17,000 in cryptocurrency. And the FBI said, do you want your data back? And they said, we need our data. And the FBI said, then pay

them.

I am sure they wouldn't demand $17,000 anymore. But there is no requirement that water systems report when they are the victims of cyberattacks. So do we really just not have much of a sense at all of how often it happens?

Mr. Dewhirst. I will just say again, WaterISAC tries to be that central repository. So we are aware of some, but they are usually anonymized, so we don't single out, we don't say a certain city or county or whatever. We try to make it just, hey, make awareness that this ransomware attack did occur. Here is the avenue by which they accessed their system. Make sure you address this vulnerability.

That is how I think we can grow together and learn together, is by that central repository.

Senator Schiff. How many are you notified by, say, within the last year?

Mr. Dewhirst. Of ransomware attacks?

Senator Schiff. Yes.

Mr. Dewhirst. I don't think that many. I mean, like a handful. For the water specific, I think it is water specific, is what you are asking.

Senator Schiff. Yes.

Mr. Dewhirst. Yes.

Senator Schiff. Some of the destructive attacks that we

have become aware of have targeted smaller water systems in kind of random locations. Do we think it is just because they were targets of opportunity, that is, that foreign malign actors, Iran, whoever, are simply looking to punish the United States, and they have identified, hey, this water system is using dated software or whatever? Is that what we think is going on with the kind of strange target selection?

Mr. Simonton. I believe that what is happening is they are attacking many systems all at one time, and looking for those vulnerabilities. Some of those systems will provide those vulnerabilities. So I think that it is a widely-cast net, and then just the unlucky few are actually getting hit.

Senator Schiff. And is the net cast by a spear phishing email that is sort of blasted out? Or how do they cast the net?

Mr. Obermann. It can be. In my current occupation, we see that weekly, that spear phishing campaign. Generally speaking, when it comes to OT networks and IT networks that are live on the internet, that is through like a random port scan. They are just scanning a whole list and they get returned values of, yes, this port is open. I am going to see if we can go further here.

Senator Schiff. And that kind of search is done not just of water agencies, it is kind of a broad search for someone using an unpatched software?

Mr. Obermann. Yes. There is really no way to tell, like

from a port scan, if it is a small water system or a large utility. It is just a wide net. As soon as they see that that port or that service is open, they dig further and see if they can exploit the vulnerability.

Senator Schiff. Last question. The major infiltrations, like the Chinese Salt Typhoon, do we know whether we are having any success in excising that stocking horse? I don't know whether that may be beyond the scope of what we can discuss in this hearing. But how much do we know about what may be lying in wait?

Mr. Obermann. I will do my best to answer this question. That is a very serious concern in the cybersecurity community.

Have we made headway? I think there is a little bit more information sharing coming down from like FBI InfraGard on some of those things. We get that information faster through the information sharing and analysis centers, like WaterISAC and ISAC and the like.

So that information does get to us faster. Whether it is acted on, I don't know if I can provide any details on that. But it is definitely a concern.

Senator Schiff. Thank you, Madam Chair.

Senator Capito. Thank you.

Senator Markey?

Senator Markey. Thank you, Madam Chair, very much.

Mr. Dewhirst, your testimony outlines recommended legislative solutions to address the cybersecurity challenges facing the water sector, including my bill, the Water Intelligence Security and Cyber Threat Protection Act. I was proud to develop that legislation with the Association of Metropolitan Water Agencies. Boston Water and Sewer played a central role in establishing the Water Sharing and Analysis Center, which is known as WaterISAC.

So water infrastructure cybersecurity is a point of pride in our State. In fact, in 2024, Boston Water and Sewer experienced a ransomware attack that WaterISAC successfully assisted them in navigating, avoiding widespread damage to our system.

Mr. Dewhirst, are there any other organizations that compare with WaterISAC in terms of services and real-time assistance to water utilities?

Mr. Dewhirst. Yes, thank you for the question, and thank you for your support of that bill. I think that is a wonderful avenue for us, all utilities, to take advantage of and to really make WaterISAC an important pillar in our response to cybersecurity threats.

I would say, many utilities have to have third party assistance at the ready. We have contracts that are typically a zero retainer contract with different firms to be ready to

respond to a cyber incident should that occur.

So I think WaterISAC can provide some initial support and some initial guidance, if something were to occur. But I go back to the need to have a plan, a cyber plan in place, and it is a response plan in place, to know how to behave as soon as that happens.

Senator Markey. But right now, there are no other organizations that are comparable?

Mr. Dewhirst. Not that I am really aware of. I will defer to others.

Senator Markey. So it is clear that if we want to support our water systems in dealing with cyber threats, we need to support this water cybersecurity organization.

Mr. Dewhirst, do you agree that the primary barrier for water utilities to access these vital cybersecurity services is simply funding?

Mr. Dewhirst. I think it is funding, and also I think time. I think we have heard up here a lot with the rural systems. They have a lot of things they are doing. They don't have dedicated staff for certain things. So I think that is an aspect.

So I think WaterISAC can hopefully --

Senator Markey. Is funding the principal reason?

Mr. Dewhirst. Funding is a big deal. So we are trying to

establish that.

Senator Markey. Vision without funding is an hallucination, right?

Mr. Dewhirst. Absolutely. We need money.

Senator Markey. Without funding, how are you going to get it done?

Mr. Dewhirst. We need funding. Yes.

Senator Markey. Thank you. That is why I introduced my legislation, which would provide the funding to water utilities to access the cybersecurity services offered by WaterISAC. I look forward to working with my colleagues on that.

