This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

Diversified Reporting Services, Inc.

RPTS BRENNAN

HIF031180

HEARING ON

RE: ENSURING THE CYBERSECURITY OF AMERICA'S DRINKING WATER SYSTEMS

WEDNESDAY, JANUARY 31, 2024

House of Representatives,

Subcommittee on Environment, Manufacturing, and Critical Materials,

Committee on Energy and Commerce,

Washington, D.C.

The Subcommittee met, pursuant to call, at 2:03 p.m., in Room 2123, Rayburn House Office Building, the Hon. Chair Buddy Carter [Chairman of the Subcommittee] presiding.

Present: Representatives Carter, Palmer, Crenshaw, Joyce, Weber, Allen, Balderson, Fulcher, Pfluger, Miller-

This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

Meeks, Obernolte, Rodgers (ex officio); Tonko, DeGette, Schakowsky, Sarbanes, Clarke, Ruiz, Peters, Barragan, and Pallone (ex officio).

Staff present: Kate Arey, Press, Digital Director; Sarah Burke, Deputy Staff Director; David Burns, Professional Staff Member; Marjorie Connell, Director of Archives; Jerry Couri, Deputy Chief Counsel; Nick Crocker, Senior Advisor & Director of Coalitions; Sydney Greene, Director of Operations; Rebecca Hagigh, Executive Assistant; Nate Hodson, Staff Director; Tara Hupman, Chief Counsel; Daniel Kelly, Press Assistant; Patrick Kelly, Staff Assistant; Sean Kelly, Press Secretary; Alex Khlopin, Staff Assistant; Peter Kielty, General Counsel; Emily King, Member Services Director; Elise Krekorian, Counsel; Drew Lingle, Professional Staff Member; Mary Martin, Chief Counsel; Kaitlyn Peterson, Clerk; Karli Plucker, Director of Operations; Carla Rafael, Senior Staff Assistant; Peter Spencer, Senior Professional Staff Member; Micheal Taggart, Policy Director; and Dray Thorne, Director of Information Technology; Timia Crisp, Minority Professional Staff Member; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff

Director; Caitlin Haberman, Minority Staff Director, Environment, Manufacturing, and Critical Minerals; Brian Hall, Minority Energy Fellow; Mackenzie Kuhl, Minority Digital Manager; Emma Roehrig, Minority Staff Assistant; Kylea Rogers, Minority Policy Analyst; and Andrew Souvall, Minority Director of Communications, Outreach, and Member Services.

*Mr. Carter. The Subcommittee will come to order.

The Chair recognizes himself for an opening statement.

STATEMENT OF HON. BUDDY CARTER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

*Mr. Carter. Before diving into today's very important hearing, I would like to take a moment to thank Representative Bill Johnson for his leadership of the Environment, Manufacturing, and Critical Materials Subcommittee over the course of this Congress.

He leaves large shoes to fill. And I would like to recognize his incredible work, especially on behalf of his constituents in Ohio after the tragic events in East Palestine.

I am honored to follow his example and I thank Chair Johnson for impressing me with his new role. As you all know I represent the entire coast of Georgia, over 100 miles of pristine coastline and I believe Georgia's 1st Congressional District offers a unique perspective on the issues before this Subcommittee.

We have abundant natural beauty that people come from around the world to see, but it coexists with a growing manufacturing base, including the mining and production of

the critical materials necessary for our modern-day life.

I believe it is an excellent example of how we can protect our environment and human health while pursuing economic growth and prosperity that our constituents deserve. I look forward to working with all of the members of this Subcommittee on the important issues before us like the one we are here to discuss today.

Water is the most essential compound on Earth. Without clean supplies of potable water and systems to treat wastewater, our lives, our economy, and our communities would cease.

We know this and so do our adversaries. China, Russia, Iran, and their proxies are constantly looking for ways to disrupt our critical infrastructure. Recent cybersecurity attacks on the water sector by Iranian hackers reminded us of this.

Luckily, these attacks did not impact the safety of our water supplies. We must learn from these attacks and enhance the cybersecurity of our water sector assets. There are just 50,000 community water systems and more than 16,000 publicly owned wastewater treatment systems in the United States.

Today we will hear testimony from organizations representing all sizes and demographics of our counties water infrastructure. We will also hear from the state agencies that have a front row seat to their work and help these utilities fulfill their essential mission.

As a former mayor, former City Council member, and a Planning Commission member of a small rural community, I understand that constraints facing many of our country's water systems and the collaboration that must be fostered to help them achieve their mission.

The water sector frequently operates on legacy technology systems and small systems regularly lack the financial resources to hire cybersecurity staff. Water utilities are also facing generational challenges.

The average age of a water system operator in the United States is 57 years old. These are individuals who did not grow up using computers and operating cybersecurity systems. Because of these circumstances, we must meet these systems and their operators where they are and build on the cybersecurity efforts already occurring in the sector.

Big American companies are working with non-profits to

pilot cybersecurity programs to coach operators on cyberhygiene practices to protect these systems.

The Water Information Sharing and Analysis Center, a non-profit managed by the water sector, serves over 3,000 water personnel and provides essential two-way communications between the sector and their governmental partners on cyberthreats.

Rather than responding to these cybersecurity threats with one size fits all regulatory standards that are costly and require and assume a level of technological sophistication to operate and maintain.

We must focus on ways to increase cybersecurity collaboration within the water sector and opportunities for the Environmental Protection Agency and Department of Homeland Security to work jointly with these systems.

The water sector is a willing partner in this endeavor and why wouldn't they be? Water systems have an inherent interest in defending themselves from cyberthreats and protecting the safety of the water for their customers.

They do not need Washington agencies to remind them of this. What they need is the technical knowledge and

resources that help them protect themselves. Cyberthreats are not disappearing and no amount of regulation, resources, or technical expertise can fully remove the threat.

However, by meeting the sector where it is and fostering an environment of collaboration, the sectors cybersecurity resilience can be greatly enhanced.

I look forward to hearing from our witnesses about the diversity of our nation's water systems and opportunities to enhance the cybersecurity of the sector. Thank you for participating in today's hearings.

At this time, I now recognize the gentleman from New York, Representative Tonko for five minutes for an opening statement.

[The prepared statement of Mr. Carter follows:]

**********COMMITTEE INSERT**********

STATEMENT OF HON. PAUL TONKO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

*Mr. Tonko. Thank you, Chairman Carter. That sounds good. Congratulations, sir.

*Mr. Carter. Thank you.

*Mr. Tonko. I do share your sentiments about Chairman Johnson. I appreciated the working relationship we had in leading this Subcommittee and look forward to a similar outcome here.

I want to start by congratulating you for taking on the leadership of the Subcommittee. I do appreciate that both you and I have experience with local and state government, whether it is addressing water infrastructure, remediating brown fields, or improving recycling system, so many issues handled by this Subcommittee require us to solve national problems that have incredibly local impacts.

Our nation's local governments are going to benefit from having a former mayor at the helm of this Subcommittee and I hope that today is the start of a great productive partnership.

So I do indeed look forward to working with you Chairman Carter.

The issue before us today is an opportunity to better understand one of these emerging challenges being faced by our local communities. And I do believe it should be in an area with some bipartisan agreement.

For example, I believe we will agree that EPA, with its knowledge of the water sector, the technical expertise, was rightfully designated as the sector risk management agency for water systems and should take the leading role in guiding the sector's response to emerging threats, including those from cyberattacks.

In the past, members of this Committee have worked across the aisle to acknowledge the increasing number and types of threats facing our nation's water systems and to make new resources available to reduce vulnerabilities.

In the America's Water Infrastructure Act of 2018, we required systems serving more than 3,300 people to assess risks and prepare emergency response plans. And the Infrastructure Investments and Jobs Act included several programs to support water systems by providing technical and

financial assistant to enhance resilience.

Water utilities in states as co-regulators with EPA have an awesome responsibility to deliver safe and reliable water services to Americans. This is absolutely critical to our economy and to our public health and we know there's a long and ever-growing list of threats to our drinking water.

Certainly cyberattacks are becoming more frequent and this is an area that deserves our attention. So I am grateful we are holding this hearing and I thank our witnesses for being here.

I also understand this is an incredibly challenging issue. There is not an easy solution. We can spend endless amounts of money and we will never achieve zero cyber risk. And I know small systems, including those in upstate New York that I represent are already stretched thin.

There are some small villages where the mayor's job description also includes fixing the water system and driving the snow plow. These communities can have a very difficult time recruiting and retaining engineers and certified system operators.

It is just not realistic to expect that they will have

sophisticated, in-house cybersecurity expertise. That is why partnerships matter. The EPA, state, circuit riders, and others must play an important role in supporting these systems with the implementation of the achievable, but also meaningful cybersecurity best practices, but to date, it seems there has been a slow and inconsistent adoption of such practices.

So while I am realistic and do not believe we should expect every small system to have cybersecurity departments, I do believe that it is reasonable for some simple, effective, and cost-effective best practices to be implemented.

Hopefully, with EPA and Congress's support we can reduce risk in ways that are proven, rapidly respond to emerging threats, and are deployable by even the smallest of systems, and I agree with what I believe we will hear from all of our witnesses that additional resources, including for training and technical assistance, are indeed warranted.

We can find effective ways to improve cybersecurity that acknowledges the challenges faced by so many water systems and I hope that utilities, state regulators, EPA, and members

on both sides of the aisle will work towards solutions to reduce risk from cyberthreats.

So I thank you, Mr. Chair, and with that, I yield back.

[The prepared statement of Mr. Tonko follows:]

**********COMMITTEE INSERT**********

*Mr. Carter. I now recognize the Chair of the full Committee, Chair Rodgers, for five minutes for an opening statement.

STATEMENT OF HON. CATHY MCMORRIS RODGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

*The Chairwoman. Good afternoon, everyone. To my colleagues, the witnesses, and to Chairman Buddy Carter, I look forward to working with you as you lead this Subcommittee.

Every day more and more of our economy and way of life moves online. Our financial health, public utilities, and energy systems are increasingly being operated electronically.

That includes our public drinking water systems. This shift has significantly enhanced the efficiency of these systems. It has improved water quality, reduced unnecessary expenses, and helped get this vital resource to more Americans.

As our technology becomes more advanced though, these systems will more likely move online more and more, making them increasingly vulnerable to cyberattacks by adversaries and other bad actors wishing to do us harm.

It is vital that we take steps to safeguard this key

infrastructure from future cyberthreats and work with utility companies and others to mitigate those risks.

Cybercriminals are estimated to have made nearly $8 trillion in 2023. A number that's expected to rise to 10 and a half trillion by next year.

Recent attacks on American drinking water delivery systems by Iranian cyber criminals underscores the need for strengthening their cybersecurity. The targeting of this critical infrastructure puts both public health and our economy in jeopardy.

The cybersecurity risk to these systems are expected to become increasingly frequent and complex. From ransomware threats where a bad actor's attack compromises internal administrative information, like customer's personal information, to criminals potentially gaining control of a drinking water system in order to compromise the quality of the water being sent out to customers.

The implications of these attacks go far beyond our water systems. Compromising them could prevent doctors from carrying out medical procedures at hospitals, disrupt the delivery of electricity, or shut down altogether emergency

services like firefighting operations. These outcomes are not acceptable.

Today, we will have an opportunity to hear from experienced and well positioned stakeholders in order to better understand the threats, as well as how we can most effectively address them.

It is important that we strike the right balance for local utilities as they take steps to improve the cyber resiliency of their facilities, including ensuring the federal government isn't getting in the way of those efforts to make progress.

Current law mandates that every five years drinking water systems, serving more than 3,300 people assess their vulnerabilities to attacks and that they incorporate the findings of these assessments into their emergency response plans.

This ensures water facility operators are better prepared to mitigate threats, while also protecting them from cumbersome and ill-suited regulations that could hinder their ability to quickly respond when threats do arise.

While there's always room for improvement, granting the

federal government sweeping cybersecurity authorities over this sector, as some have suggested, I believe may do more harm than good. A one size fits all approach for the 50,000 unique drinking water utilities around the country is unworkable.

And the federal rulemaking process is problematic. Is protracted and cumbersome. It fails to foster collaboration and it advertises to adversaries the very systems intruders will need to target with cyberattacks.

Federal agencies play an important role in the overall cyber resiliency of our water systems and the Environmental Protection Agency, as the federal expert in drinking and wastewater, is the one best suited to serve as the lead in managing risk in the sector.

EPA and others play important roles, whether that's facilitating education and outreach with operators or providing technical assistance, that said, the EPA should not be in the business of micromanaging water utilities or dictating how they maintain and operate their online systems.

Today's conversation will be an opportunity to explore the non-regulatory resources that the EPA and others already

offer to the water sector, like WaterISAC, which is an all-threats information sharing source for water utilities, or the Cyber Readiness Institute, which works with companies to empower small water systems with free tools and resources to help them to become more secure and resilient.

Resources like these can help water systems without the in-house expertise better _ help the water systems that do not have the in-hours expertise better implement cyber practices.

In order to protect people and this critical infrastructure, we must ensure water facility operators are able to innovate and adapt to evolving cyberthreats and protect the systems they oversee.

I look forward to today's hearing and discussing how we will enhance our cybersecurity to protect this infrastructure, which is so vital for the livelihoods of American people.

I yield back.

[The prepared statement of Mrs. Rodgers follows:]

353 **********COMMITTEE INSERT**********

*Mr. Carter. The gentlelady yields.

The Chair now recognizes the gentleman from New York, Representative Pallone, for five minutes for an opening statement.

STATEMENT OF HON. FRANK PALLONE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

*Mr. Pallone. Hi. I wanted to begin by welcoming our new Environment Subcommittee Chair, Representative Carter. I am pleased we are beginning your tenure with a bipartisan issue and I hope that we can continue that approach with other environmental issues where a bipartisan consensus might be possible and I look forward with you.

I mean, we have been working together for years, so I don't even know what I am talking about. You are great. And congratulations on your new leadership role.

Oh, you said I was from New York?

*Mr. Carter. I said New Jersey, didn't I?

*Mr. Pallone. Oh, I don't know. I didn't even hear it. Well, you're from Savannah and I am _

*Mr. Carter. It's one of those progressive things.

*Mr. Pallone. All right. Well, you're from Savannah and I'm from New Jersey. We'll leave it at that. All right.

Today _ oh, Yvette says _ all right. Well, you're from Brooklyn actually. Okay.

Today this Subcommittee continues our important bipartisan oversight of cybersecurity and protecting our nation's critical infrastructure from cyberattacks, specifically, we'll take a closer examination of the water sector and how we can best equip water systems and the EPA with the resources and tools needed to assess and mitigate risk from cyberattacks.

Major cyberattacks have become more frequent and more sophisticated, putting our nation's critical infrastructure at risk. This is especially true for cyber incidents targeting our drinking water and wastewater systems.

In fact, the water sector is classified as a national critical function because a disruption to water systems can have a devastating impact on the health, security, and safety of communities.

A disruption can also greatly impair the various other critical infrastructure sectors that depend on water, such as the energy and healthcare sectors.

And cyberattackers have targeted US water systems of every size in every corner in our country. An attack on a Maine based water utility in 2021 used ransomware to target

internet facing operational technology forcing the utility to revert to manual control of critical processes.

Later that year, an attack on a California based water utility utilized ransomware that went undetected for a month. And more recently an Iran-linked group called Cyber Avengers targeted Israeli made equipment at water facilities across several states, including Pennsylvania and Texas.

Now, much of our nation's critical infrastructure relies on unique systems and specialized workforces and the water sector is no exception. There are over 150,000 public water systems across the nation that range in size from serving less than 500 customers to millions and over 90 percent of water systems are small, which can being unique managerial, financial, and operational challenges as they strive to deliver safe drinking water to their customers.

So lack of capacity and resources at these water systems adds further challenges.

So that's why our Committee's bipartisan efforts to bolster cybersecurity for the water sector is so important. We work together on the bipartisan America's Water Infrastructure Act of 2018, and this law requires water

systems to complete risk assessments and develop emergency response plans that account for risk, including cybersecurity.

This was an important step, but there still are gaps in the ability of federal agencies and water systems to prevent potential cyberattacks, and I hope that we can continue our history of bipartisan cooperation to assess and address these gaps as quickly as possible.

I strongly believe that EPA is best equipped to handle cybersecurity concerns for the water sector. EPA has the institutional knowledge and expertise to engage with water systems and other federal partners to adjust complex sector-specific threats.

Currently, EPA provides technical assistance, education, and resources to help water systems bolster cyber protections. And last Congress we authorized and reauthorized several grant programs to help water systems address their vulnerabilities as part of the bipartisan Infrastructure Law.

This Committee has to ensure the EPA has the necessary tools and can leverage sector-specific expertise and

institutional knowledge to adequately prevent and respond to cybersecurity concerns.

With bipartisan congressional support, EPA can continue to develop more efficient and robust cybersecurity defenses while also partnering with the private sector and other federal agencies.

I just wanted to say, finally, I would like to submit a letter from Representative Deluzio of Pennsylvania. The water utility in his district was one of the systems targeted by the Iran-backed cybergroup and he wanted to share his experience about that incident with the Committee.

So I would ask unanimous consent, Mr. Chairman, to enter that letter in.

*Mr. Carter. Without objection.

*Mr. Pallone. And with that, thank you again, and looking forward to many hearings and markups with you as the Chair.

*Mr. Carter. Thank you.

*Mr. Pallone. Thank you.

*Mr. Carter. Thank you. The gentleman yields.

[The prepared statement of Mr. Pallone follows:]

**********COMMITTEE INSERT**********

*Mr. Carter. Now, for our witnesses, I thank all of you for being here. We are looking forward to this.

First of all, Ms. Cathy Tucker-Vogel who is the public water supply section chief at the Kansas Department of Health and Environment. Thank you for being here.

Mr. Scott Dewhirst, the superintendent and the chief operating officer with Tacoma Water. My good friend, former Georgia State Senate colleague and part-time resident in Saint Simons Island, Mr. Rick Jeffares, who is the president of the Georgia Rural Water Association. Thank you, Rick, for being here.

And Dr. Kevin Morley, the manager of Federal Relations with the American Waterworks Association. Thank you for being here.

Ms. Tucker-Vogel, you are recognized for five minutes for your opening statement.

STATEMENT OF CATHY TUCKER-VOGEL, PUBLIC WATER SUPPLY SECTION CHIEF, KANSAS DEPARTMENT OF HEALTH AND ENVIRONMENT ON BEHALF OF THE ASSOCIATION OF STATE DRINKING WATER ADMINISTRATORS

*Ms. Tucker-Vogel. Thank you. Good afternoon, Chairman Carter, Ranking Member Tonko, and members of the Subcommittee.

My name is Cathy Tucker-Vogel and I'm a past president of the Association of State Drinking Water Administrators whose 57 members represent the 50 state drinking water programs, the five territorial programs, the Navajo Nation, and the District of Columbia.

ASDWA's members work on the frontlines every day to protect public health through implementation of the Safe Drinking Water Act. I also served on the State EPA Water Sector Cybersecurity Workgroup that provided advice on EPA's 2023 Cybersecurity Memo and testified previously, before this Committee, in February of 2020, on the lead and copper rule.

I am the Drinking Water Administrator for the state of Kansas, where I've worked for over 30 years. I direct statewide programs that implement the Safe Drinking Water Act

through regulatory oversight of 972 public water supply systems and approximately 2,000 water operators.

I thank you for this opportunity to provide ASDWA's perspective on effective and efficient cybersecurity activities for the water sector. Provision of safe drinking water is critical for public health protection, economic growth, and stability.

Robust water systems, cybersecurity is essential, however, cyber risks must be treated differently than conventional contamination or hard infrastructure vulnerabilities.

Kansas has developed a program that helps ensure public water supply systems are taking the actions necessary to defend against cyberattacks. Last week we started our statewide training, in partnership with the Kansas Information Security Office and the Cybersecurity and Infrastructure Security Agency.

Through this partnership, Kansas water operators will complete cyber assessments and have access to assistance from cyber assessment experts at CISA and KISO to address vulnerabilities identified in their assessments.

I'd like to highlight four themes this afternoon for this Subcommittee to consider.

First, water utility cybersecurity is critical for providing safe drinking water and protecting public health. Therefore, solutions to improve the cybersecurity profile of the water sector must incorporate both assessments and corrective actions, which will require new funding sources at both the state and local levels.

Second, states must play a role in future cybersecurity approaches. Several states are currently using a variety of approaches, both regulatory and non-regulatory to improve cybersecurity, and any federal actions should incorporate the lessons we've learned from the state experiences and harmonize with ongoing state and local activities.

Third, federal actions on cybersecurity in the water section sector must take feasibility into account. EPA's recently withdrawn memorandum highlighted significant gaps within the water sectors ability to address cybersecurity, such as a lack of sufficient funding for both states and local water systems, the need for subject matter experts to assist drinking water programs and public water supply

systems, a lack of understanding that the frequency of assessments must align with the ever evolving nature of cyberthreats, and the lack of sufficient authorities in many states to protect sensitive data that would present a cyber risk if made public.

And fourth, future federal actions on cybersecurity must be developed in collaboration with state primacy agencies. Cybersecurity cannot be resolved the traditional Safe Drinking Water Act regulatory process, which focuses on water quality through establishment of maximum contaminate levels or treatment techniques. We must seek new approaches.

In closing, ASDWA's members are working hard to improve cybersecurity using a variety of approaches. Many water systems have made substantial progress on this issue, but more is needed.

A new cybersecurity awareness campaign for the water sector soon and ASDWA will play a significant role in that effort. We look forward to keeping Congress informed of the water sector's collective process and ongoing needs.

Thank you, Chairman Carter, and Ranking Member Tonko, and members of the Subcommittee for this opportunity to

appear before you today.

[The prepared statement of Ms. Tucker-Vogel follows:]

**********COMMITTEE INSERT**********

*Mr. Carter. Thank you, Ms. Tucker-Vogel.

Mr. Dewhirst, you are recognized for your opening statement.

STATEMENT OF SCOTT DEWHIRST, P.E., SUPERINTENDENT AND CHIEF OPERATING OFFICER, TACOMA WATER ON BEHALF OF THE ASSOCIATION OF METROPOLITAN WATER AGENCIES

*Mr. Dewhirst. Thank you, Chairman Carter, Ranking Member Tonko, and members of the Committee. Thank you for the opportunity to be here today to testify.

I am Scott Dewhirst. I am the superintendent of Tacoma Water, a division of Tacoma Public Utilities. We provide direct drinking water service to over 350,000 residents in the Pierce County and King County areas of Washington state, the other Washington, as we call it.

And about half of million or more when you include wholesale connections and partners that we have. So I also serve on the Board of Directors for the Association of Metropolitan Water Agencies or AMWA, which represents the largest publicly owned drinking water systems in America. And I also a member of the Board of Governors for WaterISAC, the Water Information Sharing and Analysis Center.

WaterISAC is the water sector's dedicated information sharing entity on cyber, physical, and natural threats.

So we all know that drinking water systems represent attractive targets for cyber adversaries and a successful attack can not only threaten water quality and public health, but also undermine American's confidence in their drinking water systems.

This is why AMWA believes that there must be a level of rigor and accountability to encourage the adoption of cyber best practices appropriate for a given water system's size and risk profile.

As a large municipal utility provider, Tacoma Public Utilities prioritizes maintaining cybersecurity best practices to minimize vulnerabilities for our water and electric systems.

We employ a dedicated cybersecurity staff and leverage resources offered by federal and sector partners, like the EPA, CISA, and the Information Sharing and Analysis Centers for both the water and electric sectors.

As the Subcommittee surveys the current landscape and explores ways to help water systems improve their cyber posture, AMWA has several suggestions.

First, we believe that EPA should remain the sector risk

management agency for the water and wastewater system sector. While AMWA disagreed with EPA's since withdrawn 2023 interpretive memorandum to add cybersecurity reviews to public water system sanitary surveys, we value the relationship that the agency has with members of the sector and believe that lays the groundwork for effective collaboration to counter cyberthreats.

Second, AMWA also believes meaningful progress on cyber preparedness can be made by expanding access to existing resources like WaterISAC, which provides member utilities information on threats, vulnerabilities, and response actions related to cybersecurity, as well as physical and natural based risks.

But as a non-profit entity, with no direct federal funding, the reach of WaterISAC is limited. AMWA is eager to work with the EPA to connect more of the nation's 50,000 community water systems to the service and we support legislation introduced by Congresswoman Jan Schakowsky that would help achieve this objective.

Congress should also fund existing EPA programs that can be used to help water systems counter cyberthreats like the

Mid-size and Large Drinking Water System Infrastructure Resilience to Sustainability Program and the Drinking Water Infrastructure Risk and Resilience Program.

With sufficient funding, both programs can work hand-in-hand to provide critical assistance to water systems. Finally, we should leverage existing resources and incentivize water systems to adopt appropriate cybersecurity best practices.

Earlier this month, EPA, CISA, and other federal partners collaborated with the water sector to release the Incident Response Guide for the water and wastewater system sector.

The Guide provides information about federal support available to water and wastewater systems throughout the incident response process and offers measures that drinking water and wastewater systems may adopt to improve their cyber posture.

But we currently have no mechanism to ensure water systems take appropriate actions. One potential model for accountability in the water sector can be found in the electric industry.