The reason I am really apprehensive about this is that there was a cyber incident called Stuxnet back in 2010. It really drew a lot of attention to this entire area. So the CIA and the national security apparatus of the United States came to me as the chairman of the Energy Subcommittee to ask me if I would pass legislation that would mandate that electric utilities in America upgrade their cybersecurity.

I took my counterpart, Fred Upton, the Ranking Member on the committee, we went down, we got the top secret briefing, we could see how dangerous it was. And we brought all the other members down to get the secret briefing. They were terrified at the fact that the Iranians and the North Koreans and the Russians and the Chinese were all attacking our electric grid

system every single day, trying to find vulnerabilities, getting ready for the moment when they could do it.

Again, Thomas Alva Edison would recognize our electric system in terms of the level of protections that are built in.

So, we had a piece of legislation, we drafted it, we passed it on a bipartisan basis. What happened was it came over here to the Senate, this wonderful institution that I now serve in. Senator Kyle from Arizona got lobbied by his electric utility, and they didn't want to spend the money, even though Fort Huachuca in Arizona is on the public grid, making it easy access into that incredibly important military facility in our Country. And it died over here, in the Senate. And it has died year after year, even though we passed it unanimously in the House. Because the electric utilities did not want to spend the money.

But it is a game of cat and mouse, right? And the cat, all of these incredibly powerful, super-sophisticated cyber giants around the world, and the mouse is our electric grid and our water systems. They are unprotected. They still haven't had the upgrade in the cybersecurity protections which they need, waiting for the eventual, inevitable, inexorable, successful catastrophic attack.

So it is just time for us to get real about this issue. It is only now 100 times worse because of AI in terms of the sophistication of the technology which can be used. And it is

time for us to put a mandate in place, and the funding that accompanies that, so that all of these vulnerable infrastructure systems are able to protect themselves against the attack which is coming. The only question is, are we going to protect against it?

Thank you, Madam Chair.

Senator Capito. Thank you. We don't have any further questions, and I would like to thank the witnesses.

Yes, Senator Whitehouse?

Senator Whitehouse. I just wanted to make one brief point --

Senator Capito. Of course.

Senator Whitehouse. -- about the distinction between nation state cyberattacks and ones that are done more by criminal organizations. Just to be clear, that there is not really a very clear dividing line between the two.

It is quite apparent that Russia, while it may engage in some specific cyberattacks on its own account through the FSB and other official organs of Putin's thug-oligarch government, also supports, encourages and funds all sorts of organizations that are driving hacks out of Moldova or out of Lithuania or out of wherever.

While those are not purely nation state attacks, they are subsidized and authorized, and they are constantly probing for

weaknesses, so that while they may get a hit at putting the target's equipment into a lockbox and extracting ransom, they are also providing information to Russia about where vulnerabilities are, so that when they want to move as a nation state to attack our resources, they can do so.

And maybe even light up these other groups to go and do it on their behalf, so they can keep a veneer of deniability, the say way that Putin is keeping a veneer of deniability of the destruction of infrastructure through the Baltic by pretending that these ships that are dragging their anchors through cables and disrupting them are somehow not anything that he has anything to do with.

So I just want to make sure that in the record of this proceeding, it is quite clear that the difference between a direct nation state cyberattack and this sort of grey zone of nation state supported semi-deniable partly kind of just gangster and criminal behavior stuff is not that clear.

Senator Capito. Right. Yes, I would like to make an additional point. As somebody who lives in a community who lost their water source through a chemical spill for many weeks, there are a couple of things beyond what happens to the destruction of the system. It becomes a very emotional response, and it can really grow, because you begin to lose trust.

Your authorities, the health authorities and otherwise, unless they are crystal clear, and we have gone through this with the CDC, because they were not in this case, begin to take on a greater role. And they have to be prepared for this, too, whether it is a cyberattack or chemical spill or whatever.

So if you are able to infiltrate successfully a cyberattack on one of your smaller systems, there might be people that would say, oh, well, that only serves 2,500 people, that doesn't really matter. But what matters is the lack of trust and the cascading effect that it has in every rural community of, this could be me, and how do I know?

So that is why I think at every level, that we need to make sure that the protections that we afford the larger systems are the same protections that we can provide for the smaller systems.

I was also thinking, if, let's say, you have the same IT person or something, they get into a small system in Ansted and then maybe that same IT system does Fayetteville, and then, is there a way in? And then you are into a bigger system, because you are into the whole IT system. So it is no longer Ansted, who has, I don't know, 600, 700 people, and they are into a bigger thing.

So I think there is a lot more connectivity here, and a lot more emotional part of protecting our rural water systems than

we really got into today. I would identify also a gap. I think we need better data on how many attacks, because nobody really had the answer to that question. I think, how many, where are they occurring, how they occurred, that is always going to be good for best practices to try to prevent.

So those are my little commentaries. I would like to thank all the rural water people who are in the audience today for coming.

Senators who wish to submit written questions, and we did hear at least from Senator Whitehouse and Senator Blunt Rochester, they are going to want to submit questions, and maybe Senator Ricketts. They have until 5:00 p.m. on Wednesday, February 18th to submit their questions. The witness responses to these questions are back to the committee no later than 5:00 p.m. on Wednesday, March the 4th, and will be submitted for the record.

With that, this hearing is adjourned. Thank you all very much. It was very interesting.

[[Whereupon, at 11:21 a.m., the hearing was adjourned.]