The North American Electric Reliability Corporation or NERC manages electric sector reliability standards that were developed by electric leaders with oversight from the Department of Energy and ensures that individual electric utilities meet all appropriate requirements.

While there are many key differences between the bulk power and water sectors, it is worth exploring whether a similar sector-led approach to the development of appropriate cyber best practices could be replicated in the water utility community.

As the Subcommittee contemplates the best approach for the water sector, it is critical to include stakeholders at the table. Any path forward should reflect a risk-based approach guided by water sector experts and focused on clear objectives rather than prescriptive one-size fits all mandates.

AMWA would welcome the opportunity to participate in any discussions with the Subcommittee to pursue these or other strategies to build water systems resilience to cyberthreats.

Again, thank you for the opportunity to testify before the Subcommittee today. My full statement has been submitted

for the record and I'm happy to answer any questions. Thank you.

[The prepared statement of Mr. Dewhirst follows:]

**********COMMITTEE INSERT**********

*Mr. Carter. Thank you, Mr. Dewhirst.

Mr. Jeffares, you are recognized for your opening statement.

STATEMENT OF RICK JEFFARES, PRESIDENT, GEORGIA RURAL WATER ASSOCIATION ON BEHALF OF THE NATIONAL RURAL WATER ASSOCIATION

*Mr. Jeffares. Thank you, Chairman Carter, Madame Chairwoman Rodgers, Vice Chair Joyce, Ranking Member Tonko, and members of the Committee.

It is an honor to testify before you today on this timely and important topic. I am Rick Jeffares. I am president of Georgia Rural Water Association and I am here on behalf of the National Rural Water Association.

NRWA represents over 30,000 water and wastewater utilities across the country. Georgia Rural Water Association has over 2,100 members, representing over 2,400 permitted systems. That's over a population of over 10 million people.

Small rural systems serving less than 10,000 people make up approximately 93 percent of those systems. I currently support and operate and manage over 90 small rural utilities throughout Georgia and six, Mr. Chairman, are in your district.

I also own four operating systems that serve over 500

people. Small and rural communities have the very important responsibility of complying with the Safe Drinking Water Act and the Clean Water Act regulations and for supplying the public with safe drinking water.

Over 91 percent of the approximate 50,000 community water systems in this country serve less than 10,000 people. Small and rural communities often have difficulty complying with a complicated federal mandates and providing safe, affordable drinking water and sanitation due to limited economies of scale and lack of technical expertise.

This difficulty is eased because of the ongoing support offered through rural water's training and technical assisted programs. As this Committee addresses cybersecurity protection for America and their drinking water systems, I have three suggestions from the small utility perspective.

A path forward must include working with the water sector in a good faith effort to achieve practical safeguards and solutions. With approximately 50,000 community water systems in this country, to adequately address an effort to this scale will require industry participation at all levels, urban and rural, and with our federal partners.

Any additional or existing technical assistance provided by Congress through EPA to address this issue should be carefully drafted to ensure anticipated outcomes are feasible, including third-party non-profits that are selected for funding, have qualified and experienced personnel that possess cyber expertise combined with the practical knowledge of how a local water system works.

Cybersecurity of our water infrastructure must be a shared responsibility. Vendors that have the benefit to receive federal dollars that sell or install automated equipment should be required, by standard protocols established by EPA and from other agencies, to better protect water utilities from cyberattacks.

Any federal government policy for cybersecurity must treat small and large communities very different while recognizing the fundamental differences in the complexity of the water system, financial resources, and technical capabilities.

It is certainly not one size fits all. Remember for small towns in Georgia, a $5,000 is a significant expenditure. When I started my career in 1982, and the

Chairman mentioned it earlier that the average age is 58, I'm 59.

In rural Georgia computers didn't exist when I was in this. We had no data systems. There was no cell phones. There was no remote access. Let's just say it was easier to operate a water system back in those days.

And that reality is, as you mentioned, 58 years old. That's the reason we've got to get out. We've got to train people. We've got to get the young people involved in this field. Rural water had been doing this through a registered apprenticeship program and it's working. So we would like to expand that.

We anticipate the next generation of water operators will have a higher level of computer and cyber sophistication than I possess, but in the meantime, we all need to continue to be proactive in implementing basic cybersecurity measures.

In summary, National Rural Water is an active participant in the cybersecurity arena. For many years, Rural Water has invited EPA officials, cybersecurity experts to any and all of our national and state conferences.

As a matter of fact, Mr. Chairman, this year our

(inaudible) will meet this fall in Savannah, Georgia, you'll have everybody. And we will have people on the agenda that will be talking cybersecurity and these things.

Despite the overarching challenges, cybersecurity threats of the present, all responsibility for providing safe, clean, and affordable drinking water and wastewater services does not change.

We stand ready to continue providing industry leading training and technical assistance as we work together to secure this water sector.

Thank you for this opportunity to participate in today's hearing. I stand ready to answer any questions.

[The prepared statement of Rick Jeffares follows:]

**********COMMITTEE INSERT**********

*Mr. Carter. Thank you, sir.

Dr. Kevin Morley, you are recognized for your five minutes.

STATEMENT OF DR. KEVIN MORLEY, Ph.D., MANAGER-FEDERAL RELATIONS, AMERICAN WATER WORKS ASSOCIATION

*Dr. Morley. Thank you, sir. Good afternoon, Chair Carter, Ranking Member Tonko, Chair Rodgers, Ranking Member Pallone, and members of the Subcommittee.

My name is Kevin Morley. I'm the Federal Relations Manager for the American Water Works Association. I appreciate this invitation to share what we believe are opportunities to improve cybersecurity in the water sector.

AWWA is firmly committed to advancing the security and preparedness of water systems. Our standards, manuals, and trainings are designed to provide a foundation for an effective all-hazards risk management approach, which includes cybersecurity.

Cybersecurity is a shared responsibility that we believe can be improved by a combination of regulatory and non-regulatory actions.

Water utilities are robust and resilient, but like all other critical infrastructure systems, we are not immune to cyberthreats.

Several incidents led AWWA, in 2021, to assess potential regulatory options, which resulted in a recommendation to establish a new cybersecurity governance framework in the water sector.

This collaborative approach builds on a similar model that has been applied in the electric sector very effectively, with congressional approval.

Our recommended approach would create an independent non-federal entity to lead the development of cybersecurity requirements, leveraging subject matter expertise from the field in the water sector, with federal oversight and approval of requirements that would be provided by the EPA, as the sector risk management agency.

The governance model would use a tier risk-based and performance-based approach that accommodates the differences and operational complexity and maturity of water systems in the sector.

This recommendation aligns with calls for greater public-private collaboration included in the National Cyber Strategy. We believe it is timely and prudent for Congress to work with the sector on this recommendation that ensures

utilities are directly engaged in developing appropriate cybersecurity requirements, with oversight from EPA, to create a robust cybersecurity risk management paradigm in the water sector.

In addition, it is critical to recognize the non-regulatory opportunities, which there are many, to advance cybersecurity in the water sector. We should collaborate like we did following 9/11 where EPA supported an aggressive degree of training provided by trusted partners, like AWWA, to address new national security risks facing drinking water systems.

In that regard or in that context, we should begin with the following. One, launch of collaborative campaign to expedite enrollment in CISA's vulnerability scanning service to help utilities address threat exposure. This is a highly valuable service for systems with limited in-house resources to provide timely information on exposures and recommended mitigations.

Two, invest in capacity development to empower utility owner/operators to effectively engage the cybersecurity issue. For example, we believe AWWA's small systems

guidance, developed with support from USDA, provides a very robust getting started guide that is focused on six key domains from the NIST Cybersecurity Framework.

This type of capacity engagement delivered by trusted partners, is a force multiplier in delivering the awareness and knowledge utilities need to grapple with evolving cyberthreats.

Further, we support the initiative recommended by the National Rural Water Association to deploy cybersecurity specialists to help rural water systems that often lack the resources and in-house expertise to implement cybersecurity best practices.

As noted in other comments, funding that prioritizes technology upgrades to address what I would call a digital divide that is difficult to overcome, especially in small systems, given cost and complexity.

Many of these legacy operational technologies simply cannot operate on the newer enterprise platforms that advance at a much quicker rate. In many instances, this would require a rip and replace project that are capital intensive and can take several years to complete.

These technologies and those providers need to be secure by design, as discussed by CISA, as they support the critical infrastructure sector that may have unknown vulnerabilities that put us at risk.

Improving threat information sharing. We recommend that CISA and EPA work with partners, like the WaterISAC and the Sector Coordinating Council to establish a standard operating procedure for the inclusion of SMEs in the development of threat alerts and advisories to ensure that the information transmitted is concise, actionable, and properly contextualized.

Last, research and development can also play an important role in supporting the sector. The Water Security Testbed operated by Idaho National Labs and EPA provides a platform to evaluate cyber intrusion scenarios that, if properly supported, can provide realistic mitigations for utilities.

To conclude, there are ample opportunities to collaborate on multiple fronts to address cyberthreats facing the water sector. AWWA is ready and willing to work closely with federal partners, including Congress, to provide

actionable solutions that address the needs of the water sector.

[The prepared statement by Dr. Kevin Morley follows:]

**********COMMITTEE INSERT**********

*Mr. Carter. Thank you, Dr. Morley.

Okay. We will now begin questioning and I recognize myself for five minutes.

Ladies and gentleman, recent cyberattacks on the water sector have exposed concerning cybersecurity vulnerabilities. As Congress examines what occurred and the best steps to improve resilience to threats, I believe we must work collaboratively with the sector to accommodate the diversity of our nation's water systems.

I believe if there was one common theme throughout all of your speeches, it was collaboration and we all recognize that is extremely important.

Mr. Jeffares, I will start with you. Can you please discuss the various cybersecurity challenges facing our rural water systems? And then I'm going to ask Mr. Dewhirst for his on the large systems.

*Mr. Jeffares. Thank you, Mr. Chairman.

As I mentioned earlier, I look after 90 rural systems and only one has any connection to the internet. These are still systems. They get in the truck in the morning. They ride out. They look and they see the water tanks half empty,

they go turn the well on.

They don't even have telemetry systems. That's probably 80 percent of your systems were talking about. A lot of the telemetry systems radio read, so it's not connected to the internet.

So as far as rural goes, when we're talking about the less than 3,300 and most of them, or less than 1,000, when you get down and look at it, it's not as big a concern to us. I worry more about a physical attack, where somebody dumps something on me, than I do cybersecurity.

Not meaning that that's not true for Atlanta, Macon, Columbus, the bigger systems. But rural? It's just not, you know, what we were talking earlier.

When we do the vulnerability assessment, you know, the 3,300 and more, a little system like I run, you could probably do a vulnerability assessment that's half a page of just a checklist.

Are you looking at these things? But there's just a huge difference when you're trying to compare water systems.

*Mr. Carter. Right. Thank you for that.

*Mr. Jeffares. Thank you.

*Mr. Carter. Mr. Dewhirst, building on what Mr. Jeffares said, can you contrast that with the cybersecurity challenges facing large systems?

*Mr. Dewhirst. Sure. So obviously, we feel like we have a, I'm not saying a bigger target, but we have _ there is more impact if a bigger system is attacked and successfully implemented.

So we benefit in Tacoma from having a power utility that's very cybersecure, given that the NERC requirements that they have to face. So we have a number of cyber tools that we utilize, at that level, to detect.

Really, the biggest thing we're doing with most of our cyber posture is endpoint detection. We're always checking to see who has talked to our system and for how long and we're logging all those things and we're verifying when things are not normal.

For instance, last time I was in Washington, D.C. back in December, I logged into our network and I got a chat about within an hour that said, hey, we detected a login from Virginia, is that you? Again, just to verify that it was indeed me and it was not someone acting elsewhere.

We do vulnerability management, so we're scanning our systems on a regular basis. We scan daily and patch weekly. So this is the standard practice we use. We also have other tools that create like a protocol break between our systems so that, in essence, there's like an air gap between our system and what it looks we're interacting with and what we're actually touching.

Most of our, if not all of our, control systems are not on the internet. So they are network isolated. So there are ways to network isolate some of these things so that they're not really accessible to the outside world.

And then I would say that two, because of water and the internet _ the difference between water and power, just to give you a little bit on that. We are a lot less interconnected than power is.

Power generally, with generators and also the balancing authorities. They have a lot communications going back and forth across. Water systems are a little bit different because we are kind of our own grid.

We're not trying to manage a grid collectively. We have our own grids. That's what a water system essentially is to

ourselves. So if that addresses the question. Thank you.

*Mr. Carter. Great. Thank you. Thank you.

Our country's systems are incredibly diverse and face numerous challenges. We recognize that. I have concerns that a one size fits all regulatory proposal from EPA to address cyberthreats would not necessarily be the best way to accommodate these differing circumstances.

Dr. Morley, you represent water systems of all sizes and in your opinion, do you support a purely regulatory response to addressing cybersecurity?

*Dr. Morley. Mr. Chairman, I believe this requires a combination of activities that are in part regulatory and non-regulatory, as I discussed before.

We have outlined a possibility of what we believe is a reasonable regulatory approach that addresses that diversity and complexity of the operations, but as I said, and my colleagues have said, there are a number of opportunities that we can force multiply to empower utilities to take directed action on implementing this best practice.

*Mr. Carter. So if it were purely a regulatory proposal, could it make it worse?

*Dr. Morley. Well, that's a possibility. That's always a possibility. Yeah.

*Mr. Carter. Good. Well, thank you all. My time is up.

At this time I'm going to recognize the gentleman from New York, Mr. Tonka, for five minutes.

*Mr. Tonko. Thank you, Mr. Chair.

Sophisticated cybersecurity can require expertise that can be difficult to develop and I heard some common themes from our witnesses that additional resources would and could be necessary.

But I do not want it to be suggested that EPA has not been doing anything. This is a fact sheet from EPA that describes funding opportunities, technical assistance, training efforts, and the agency's support for planning, threat briefings, incident response, and others.

It seems EPA has been developing toolkits and assistance that can be provided to water systems, to states, and to technical assistance providers.

I would like to ask all of our witnesses for their assessments of whether the TA and tools being developed by

EPA are meeting the needs of their systems?

So why don't we start with Ms. Tucker-Vogel, please?

*Ms. Tucker-Vogel. So there have been a lot of tools developed. I think the communication on how to best deploy those tools has sometimes been challenging between EPA headquarters, regions, and states.

As I mentioned in my testimony, we've been working very closely with the CISA state coordinator at the state level and our Kansas Information Security Office. And that coordination has been excellent and I think we've got a great path forward.

EPA has developed a lot of tools, however, they're memo, that they sent out last March directing us to take a regulatory approach, that created some challenges for us to, I'll say, trust in using their tools because we believe that states _ this is better implemented at the state level, both through regulatory and non-regulatory approaches.

*Mr. Tonko. Thank you.

Mr. Dewhirst?

*Mr. Dewhirst. Yes. I would just add, I think she answered the question very well, from that standpoint. I

think a lot of times these things are put out that resources are available, but they're not very well advertised or very, you know, almost like you need someone to hold your hand to really understand it.

Depending upon your level of cybersecurity awareness. You know, for someone like our shop, we have dedicated cyber professionals, so they can digest that material very easily. Sometimes that's not always the case.

So I think that's a challenge and you have to go get this material. It's not being pushed to you in many cases.

*Mr. Tonko. Thank you.

Mr. Jeffares? Did I say that correctly?

*Mr. Jeffares. That's correct.

So as an operator, been doing it 42 years, when you get EPA and EPD on the state level involved, your little towns automatically go into uh-oh, we're in trouble. And that's the way they see it.

So I think it take the rural waters, the AWWA, the people they trust, the people that get out every day and do this to come and do, you know, let them set up the tools. Okay, here's what we got. Let us administer it and go from

there.

Let us do the technical assistance because, like I said unfortunately, when they show up at our little systems everybody panics that something bad is fixing to happen.

*Mr. Tonko. Thank you.

Dr. Morley, please?

*Dr. Morley. Yes, sir. What I would say, just to add to that. You know, a trusted partnership is a really critical element that I think could be improved significantly.

AWWA developed guidance and resources specifically on cybersecurity risk management practices based on NIST framework in 2014 and have been out there in the field training systems on this.

We are a non-profit organization. We can only reach so many people. Leveraging support with EPA to have a shared and unified messaged on those best practices would be very effective.

*Mr. Tonko. Thank you.

And would any of you want to comment on how to make certain these tools are fully being taken advantage of?

Anyone?

*Ms. Tucker-Vogel. Could you repeat the question? I didn't quite hear it?

*Mr. Tonko. Yeah. What could be done to make certain these tools are fully being taken advantage of?

*Ms. Tucker-Vogel. So I think making sure that we have two-way communication with EPA at the regional level. A lot of the cyber discussion was occurring at the headquarters level and it wasn't necessarily trickling down through the regions, which, from the state regulatory perspective, that's who we work with most often _

*Mr. Tonko. Okay.

*Ms. Tucker-Vogel. _ are the regional people. So having that pathway gets to us at the local level, I think would be helpful.

*Mr. Tonko. Thank you.

And Mr. Dewhirst and Dr. Morley, how might larger systems share their expertise and services with smaller operators?

*Mr. Dewhirst. I think I'd welcome that opportunity to really explore that further. I think, when I prepared for

this hearing today, I had talked to our folks about that. They would love the opportunity to say we can be that trusted partner.

But again, I think it's Mr. Jeffares talked about it's got to be trust. You know, it's got to be something that they can trust and not looking like we're trying to impose our will on them, but we're here to be a partner with them. And I think that's how it works with the state primacy agencies.

We want to be partners in drinking water quality. So.

*Mr. Tonko. Thank you.

*Dr. Morley. Yeah. We have worked very effectively, since post Katrina, to develop a mutual aid program amongst utilities in almost every single state.

That has provided a very trusted relationship amongst the utilities within that community to information share. Not just to go actually help fix the utility after a disaster, but there has been an extensive amount of information sharing, as it relates to cybersecurity, largely coming from larger systems that may see things sooner than smaller systems.

That's been a very useful process.

*Mr. Tonko. Thank you.

Well, I've exhausted my time and I'm thankful that the Chair, on opening day, has given me a little leeway.

Thank you. I yield back.

*Mr. Carter. Thank you. The gentleman yields.

The Chair now recognizes the Chair of the full committee, Representative McMorris Rodgers from Washington.

*The Chairwoman. Thank you, Mr. Chairman.

And thank you, again, to our witnesses for being here. The stories of cyberattacks on water systems are very concerning. Not because of what they've done, but the potential as to what they could do.

We cannot have our geopolitical enemies threatening the safety of our water supply and the wellbeing of our communities. It's important to understand the extent of the challenges, what solutions make sense, and what type of resources are already available before acting.

So to each on the panel, I just had _ my first question is around what is currently required of you under the Safe Drinking Water Act, Section 1433?

Because some people believe that without more regulation the sector will not do anything to address cybersecurity, but there is a lot that is happening already in the water sector, including mandatory compliance with America's Water Infrastructure Act, Cyber Hygiene, and other assessment tools offered both publicly and privately.

So would you just talk about what's currently required of you?

*Mr. Carter. So under 1433, nothing is required of the state primacy agencies. That is directly from the water system to EPA. So the vulnerability assessments had to be completed and certified to EPA.

Then the Emergency Response Plans that were required to be developed based on those assessments, those certifications went directly to EPA.

So the only role that we played, at the state primacy level agency, is when EPA needed contact information about a particular water system. We provided that information on who to contact at the water system.

But as far as actual engagement, we did not have a lot.

*The Chairwoman. Okay.

*Ms. Tucker-Vogel. Now, I want to add that in Kansas, we're a little bit unique in that we have state regulations that require all community water systems to have an Emergency Response Plan and we review those.

So we have sort of a state control that was outside of the 1433 requirements.

*The Chairwoman. Okay. Thank you.

*Mr. Dewhirst. Yeah. So everything she talked about that they were kind of overseeing, we actually do.

So we actually went through a vulnerability assessment process. We developed, from that, as part of that vulnerability assessment process was inclusive of a look at computer systems.

For that we did engage with our cyber team to really evaluate our systems. They are very accustomed to doing their own audits, as part of their NERC program. So that was something that they kind of did for our system, was actually do like a vulnerability audit to our internal system network.

We also have Incident Response Plans for any penetrations that we would have. And then we have like the Emergency Action Plans. Sort of similar to that. So yes.

*The Chairwoman. Okay. Okay. I'll give the other two a moment, but I do have another question.

*Mr. Jeffares. In Georgia, anything over 3,300 population had to do a vulnerability assessment. We had to do the Emergency Response Plan. We had to certify it. We hoped and what we tried to get out when we were riding around talking to them is that they implement it. Don't just do it, let's hope you implement it so you know what to do in an emergency.

And exactly what they said _

*The Chairwoman. Okay.

*Mr. Jeffares. _ we did, my little systems, we talk about it.

*The Chairwoman. Okay.

*Mr. Jeffares. But there was no assessment done.

*The Chairwoman. Okay. Thank you.

*Dr. Morley. Yes, ma'am. The resources that AWWA has developed, including several ANSI standards are specifically aligned with provisions in 1433. We commend this Committee for expanding the coverage on cybersecurity to be both enterprise and operational technology.

Those resources, that we've provided, do help facilitate the utilities compliance with these provisions, including demonstrating due diligence. And so that's how we've helped _

*The Chairwoman. Okay.

*Dr. Morley. _ try to enable utilities to address the statutory requirements.

*The Chairwoman. Thank you. I also wanted to ask each of you.

So the Inspector General, at Department of Homeland Security recently criticized CISA for poor public outreach when it comes to cybersecurity. And I've heard concerns that EPA outreach and collaboration is also lacking.

Federal regulators are not always transparent, from their level of respect for input from regulated stakeholders. So how important is EPA outreach to the sector to help move the sector towards a better cybersecurity posture?

We'll start with you.

*Ms. Tucker-Vogel. So I think it's very important that the outreach be improved.

*The Chairwoman. Okay.

*Ms. Tucker-Vogel. But I also think it's important that there is two-way communication.

*The Chairwoman. Yes. Okay.

*Ms. Tucker-Vogel. It can't just be one way and just in regards to the IG CISA report. That has not been our experience in Kansas.

*The Chairwoman. Okay. Thank you.

*Ms. Tucker-Vogel. CISA has been _

*The Chairwoman. Okay. Thank you. Okay. Good. I want to give others _

*Ms. Tucker-Vogel. _ outstanding to work with.

*The Chairwoman. _ a minute. And just if there is anything that you would improve?

*Mr. Dewhirst. I don't know if I could add to that.

*The Chairwoman. Okay. Good.

*Mr. Dewhirst. So thank you.

*The Chairwoman. Okay.

*Dr. Morley. I think if more collaborative engagement with the stakeholders to ensure the messaging is on target and we can force multiply, as associations, on that message, would be much improved.

*The Chairwoman. Okay. Very good.

Thank you all. I yield back.

*Mr. Carter. The gentlelady yields.

The Chair now recognizes the Ranking Member of the full committee, the gentleman from New Jersey, Mr. Pallone for five minutes.

*Mr. Pallone. Thank you, Mr. Chairman.

It's vital that we bolster the cybersecurity of critical infrastructure, like the water sector, to ensure the health, stability, safety, and security of our country. And to that end, EPA works directly with the thousands of drinking water and wastewater utility providers to ensure safe clean drinking water for all our communities.

So let me start with Mr. Dewhirst. What are some of the unique challenges facing the water sector when it comes to cybersecurity and how does the water sector differ from other critical infrastructure in this respect?

*Mr. Dewhirst. So I think some of the things and the challenge of the water sector is there's a lot of water systems out there. I think that's a huge challenge. In order to reach and really engage with all the systems that

need to understand some of the basic tools that are even available to them today.

So that, to me, I step number one. You know, number two, we see the threat. We see the attacks that are coming. So we realize that our mission is paramount to provide safe drinking water.

And so none of us want to see this happen. So I think the partnerships that we would like to have with EPA and CISA and the other agencies are critical. And I also think some of the challenges are funding.

And this is a _ we have a lot of stuff coming at us right now, as a utility industry. We have regulations such as lead and copper improvements, PFAS (sic) and the like and it's easy to get distracted from those other tasks or from cyber because these other things are facing us.

*Mr. Pallone. Thank you.

Now, as the sector risk management agency, EPA is the primary federal agency in charge of carrying out specific security and resilience responsibilities for the water sector.

So again, Mr. Dewhirst, how does EPA's institutional

knowledge and sector specific expertise aid in preparing public utilities to counter cybersecurity threats?

*Mr. Dewhirst. I think it's important as we engage in this topic to really make sure that everyone, as we've heard here a few times, collaborates on best solutions. EPA does have a relationship with us, through the primacy agencies, in many cases, and we view one another as partners.

I know oftentimes we think of regulators as, you know, domineering and that sort of thing. I don't think that's how I would paint the picture for you or the public. I think oftentimes it's really a partnership between us and the agencies to _ we want the same thing. We want to provide safe drinking water to our public and to our consumers and we don't want anything to get in the way of that.

So I think the more we can see each other as a partnership, and again, she said have two-way communication, to hear each other, it's important to have them, to me, at the lead because they understand water systems, they understand how we operate, what things we need to have to operate, how the control systems work, how they interface and those sorts of things.

There's some sector knowledge that's really critical to come up with the best solution here.

*Mr. Pallone. And I agree with you and that's why I think that EPA is best suited to handle the cybersecurity efforts of the water sector.

But let me go to Mr. Jeffares. In your testimony you mention the National Rural Water Association support of EPA's Cybersecurity Technical Assistance Program and the Water Cybersecurity Assessment Tool.

Could you just explain the importance of these technical assistance programs and other assistance EPA provides in helping water systems develop strong cyber programs?

*Mr. Jeffares. Yes, sir. As I mentioned earlier today, when we have our state association meetings and when we have national and we're in Savannah, EPA is going to be there to speak. They're going to speak about the cyber. They're going to talk about these things.

What we really need though, is once we figure out what we're doing, give it to us, let us run it from there or a third party, somebody needs, like I mentioned earlier, operators like operators.

They don't like EPA. They don't like the state and they're scared. So I think you got to pass this off to a third party. Let the associations helps get this done. Let's figure out what we need to do and then let us take it from there.

*Mr. Pallone. Well, I appreciate that. I think it's imperative that the EPA continues to lead cybersecurity for the US water sector, as the sector risk management agency, and that's because the agencies extensive sector-specific knowledge and deep understanding of the challenges facing water utilities.

And I think Congress should ensure that EPA has the tools and resources to be effective in their role, especially when it comes to water systems facing a bombing threat. So I want to thank the panel again and thank you, Mr. Chairman. I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the Vice Chair of this committee, the gentleman from Pennsylvania, Dr. Joyce for five minutes.

*Mr. Joyce. First, I want to thank our new Chair,

Chairman Carter, and Ranking Member Tonka for holding today's hearing. And for the witnesses for being here. It's such a critical issue and thank you for addressing that.

Before I came to Washington, I spent my time as a practicing dermatologist and each and every day I would evaluate pigmented lesions, the risk that they pose to patients, and then the subsequent appropriate actions to take.

Whether it needed to be biopsied, whether it needed to be excised, what was the best-case scenario? When I came to Congress, I applied the lessons that I learned in medicine as I spent my first term on the Cybersecurity Subcommittee of the Homeland Security Committee, hearing about the emerging risks to American institutions in the cybersecurity arena.

Unfortunately, today, these are no longer emerging risks. They are representing a clear and present danger. We saw this late last year when the Aliquippa Water Authority, in my home state of Pennsylvania, was hacked by Iran.

Foreign state actors are increasingly willing and able to attack the critical infrastructure that Americans rely on each and every day. Local water authorities are certainly no

exception.

As the son of a city engineer, I know firsthand the challenges that municipal infrastructures can face. My father participated in founding and developing the Altoona Water Authority.

I have seen the diligent work of local officials to keep these often-undercapitalized utilities safe and to keep them reliable for the public good. With unfunded mandates like lead service line replacement and PFAS coming down the pipe, Rural and small-town water utilities are already under significant pressure.

Now, the need to implement significant cybersecurity adds another layer of financial strain to an already overburdened organization. This is a growing problem that I believe Republicans and Democrats can come together on, and I am encouraged to see that our subcommittee is spending time to highlight this issue today.

My first question is for you, Mr. Jeffares. To start us off, can you describe the sort of damage that a cyberattack could cause to a rural or a small-town water utility?

*Mr. Jeffares. As I mentioned earlier, smaller systems,

they usually are not connected to the internet. They don't they do not have any telemetry. Somebody would literally have to come in and do something, which I would say would be a physical attack.

Because earlier, as I mentioned, some of these systems I look after, they ride down the road, look up at the water tank, see the level, go turn the well on, fill it up.

So as far as the ones that I say are less than a 1,000 population, I don't see _ I mean, they may hack city hall. They might get a database from your water customers, that would be about the only thing we would see on the smaller level.

*Mr. Joyce. Ms. Tucker-Vogel, from your experience, do water systems want to become more defensive and more active on cybersecurity?

*Ms. Tucker-Vogel. Yes, they do. And as I mentioned in my testimony, we've started a training program and the feedback that we received last week, and I hear from my staff this week, that water system, water operators are very receptive and they want the training and they want to make sure that they're putting appropriate protections in place.

So there's not a resistance to doing something, it's just they have a lack of understanding of what it is they need to do. And when you start talking cybersecurity, it's almost like a foreign language.

*Mr. Joyce. And are states participating in the training and the technical assistance? Do they provide circuit rider programs to get people more active in taking those necessary steps to be more protected?

*Ms. Tucker-Vogel. Yes. So states take a variety of approaches depending on which state you're in, but we all have the ability to provide some level of technical assistance.

And the example in Kansas. We are actively participating with CISA and with our Kansas information Security Office. So we've brought the water people _

*Mr. Joyce. That's encouraging to hear that active collaborative effort.

*Ms. Tucker-Vogel. Yes.

*Mr. Joyce. Dr. Morley, smaller water systems frequently operate on legacy technology systems due to limited financial resources that are available to have those

ongoing upgrades that are so necessary.

Recent reports indicate that the Chinese hacking group known as Volt Typhoon is targeting legacy computer systems that are used in water utilities because original manufacturers are no longer issuing that those technical updates, leaving an obvious vulnerability.

Can you discuss the prevalence of legacy systems in the water sector, and are there severe cybersecurity vulnerabilities due to those legacy systems?

*Dr. Morley. Yes, sir. So, part of the part of the complexity of that is the operational technologies that automated systems say 15, 20 years ago, right?

They were not designed for the security challenges that we face today. Subsequently, the IT or the enterprise system, say, like Microsoft Windows platform, right? The newer versions of that can't read into the older operational technologies because they haven't been updated.

So there is this kind of digital divide that's evolved, that is complex to transition to. And so we need a combination of support from the technology providers to address secure by design principles in the resources that

utilities use to operate their systems.

At the same time, if we're going to move those forward to newer platforms that's going to require rip and replace.

*Mr. Joyce. Thank you for discussing that vulnerability.

My time has expired, Mr. chairman, and I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the gentlewoman from Illinois, Ms. Schakowsky.

*Ms. Schakowsky. Thank you so much, Mr. Chairman, and thank you to our witnesses.

As I know has been said over and over again, that cyberthreats to our infrastructure are absolutely real, and we have to take steps to make sure that we're doing everything we can to make ourselves safe.

And we must ensure that water systems, in my view, you know, above all, maybe, water systems and the owners and the operators have to make sure that they have access to the latest information about cyberthreats and what to do about it.

One resource that it is available, again, I think that

has been talked about pretty much, has been WaterISAC, and making sure that all of the large and small water systems have availability, that they're able to join and have the resources to join.

And so I that's what I really want to talk about too. Last year, along with Senator Markey, I introduced, legislation that would ask or allow and ask the Environmental Protection Agency to actually offer a grant to some of the smaller systems that may not have enough money to be able to join what is a not-for-profit WaterISAC.

And, I wanted to, ask you, Mr. Dewhirst, if you think this kind of information, and maybe there's others, that need to be available to water systems large and small that this can really make a difference in the outcomes?

*Mr. Dewhirst. Thank you for the question.

Yes. I would definitely agree with your assessment, and thank you for introducing that bill. I think it will make a huge difference.

One of the things that WaterISAC does, and you've heard it mentioned before, it's more than just cyber. It does cyber. It does physical threats. It does natural threats as

well.

So it's trying to really raise the awareness and raise the culture of our industry to all those different things. Also at WaterISAC, there's a number of tools that have been developed.

We have the 15 fundamental cyber tools for all water utilities to be aware of. I think if we could get that more widely known, sort of like we've heard about the EPA documentation has been provided, if we make people aware of it and what it is, I think it can go a long way to implementing some very basic cyber protections that we all need.

And lastly, the thing I think that brings WaterISAC a lot of value is these threats and these bulletins that they assemble, they research and verify what the threats are. They then push that information out.

It's not something people have to go get. People can, once they're part of the system, they get signed up and they can send the email to multiple people in their utility, whoever they want to include on the list is acceptable.

Therefore, they don't have to go looking for

information. It comes to them when they need to, perhaps, look at what's out there and take appropriate action. So thank you.

*Ms. Schakowsky. What are small water systems likely to miss? Not just about cybersecurity, but the things that they could also, in addition, learn from organizations like ISAC?

*Mr. Dewhirst. Well, I can answer that or you can answer that. I'm not sure.

*Ms. Schakowsky. Okay.

*Mr. Dewhirst. You know, maybe you want to take a shot?

*Mr. Jeffares. Sure. So there's a rural water association in every state, and we have circuit riders. We have people go out. As we get, as is when we get these things, we go out and we do one on one training with the systems. They know who to call if they don't know the answer to something.

They know to call us and we'll send somebody down. And, you know, once we come up with the best tools, the best things we can for cybersecurity, you're going to need people that know the water industry, how to run them, and go train all these systems.

I mean, you're going to need a couple of people riding around training. You know, hold something in Savannah. Hold something in Macon. Invite everybody there. Come to our conferences. Let us show you how this works and where we go from here.

*Ms. Schakowsky. Great.

*Mr. Dewhirst. Yeah. I would just add to that if I could?

*Ms. Schakowsky. Sure.

*Mr. Dewhirst. It's those fundamental things that are really simple, you know, that I think a lot of people without have an awareness to it.

When you talk about building a culture of cybersecurity, awareness is like process number one. Everyone needs to understand how can the attacks happen. What are the vectors they can use? How do we maintain our passwords? Do we know what our assets are? What's your inventory of assets that we have that even half connectivity?

So I think there's some basic steps, very foundational, which is why they're called the fundamentals, that WaterISAC has already put forth, and this is updated periodically. So

it was updated, couple years ago and their process updated again now.

So I think that type of insight and forward thinking is essential for everyone to have at all levels.

*Ms. Schakowsky. Well, thank you. And thank you for all of you who weighed in on this. I really appreciate it. We have work to do, but I think it's at hand. We can make it happen.

So thank you, and I yield back.

*Mr. Carter. The gentlelady yields.

The Chair now recognizes my colleague from Georgia, Mr. Allen, for five minutes.

*Mr. Allen. Thank you, Chairman Carter, for holding this important Subcommittee hearing to discuss cybersecurity in our water infrastructure system. I would also like to congratulate you as the new chair of this Subcommittee. I look forward to working with you on these critical issues and your leadership.

I appreciate our witnesses being with us today and our hometown Georgia witness. The 12th District of Georgia is leading the way in cybersecurity and with the Georgia Cyber

Innovation and Training Center located in my home in Augusta and it collaborates between academia, government, and industry stakeholders to educate and train a superior cybersecurity workforce.

Fort Eisenhower is also there in the district, which is home to the US Army Cyber Center of Excellence, and as well as NSA Georgia, the 2nd largest NSA Facility outside of Fort Meade in Maryland.

I am proud of all the cybersecurity assets in my district and state and the work being done in my district to improve cybersecurity and the synergy between these various institutions.

Mr. Jeffares, first off, thank you for all you do to protect water supplies for smaller rural communities in Georgia. Smaller rural water systems constitute a large percentage of our water infrastructure nationally.

Do you feel your concerns and challenges, as a representative of small and rural water infrastructure, are heard here in Washington?

*Mr. Jeffares. I think they are. I mean, we're working through National Rural Water. We're getting to this level.

I mean, I'm here with them today. So I think we are being heard. Maybe it could be a little better.

I mean, that's what I would like to add. So I think we are.

*Mr. Allen. How do you make sure that our rural water systems are not left behind in having the, you know, the challenges that have been brought to our attention today and obviously with the immense resources that we have, that I have just explained, not only there in Georgia, but in our district, that our resources of the federal government and to deal with this cyber issue that we're talking about today?

*Mr. Jeffares. Right. And I've talked mostly about rural. But, you know, there are some middle systems in Georgia, you know, in Fayette County now, they've implemented all the security stuff. I've been knowing those guys for 40 years. They won't let me in the water plan anymore until I go get a background check and hand it to them.

I mean, so they're probably going a little overboard, but if that's what they want to do, let them do it. So, yes, all your _ some of your bigger systems, the Henry Counties, Columbia County, they're implementing this stuff. They're

making sure.

And like I said, Fayette went a little overboard, that's okay. That's their prerogative. So I think the middle systems, you know, the 10,000 to 25,000, and your bigger ones. I'm sure, DeKalb, Gwinnett, they're all taking this very seriously.

*Mr. Allen. Well, I remember what President Bush said after September 11th. He says, we have to be right every time. They only had to be right once. And, so we know that threat is real.

The federal government, whether it be Environmental Protection Agency or the Cybersecurity Infrastructure Security Agency has all of these tools to address this cybersecurity.

In addition, the water sector also has free resources that we talked about earlier in the meeting. Can you share challenges that we are having with the rural water systems face when trying to participate in these programs?

*Mr. Jeffares. I can't speak for every state, but I've been involved with Georgia rural water for a long time. We have a very great workforce. The guys we've hired, they've

all been operators.

We got trainers. I used to teach basic and advanced water treatment back in the '90s. I feel like and it's not just Georgia. I mean, with National Rural Water, we got some great state associations out there.

And there's a few they're probably lacking, but they're getting better. But I think with the help of, like, in Georgia's GAWP, who works with the AWWA, we're getting the word out there, but it just takes time.

I mean, as I mentioned, there's tens of thousands of these little systems out there.

*Mr. Allen. Right. Well, let us know how we can _

*Mr. Jeffares. And so somebody's got to get in a truck and go ride and see them.

*Mr. Allen. Right. Let us know how we can expedite that.

And, Mr. Dewhirst, I have a question for you. I'll submit it. I'm out of time. I'll submit it for the record.

Again, thank you all for being with us. And with that, Mr. Chairman, I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the gentlelady from New York, Representative Clarke for five minutes.

*Ms. Clarke. Good afternoon, everyone, and thank you to, Chairman Carter and Ranking Member Tonko for holding this hearing today.

I also want to thank our witnesses as well for being here today to testify on the importance of cybersecurity for our nation's infrastructure.

As cyberattacks and criminals continue to grow and evolve in size and complexity, now more than ever, it is critical to bolster our cybersecurity as it pertains to our infrastructure.

Water infrastructure affects everyone. Water systems serve millions of customers and gaps in cybersecurity open the door for disastrous effects on the health, security, and well-being of individuals all over the country.

The importance of providing safe water to consumers often occupies the top-of-mind water systems. Since cybersecurity isn't always the most immediate need, it can fall lower on the priority list.

As we work together to bolster cybersecurity in this

sector, we must keep in mind that there's no one size fits all approach. That is why it is essential to create and promote a cyber culture within the utility.

Mr. Dewitt (sic), in your written statement, you referenced a 2021 Cybersecurity State of the Sector Survey conducted by the Water Sector Coordinating Council.

I ask unanimous consent to submit the report into the record.

Thank you, sir. The report found that the number one challenge for systems serving more than 100,000 people or 100,000 is creating a cybersecurity culture within the utility.

Mr. Dewitt (sic), how important is cyber culture to mitigating cyber vulnerabilities at water systems?

*Mr. Dewhirst. I can speak from direct experience. It's, you know, it's very challenging. I alluded to a few minutes ago just the knowledge that people lack in the ways that attacks can occur. Whether it be a USB drive you plug into your computer or various different tools.

So it's a constant training and retraining to educate and to keep the workforce aware of threats and the avenues

that they can be taking. So that's why I really do believe that having a trusted partner, you know, along the way and have having tools available that can lead people down that path and have a learning system in place to continue that learning and relearning, because people need to be retrained all the time.

But that is a huge impact to just understanding how people can get in.

*Ms. Clarke. And would you please, excuse me, I meant to say Mr. Dewhurst.

*Mr. Dewhirst. That's okay.

*Ms. Clarke. My aunt's name is Dewitt. Excuse me.

*Mr. Dewhirst. It's okay. It's not a common name, so I understood.

*Ms. Clarke. Okay. I am proud to say that this Committee has a strong bipartisan history supporting cybersecurity efforts. And it remains our priority to continue to close potential gaps and prevent cyberthreats against our infrastructure.

Fostering a cyber culture would mean having the infrastructure in place to address evolving risk, but also

having employees be mindful of best practices in day to day work.

Mr. Dewhirst, what tools and resources do water systems need to help foster a strong cyber culture and posture? And how can the EPA and Congress support the water sector as they work to build more awareness in cyber culture?

*Mr. Dewhirst. Yeah. I think I'll just elaborate a little bit further on what I just shared.

You know, I think having basic education. I mentioned the 15 water sector cybersecurity fundamentals, that is a base level understanding that I think would be very important for everyone in the sector to truly understand because it goes into a lot of different low hanging fruit, so to speak, of things that people can do.

I think the other thing is we should all have response plans to know what will we do if something were to happen. How do we stop the attack? How do we, you know, pause what's happening and get back control of what we need to get control of?

I think I just want to, you know, shout out to those who have had some incidents. They responded quickly, and they've

addressed it to where it wasn't a bigger issue.

So I think having that part of the culture too is really vitally important so that if and when it were to happen, we know what to do and how to respond to that, and we can operate our system with or without, you know, that other system in place.

So I think that's part of our culture that we have to develop and, you know, it's been heard. We rely a lot upon control systems. We rely a lot upon computers and to run our daily activities at a water utility.

We've made it to where people don't have to do as much because we have machines that do it in some way. So that's just an aspect that we've, you know, got to remind people how to go back to that if we have to. What do we have to do in case that were to happen.

*Ms. Clarke. Very well. Thank you so much, and I thank you all for your expertise on panel today.

Mr. Chairman, I yield back.

*Mr. Carter. The gentlelady yields.

The Chair now recognizes the gentleman from Ohio, Mr. Balderson, for five minutes.

*Mr. Balderson. Chairman, thank you very much, and congratulations. It is very kind of you to say that about Mr. Chairman Johnson. So thank you and you'll fill the great role here. So appreciate it.

Good afternoon, everyone. One of the major concerns _first of all, this question is for, I am sorry. Got so excited about the new chairman that, Ms. Tucker Vogel, this this first question is for you. I apologize.

One of the major concerns in any security regime is the importance of information protection. Currently, the Safe Drinking Water Act does not have any affirmative protection for water systems, vulnerability assessments, site security plans and other records collected from an on-site inspection that relate to those items.

Ms. Tucker-Vogel, do you believe that protecting this information from public disclosure is necessary?

*Ms. Tucker-Vogel. Absolutely. And that's one of the concerns that we had with the earlier EPA Cybersecurity memo that was asking us to do cyber assessments during regular drinking water system inspections.

All of those are public record and, any enforcement

action we take has to be a public record. Any violation we issue is required to have a public notice. So taking that approach would have meant that all the water systems vulnerabilities would have been out there in the public for anyone to take advantage of.

So we definitely have to have some way to protect that data.

*Mr. Balderson. Thank you. Are states capable, under their own laws, of protecting the public's release of systems vulnerabilities?

*Ms. Tucker-Vogel. It depends on the state. Some state open records laws are, they're different in each state. In Kansas, we can protect the data as long as we it's not under the umbrella of the Safe Drinking Water Act, which requires us to make certain information public.

So whatever we do, it will be outside of Safe Drinking Water Act and under state specific regulations so we can protect the information.

*Mr. Balderson. Okay. Thank you very much.

My next question is for Mr. Morley. Thank you for being here. I understand that you are a big fan of capacity

development for cybersecurity. Can you discuss how what you have in mind for the capacity development is different than asset management?

*Dr. Morley. Yeah. When I when I speak to capacity development, it's really empowering utility owner operators to get a handle on the cybersecurity issue in this case, which is new and evolving, and some of the actions that we would expect them to take, recognizing, as we've heard from our colleagues here, water utility operators are very excellent at their job, but they're not cybersecurity experts.

So while we have many lists and checklists, actually, the how part of implementing some of those provisions requires additional assistance, such as what was discussed here today. Those are the types of things where I think we could be more effective in providing direction and support on actual implementation, not just providing a checklist, and expecting people to implement.

*Mr. Balderson. Okay. What is the best way to deliver this kind of assistance, especially for smaller systems?

*Dr. Morley. Yeah. I'll just reiterate. I think

leveraging trusted partnerships with the associations such as those here today, is the most effective way to force multiply.

We already have the boots on the ground. Let's, leverage that capability, like we did in the past, and get it out there.

*Mr. Balderson. Okay. Thank you very much.

Ms. Tucker-Vogel, I'm going to come back to you. Mr. Morley's talked about funding from the revolving loan fund, excuse me, through the Infrastructure Investment and Jobs Act.

Congress provided significant resources to the Clean Water State Revolving Fund and the Drinking Water State Revolving Fund. As you know, states receive these capitalization grants from EPA to provide financial assistance to water systems for projects, including cybersecurity.

As these dollars are sent down to the states, do you feel cybersecurity is being prioritized as an eligible use of water systems?

*Ms. Tucker-Vogel. So it's definitely an eligible use.

I would not say that, at this point in time, cybersecurity is being prioritized over say a project that would resolve a water quality compliance issue.

So the SRF, the State Revolving Funds, you know, they are they are, first and foremost, to resolve compliance problems and make sure that water quality meets all applicable standards.

But cyber certainly could be used. There's no prohibition. At this point, I don't know that it's being prioritized over water quality issues, though.

*Mr. Balderson. Okay. Thank you all very much.

Mr. Chairman, I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the gentleman from Maryland, Mr. Sarbanes, five minutes.

*Mr. Sarbanes. Thank you very much, Mr. Chairman. Appreciate the opportunity to discuss this very important topic. And I am interested in how the response to these threats, when we're talking about our water infrastructure, is addressed in a kind of collaborative way at different levels of government?

We have had some experience in the Baltimore region. I represent Maryland where there was an exposure like that, and, you know, we had to scramble. And local authorities were trying to figure out what their responsibility was under those circumstances. And also what it means to prepare for the next thing.

And preparing for the next thing is critical because you want to anticipate these problems. You want to know what the role of others is going to be, so where you need to step up.

So I am interested to get a sense of what that collaboration can look like, and maybe from your perspective, Ms. Tucker-Vogel, if you could speak to that a little bit because there's an all hands on deck dimension to responding in these situations, but that can either look like a scramble, or it can look like a very, kind of, comprehensive and well-coordinated response where you can tell that people kind of understood their particular responsibilities and roles ahead of time and then they step up into the situation and respond as best they can.

So maybe you could start with some perspective on that?

*Ms. Tucker-Vogel. Sure. And I can speak from an

actual incident.

*Mr. Sarbanes. Okay.

*Ms. Tucker-Vogel. So that that might provide you some good insight. So we had a water system, it was not a state actor, but it was a disgruntled employee that was fired. And, you know, they failed to remove his access that he had from his cell phone, so he actually hacked in and shut the water system down.

So the water system, they are accustomed when they have problems to calling the state agency, the state primacy agency. So that they weren't getting a lot of response from local law enforcement because as you said, I'm not sure law local law enforcement knew what to do.

So they contacted my office. We have a very good working relationship with EPA Region 7's Criminal Investigation Division. I have their numbers, 24/7, I can call if there's an event. I called them, reached out. They contacted the FBI.

The FBI then responded and helped the local law enforcement. You know, they all started working together. And at that point, when the water system was brought back

online, and fortunately, there was no bad things that happened because of that, then the law enforcement agencies took that over.

Then as they went through the indictment and prosecution process, they would call us and ask for certain information about an individual, that type of thing.

So I think that's an example of where the collaboration between the state, local law enforcement, and federal law enforcement worked very well, and we were able to respond very quickly.

*Mr. Sarbanes. I mean, nobody wants to see these incidents and attacks occur, but to the extent they aren't hugely debilitating, they can represent teachable moments for everyone who's involved, and the result is everyone then ups their game to be ready for the next situation that could present itself.

I don't know if anybody else at the table would like to comment on this, Mr. Dewhirst, I don't know if you have a perspective you'd like to share?

*Mr. Dewhirst. Yeah. Yeah. No. I appreciate the question.

I think one of my most proud moments of being a utility leader is when we have crises, because I think we rally to the moment, and we all do a great job of, you know, getting the thing taken care of, right? And we do reach out to our primacy agencies.

We do have a part, as I mentioned earlier, we are a partnership to provide public health and safe drinking water. I also would just want to reiterate again, I think WaterISAC has a role in that too, where this, you know, once those incidents occur, we want to make sure that the community then understands it.

So to your point, we want to make sure people understand what occurred, how do they get access so we can ask ourselves of our individual utilities, is that a threat for us.

So I think the more that we stay connected and can learn from everyone's experience, and I think WaterISAC is that central force to do that.

*Mr. Sarbanes. Right.

*Mr. Dewhirst. For those types of things, it's very valuable to us.

*Mr. Sarbanes. Okay. Appreciate it. Thanks very much.

I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the gentleman from Idaho, Representative Fulcher, for five minutes.

*Mr. Fulcher. Thank you, Mr. Chairman. And, to the panel, thank you for being here. I wasn't able to get the opening statements, but has not been able to participate with all the discussion. But I have a couple of questions.

Today's discussion is relevant to me and my state in a number of ways. Not just because I have drinking water utilities in the district, but I used to work in the computer sector and I have some interest in this area, but we also have Idaho National Lab in Idaho, and they do a lot of good work with water systems operations and how to address those vulnerabilities at the lab.

And so I am going to start with Mr. Dewhirst, but, really, there are others on the panel who may want to chime in on this.

It appears, from the work at the lab, that they are finding how degraded piping and other problems can undermine the ability of chlorine to prevent Regrowth of bacteria in

certain pathogens.

Mr. Dewhirst, can you help me understand and explain this? Is cyberattack, likely, able to leverage that in certain ways to spoof the water quality drinking systems? Any insight on that topic you might have?

*Mr. Dewhirst. Well, I think the safest answer to that question, everybody, it's possible. You know, I think it's it depends solely on a utility, how their network has been configured and established, but I know we've had some incidents, that have been recorded, where they can take part of the control system and take over that operation and cause some changes to it.

So from that standpoint, I guess the answer to your question is yes, it's possible. But I think for many of us, we've tried very hard to not allow that type of access, but it's not always true.

*Mr. Fulcher. Others on the panel? Yeah. Yeah. Yes, Mr. Morley?

*Dr. Morley. Yeah, I'll just add to that. You know, I think the important thing to remember, in terms of utility culture and how we operate, we apply a multi barrier approach

that applies to cybersecurity as well in terms of ensuring water quality.

As it relates to the Idaho National Labs, you know, they do have the water security test bed where they have been _

*Mr. Fulcher. Right.

*Dr. Morley. _ having some conversations with EPA about doing some of the destructive testing that would examine vulnerabilities. Support for continued research in that realm would be very effective.

AWWA has also worked very closely with Idaho National Labs on some of their programs on consequence informed Cyber-Driven Engineering or CCE. We believe that's an excellent, level of maturity in assumed failure of certain technologies and how you overcome that.

So that kind of work with Idaho National Labs is very, very productive.

*Mr. Fulcher. So as you mentioned, and thank you, Mr. Morley. So I am going to come back to you. We do have the test bed at the lab there. And so I believe that that is a proper role of government, in terms of the work they are doing in this regard.

What else should we be doing as Congress to be addressing this? And forgive me if this is a repeat question because, again, some of us have more than one Committee at the same time. But what should we be doing? What is the proper role for Congress here, without meddling, but hopefully helping?

*Dr. Morley. Yeah. Well, I mean, the test bed, certainly, you're familiar with that. That's an important, valuable research opportunity to understand things.

In addition, I think a very concerted effort to elevate enrollment and awareness of things like the CISA's Vulnerability Scanning Tool, super effective for small systems, especially some of the incidents that we talked about earlier, that were result of publicly facing devices.

That resource is specifically targeted to mitigating that vulnerability exposure. That would be my number one priority.

*Mr. Fulcher. Okay. Thank you for that. Is there anyone else? I have got a minute left. Anybody else on the panel want to address that? What should be we be doing? Mr. Jeffares.

*Mr. Jeffares. We talked about it during the course of the meeting, you know, when EPA is involved, we're going to write guidelines, you know, technical assistance, we've talked _ that's the word that's been said all day long.

We're going to need funding. We're going to need training. And we're going to have to get that message to the operators around the state. That's the long-term solution.

*Mr. Fulcher. Great. Thank you again to the panel.

Mr. Chairman, yield back.

*Mr. Carter. The Gentleman yields.

The Chair now recognizes gentleman for California, Dr. Ruiz, for five minutes.

*Dr. Ruiz. Thank you, Mr. Chairman.

As I have highlighted in prior hearings, cybersecurity stands as one of the foremost national security challenges our nation is confronting.

In the last five years, cyberattacks have been on the rise. In my district alone, the College of the Desert, the Imperial Community College, and Imperial County were all hit with cyberattacks.

These offices provide critical infrastructure support in

my district. Not to mention we have had some hospitals also, been attacked through cyber means. While, thankfully, no infrastructure was damaged, I continue to be heavily concerned about potential future attacks.

One area of specific concern is the vulnerability of our water systems. Security lapses in a water system can jeopardize the safety and purity of water sources. Attackers might manipulate treatment procedures or introduce hazardous substances leading to significant health risks.

Unfortunately, smaller water systems that serve some of the country's most vulnerable populations, like those in my district, rural, underserved, under resourced, often lack the resources to prepare for and mitigate the impacts of water system disruptions, including those caused by cyberattacks.

I live in the desert, so you can imagine what a stoppage of water would look like to the community and our livelihoods.

Mr. Dewhirst, what would you highlight as some of the unique challenges that smaller and under resourced water systems face in preparing for and responding to cyberattacks?

*Mr. Dewhirst. I would answer that by saying that I

think in many cases, it's fundamental information. I think there's some foundational tools that are out there and some information that that is accessible to smaller utilities that if they had someone to walk them through these basic fundamental things, they could look at their system, understand what the vulnerabilities are, and really how to shore them up and address.

*Dr. Ruiz. Where can one find these resources?

*Mr. Dewhirst. WaterISAC has put out free resources for just that purpose. We have 15 cybersecurity fundamentals for water systems that is accessible to anyone. So that's the first place I would start.

*Dr. Ruiz. Okay. And throughout this hearing we have discussed how some of the requirements under the section 1433 of the Safe Drinking Water Act require water systems to conduct a risk assessment and prepare an emergency response plan incorporating their assessments.

Mr. Dewhirst, what recommendations do you have to help smaller and under resourced community water systems identify their unique system risks and take steps to mitigate them?

*Mr. Dewhirst. So I think, again, the most important

thing is to find a trusted partner. I think Mr. Jeffares have talked about that quite a bit for rural systems.

They often don't want a large utility, maybe someone like myself, to come in and try to show them the way. They trust, you know, people like themselves and I think the more we can link up resources like that together and provide their, you know, trust and partnership together, that'll go a long way in really implementing proven procedures.

*Dr. Ruiz. Mr. Jeffares, what _ do you want to add anything?

*Mr. Jeffares. As we mentioned earlier, you know, The rural water stations went out. We helped these little systems do the vulnerability assessments, the ones who are required to do it.

I mentioned earlier, when it comes to emergency response plan, it's one thing to develop emergency response plan. But did you implement it? So when that emergency does happen, does somebody know what it actually says and what's the first move and where do we go from here?

That's what we try to preach to our small systems, know what to happen when there's emergency. Tornado, what

whatever it is. Know the steps and that's the hardest part we have is to get it implemented where they know what it says and what they need to do first.

*Dr. Ruiz. Well, I understand you are from Georgia, so you are familiar with tornadoes. I am from Southern California. We are familiar with earthquakes.

*Mr. Jeffares. Yeah.

*Dr. Ruiz. Mr. Dewhirst, can you elaborate how the grant programs, you mentioned in your statement, would help water systems address potential risks and threats?

*Mr. Dewhirst. Yeah. I mean, there's a number of funding opportunities that have been authorized by Congress. Some of them have been appropriated, but not to the level that was promised.

So I think the more we can show that cyber is a priority and that, you know, as Ms. Tucker-Vogel indicated, a lot of funding has been put forth from a lot of different infrastructure, and we've been focused on the quality issues of water, not necessarily cyber.

But if it's actually kind of told this is for cyber purposes, I think that you would see some action take place

and that would really promote people to really take a look at it because you're offering a way for people to solve the problems.

*Dr. Ruiz. And my understanding, just to name a few for those who are who are watching, are the Water Technical Assistance Information Grant, the Midsize and Large Drinking water systems infrastructure resilience sustainability Program Grant, and the Advanced Drinking Water Technologies Program Grants, correct?

*Mr. Dewhirst. Yes.

*Mr. Ruiz. Awesome. Awesome. Well, I ran out of time, but I appreciate the indulgence, and I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the gentleman from Texas, Mr. Pflueger, for five minutes.

*Mr. Pfluger. Thank you, Mr. Chairman. I wanted to ask my colleague, Mr. Ruiz, how many people he has watching back home. But I know it is probably a lot.

*Dr. Ruiz. That was my mom and my wife, but appreciate it.

*Mr. Pfluger. We appreciate the witnesses. This is an

important issue. I think I am the only member on ENC that serves on Homeland Security as well, and I think there is some shared jurisdiction when it when it comes to the protection of critical infrastructure, obviously, drinking water being, being very, very important.

So you know, I will just start by saying I do have some serious concerns about the EPA being the cyber watchdog, if you will. I think that there are some, and maybe we'll get to some of that.

So, Mr. Dewhirst, you mentioned that your utility in Tacoma houses both electricity and water, and you also mentioned that the Committee should look at NERC as the model used in electricity. What do you think the key differences are between water and power sectors that you think we should know when looking at this and investigating this issue?

*Mr. Dewhirst. Yeah. Thank you for the question. I do, come from a utility that has a water and a power component to it. We jostle about which one's more important, but we won't go there right now.

I think the one thing to know, the bulk electric system is much more interconnected than water systems are. So

that's generally very interconnected because of the grid stability and the up generation and also balancing authorities talking back and forth all the time across their networks to make sure the grid stays stable.

So that's a really key difference. We're much more isolated. Our product weighs, You know, eight and a half pounds per gallon or so. So to move, it takes a lot of infrastructure that's not really cost effective to do.

And there's also a lot more of us, right? But I think there's some things we can learn from that NERC model. You know, you expressed maybe some concern with EPA as the lead.

I mean, FERC is definitely the lead of NERC, you know? And what they do in that process is FERC will actually issue a proposed regulation and then NERC will then meet with sector leaders, and it's a sector led group, that's going to then say, how can we address this as a sector? How can we take this into account and put forth a solution that will work for the water utility sector in our case?

So it's made up of folks who understand cyber. They also understand how water utilities work and what they need to have happen as we implement whatever solution we want to

go with.

I also think the other aspect of NERC that's really important to think about is it's a risk-based approach. So we've heard the gentleman, I think another gentleman from Texas there talking about his dermatology and risk, and he asked accordingly.

I think we should take the same approach with this. Those systems that have treatment systems that serve greater populations that are wholesalers to others that would have a much bigger impact should be held to a higher standard.

And we should then think about a lower standard for those who maybe just have a distribution system or what level of protection do they actually need.

I mean, Mr. Jeffares has commented on that here today. It's a lot different and there's 50,000 of us across country. So, you know, that's a couple of the things that I think are really important to think about.

*Mr. Pfluger. Thank you very much.

Ms. Tucker-Vogel, some people would argue that the EPA should treat oversight of cybersecurity at water systems the same way that EPA and its federally delegated states treat

drinking water contaminants at drinking water systems.

So from you and your member's perspective, can you talk to us about why cybersecurity should be thought of as a different entity than assessment of contaminants and drinking water disinfection and treated water provision of the Safe Drinking Water Act?

*Ms. Tucker-Vogel. Well, I would say the primary difference between cybersecurity and water quality and the Drinking Water Act is it makes sense to have transparency and public information on water quality that people are consuming.

People need to be informed about the quality of the water they're drinking. What we don't want to do, with cyber, is make the cyber vulnerabilities at water systems public knowledge. So that's the big difference.

You know, the Safe Drinking Water Act is really focused on public knowledge, public information. We can't treat this the cyber sector the same way.

*Mr. Pfluger. Being a military guy, you always protect your vulnerabilities.

*Ms. Tucker-Vogel. Right.

*Mr. Pfluger. That is the thing that remains classified. I couldn't agree with you more on that.

Mr. Morley or Dr. Morley, sorry about that. Do you agree with that? And if not, you have different thoughts, or should the EPA be the only one to decide what methods should be used by utilities? You know, talk about the collaborative approach you'd take?

*Dr. Morley. I appreciate the question, and I agree with Cathy on the need to protect that information from public disclosure that could be used against any system.

Secondly, in terms of a construct, I think a collaborative approach is the most effective in understanding the differences in operational complexities that you've heard about today.

That kind of shared engagement through a process, like, you know, this collaborative model, I think is most effective in getting us down the road.

*Mr. Pfluger. Thank you, guys. It is important that our agencies share information with you. If that's not happening, we need to know that. That is the accountability we can provide, and whether it is FBI or CISA at Homeland

Security, EPA, doesn't matter. They need to be sharing in that public-private partnership.

Mr. Chairman, thanks for the hearing. I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the gentleman from California, Representative Peters, for five minutes.

*Mr. Peters. Thank you, Mr. Chairman, and thank you, for serving as Chair. We are lucky to have you, and we look forward to working with you in that role. Thanks for having this hearing.

Cyber criminals and foreign adversaries are increasingly targeting our critical infrastructure in ways that are increasingly sophisticated and potentially dangerous. These attacks, especially, cyberattacks on our water and wastewater systems could have very serious consequences to public health and customer privacy and have to be mitigated.

The Infrastructure Investment and Jobs Act was specifically crafted, in part, to help address these potential weaknesses. And among other protections, provisions we directed EPA to study existing and potential future technologies that could help address cybersecurity

vulnerabilities while providing grant funding to help communities address their resilience to both cyber and physical threats.

And back in my district in San Diego, the San Diego County Water Authority performs regular, vigorous, and comprehensive security assessments that are very expensive and time consuming.

But not everyone can afford to do that kind of work on their own, so we can't leave anyone behind when it comes to hardening our critical infrastructure.

Mr. Dewhirst, I want to ask you to put a finer point on something you have addressed. A lot of water systems operate on older legacy systems that are tricky to upgrade or bring into the cloud with other more secure systems.

Can you give us some specifics on how the incorporation of existing technology or the development of emerging technology practically helps day to day water systems mitigate their gaps in cyber preparedness?

*Mr. Dewhirst. I'm not sure I completely understand that question. Can you go one more time?

*Mr. Peters. How are you going to use technology as a

water system? How would I explain to my constituents why technology is important to the way you operate their water system and why it has to be secure?

*Mr. Dewhirst. Okay. Yeah. I mean, the reason it needs to be secure, first and foremost, is we rely upon a lot of computer technology to operate the system. You know, it's really the backbone.

We call a system called SCADA. SCADA stands for Supervisory Control and Data Acquisition. So a lot of what we do with our control systems is actually collect the data that we then send to our primacy agency to demonstrate that we're meeting compliance and we're meeting drink water standards. So that's why that's really important to safeguard.

And also then the overall operation of the system control is actually in that same system. So it's a critical component to any water system.

*Mr. Peters. And I think constituents and ratepayers would understand, you know, from their own experience with computers, the need for cybersecurity.

I might also understand that Congress, with the

resources that we have, could provide technical help to agencies. What specifically would you like to see Congress do to help agencies like yours proactively harden your cyber security infrastructure?

*Mr. Dewhirst. I alluded to it in my testimony, but there've been a number of programs that have been established or I guess or authorized is the appropriate term here in Congress, through different acts.

I think to actually appropriate the funds to fund those fully would really put a put a priority, a national priority on the importance of cybersecurity. I think a lot of great things that started with Congress has allowed a gentle push to kind of get the ball rolling down the hill that would then be followed through, and people will then start to understand the value in investing in that sort of thing. I mean, yeah.

*Mr. Peters. So it is not so much new laws as funding the laws we've already passed?

*Mr. Dewhirst. Correct.

*Mr. Peters. Is what I hear? And then finally, what should we expect of water agencies? What do you think their duty is? What can we count on them to do? Because,

obviously, we can provide resources, we can provide, technological assistance _

*Mr. Dewhirst. Right.

*Mr. Peters. _ but what should we expect of water agencies in return?

*Mr. Dewhirst. Well, I mean, I think we, like you and everyone in our community, does not want to see a threat happen. We do not want to see anything like this happen.

So I think we need to take it upon ourselves to ensure that we are following the guidance and the available resources we have.

So you mentioned about looking at new technologies. I think we already have a lot of tools, a lot of things already in place across our industry that if we could get consistent application and really, you know, diversified across the entire community, that will go a long way to, like, at least stopping the initial threat of this concern.

*Mr. Peters. Great. And there has been already a lot of discussion of the difference between smaller and rural and urban. I won't go over that, but I appreciate the witnesses all for being here today.

And again, Mr. Chairman, thank you for having the hearing, and I yield back.

*Mr. Carter. The gentleman yields.

The Chair now recognizes the gentlelady from Iowa, Ms. Miller-Meeks.

*Ms. Miller-Meeks. Thank you very much. And, again, congratulations to our new Chair, Representative Buddy Carter. And also thank you to our witnesses for testifying, to the Committee today.

Like the past Republican who spoke, Representative Pflueger, I too was on the Homeland Security Committee last term and so carry that over with me as we look towards both high quality water, the staffing that's needed to be able to perform those functions, and then also the cybersecurity, which is a national as well as the water quality issue.

Mr. Jeffares, your testimony talks about the need for rural water systems to receive help on technical assistance and how to implement the best cyber protections and coming from an agricultural state with a lot of rural areas and rural water in my district, I think it is important that which system is going to work best and what is a better model

to reach solutions, compliance enforcement, or technical assistance?

*Mr. Jeffares. It's definitely technical assistance. Getting the people, rural water, whoever the third party is to come out and train operators. You know, and I've said it earlier, it's always better when an operator is talking to an operator.

So let's train a good operator in cybersecurity and let him be the one that goes out and rides the states. You know, I think each state's going to need two people tied directly to just cybersecurity that are out training, teaching.

I always like to use the word coach. Sometimes you got to coach them along. And I think that's the answer.

*Ms. Miller-Meeks. That is what the people in Iowa tell me as well too. What is the best way to maximize the use of technical assistance for cybersecurity for rural systems? You can get back with us on that.

*Mr. Dewhirst. We will. Thank you.

*Ms. Miller-Meeks. Okay.

The EPA is planning to use a one size fits all regulation for lead, copper, and certain PFAS and water

systems.

And, Mr. Jeffares, you made the point that each water system is unique. Can you explain why cybersecurity solutions need to be scalable, sizable, and affordable?

*Mr. Jeffares. Yes. As I mentioned earlier, affordability is the key. You know, a $5,000 bill from a little system, it's a lot of money.

And so and we talked about the vulnerability assessments. You know, see in Atlanta, that vulnerability assessment might be 100 pages long. You get down around some of these little small towns in South Georgia, you probably come up with a ten-point checklist that would take care of all their cybersecurity needs.

So that's just the difference in the big systems and the little systems. But, you know, technical assistance is going to be the key for the big ones and the small one. People out training, teaching us how this works.

Earlier, I mentioned, you know, the average age of an operator is about 58 years old. And we're all leaving here in about seven, eight years, and I don't know who's going to take our place. So we got a lot of work to do.

*Ms. Miller-Meeks. I hear that in Iowa also. And you may have answered this question, but with a limited budget, how do you prioritize compliance with these issues?

*Mr. Jeffares. With the cybersecurity? As I mentioned earlier, a lot of them don't _ they're not hooked to the Internet, so they're not a concern now. But as technology grows, that day is going to change. And so it's going to be financially, and it's going to be training technical assistance. Those are the ways we're going to make this work.

*Ms. Miller-Meeks. And then I am going to direct this question to all of our witnesses. And if you can, be brief in your answers because I am running out of time.

Given the EPA's challenges in rolling out guidance to address cybersecurity and water systems, it is clear that a new approach is needed to improve resilience without imposing new costly mandates on water authorities. What role does private cybersecurity industry play in providing real time cyber risk monitoring systems?

*Ms. Tucker-Vogel. So the question was what role do private cyber companies play?

*Ms. Miller-Meeks. What does the private cybersecurity industry play?

*Ms. Tucker-Vogel. Well, they can play a good role. I think that, you know, they can do some assessments. They can help do some training. I would suggest that state agency's role, in working with third parties, is to make sure that the third parties are qualified third parties, and we look to our Kansas Information Security Office, when somebody has had a third-party vendor do an assessment, to make sure that that vendor was an approved knowledgeable vendor.

There are, as with any case when there's a hot topic out there, people come out of the woodwork to provide services, and so we want to make sure that the services are being provided by qualified people.

*Ms. Miller-Meeks. Thank you, Dr. Vogel.

Mr. Dewhirst, quickly.

*Mr. Dewhirst. I think that's an excellent point. I do believe too that, you know, we need to take advantage of all the knowledge in this space. I don't think we could just put ourselves in a vacuum and think we all have it figured out.

So I would invite, you know, others to come to the table

to provide insight.

*Ms. Miller-Meeks. Thank you.

Mr. Jeffares?

*Mr. Jeffares. There's certain vendors and there's certain equipment that you buy that has its own built in ties into the internet. And I mentioned in my testimony, we need to make sure they are looked at. The guidelines, that they're meeting the guidelines. Somebody is monitoring them who's selling this this type of equipment that needs the internet to run.

*Ms. Miller-Meeks. And Dr. Morley?

*Dr. Morley. Yeah. I would just add on that that the system integrators that are involved in supporting systems, especially smaller systems that don't have in-house capability, really need to have a standard of care from a professional ethics perspective is something to consider. Thank you.

*Ms. Miller-Meeks. Thank you all very much.

I yield back my time.

*Mr. Carter. The gentlelady yields.

The Chair now recognizes the gentleman from Alabama, Mr.

Palmer, for five minutes.

*Mr. Palmer. Thank you, Mr. Chairman. And like everyone else, congratulations on the chairmanship. I know you will do a fabulous job, and we will do all we can to help you.

Mr. Dewhirst, you have got a diverse background. You are an engineer. You have been involved in multiple systems. And one of my concerns is, when we talk about cybersecurity, a lot of times people think it is about someone shutting down the system with malicious purposes for, you know, introducing something in into our water. The ransom attack, weren't ransomware attacks also an issue? Have we seen those?

*Mr. Dewhirst. I'm aware of at least one or two.

*Mr. Palmer. Okay.

*Mr. Dewhirst. So I think that they can occur, which again, is why it is so important and critical to have, you know, your incident action plans in place and really have your recovery plan ready in case something like that would occur.

There are ways to plan for that sort of thing to where you can restore your network to where it was before that

happened. So.

*Mr. Palmer. Well, anyone of you can answer this. In my district, we have the National Computer Forensics Institute, and they do, basically, war gaming to help systems prepare for something like that. Have any of your systems taken advantage of that?

*Ms. Tucker-Vogel. So we haven't taken advantage of work games, but we do encourage training and tabletop exercises that includes cybersecurity as well as kind of an all-hazards approach.

And to your previous question about ransomware. In Kansas, in the last, oh, three months, we've had, I believe, is four or five ransomware attacks on public water supply systems.

The fortunate thing is the operational side, where the water is treated, is isolated from the business systems. And it's the business systems, the billing systems, you know, the administrative sites that have been attacked.

*Mr. Palmer. So you wouldn't have an issue like we did with the Colonial Pipeline, where they could shut down your water distribution?

*Ms. Tucker-Vogel. No. And in every case, when we've heard of these attacks, the first thing we do is we contact the water system to say, is your treatment plant jeopardized? And in all cases, they've said, no. We're isolated from our business system.

So there's a good awareness out there about the need to have water treatment isolated from business systems.

*Mr. Palmer. Did you know there is public concern about contaminants that could possibly be introduced into the water system? And one of the questions, one of the points that was raised to me, is whether or not our water systems ought to have analog systems as backups.

And it made me wonder what type of backup systems you might have in the event of a cyberattack?

And, Mr. Dewhirst, Mr. Jeffares?

*Mr. Dewhirst. So again, I think if we had a cyberattack occur in our system, we have ways to detect that and then isolate that incident. And then we'd have to do an assessment about what was impacted. Was a control system in any way _

*Mr. Palmer. But what about the smaller systems? I

grew up in a really small town, and we didn't have _ we didn't have any cyber worries back then because we didn't have any systems.

*Mr. Jeffares. Right. And a lot of them still don't. So there's really not a backup, you know? Like I said, we've talked about it. We've trained them in it. You know, we're trying to familiarize people with what's going on?

But, you know, going back to the ransomware. I guess it was two years ago, my hometown, they got into the county commissioner's office. You couldn't get a tag. I mean, they shut them down for about two weeks before somebody finally did something.

And that's really all, and I think she mentioned it earlier. It's really all you can do to some of these water systems. Yeah, you may hack their office. You may steal identities. You may shut them down, but most of these water plants do not have where I can call in and change things.

I mean, they can, but most of them don't. And even when you make a change at a surface water plant, usually your chemical feeders got a range. So you could only go so high or so low, probably not ever going to contaminate.

You may mess up the operations for an hour or two, but probably never going to do anything dangerous because the range on the feeders is so small.

*Mr. Palmer. Mr. Morley, since you are the only one who hasn't had a chance to answer a question in the last few minutes, I will leave this with you.

It appears to me that we don't need a one size fits all, approach to this because you have got such diversity in our systems. And you can use remainder of my time to respond.

*Dr. Morley. I appreciate it.

*Mr. Palmer. You are the only one between us and going to vote.

*Dr. Morley. I think having some awareness of the capability to maintain manual or analog control is really critical. As part of the fundamentals of the Idaho National Labs consequence driven cyber inform engineering protocols that we're working with them on for the water sector.

So that is an important redundancy for utilities to keep into consideration as automation and pressure towards automation increases. And, in fact, some of the technologies that we would have to implement to address a new regulatory

regime requires significant amount of automation. So that that is something to keep in mind.

*Mr. Palmer. Thanks you for your testimony and for answering our questions.

Mr. Chairman, I yield back.

*Mr. Carter. The gentleman yields back.

I believe that all members have been recognized at this point who want to participate. I want to thank the witnesses for being here. We appreciate your time and your effort to be here.

I remind members that they have ten business days to submit questions for the record and I ask the witnesses to respond to the questions properly.

I also ask unanimous consent to insert in record the documents included on the staff hearing documents list.

Without objection, that will be the order.

Without objection, the Subcommittee is adjourned.

[Whereupon, at 4:08 p.m., the Subcommittee was adjourned.