Table of Contents

U.S. Senate Date: Wednesday, July 21, 2021

Committee on Environment
and Public Works

Washington, D.C.

ADDRESSING CYBERSECURITY VULNERABILITIES FACING OUR NATION'S PHYSICAL INFRASTRUCTURE

Wednesday, July 21, 2021

United States Senate

Committee on Environment and Public Works

Washington, D.C.

The committee, met, pursuant to notice, at 9:51 a.m., in room 406, Dirksen Senate Office Building, the Honorable Thomas R. Carper [chairman of the committee] presiding.

Present: Senators Carper, Capito, Cardin, Whitehouse, Markey, Padilla, Boozman, Sullivan, Ernst.

STATEMENT OF THE HONORABLE THOMAS R. CARPER, A UNITED STATES SENATOR FROM THE STATE OF DELAWARE

Senator Carper. Good morning, everyone. I am pleased to join Senator Capito in calling this hearing to order.

I want to thank each of our witnesses here today for your willingness to share your perspectives on cyber vulnerabilities that our infrastructure systems face.

We are joined this morning by leaders who will discuss cyber vulnerabilities in our highways, our municipal drinking water, our wastewater, rural water systems, as well as inland waterway systems. A warm welcome to Sophia Oberton, to John Sullivan, to Shailen Bhatt, and to Evan Pratt.

We are also delighted to be joined today by two of our colleagues, one former governor colleague I served with as governor for many years, our friend Angus King here in the Senate from Maine and Representative Mike Gallagher. They serve as the Co-Chairs of the Cyberspace Solarium Commission, the bipartisan intergovernmental body created in 2019 to develop a strategic approach to strengthen our defenses against cyberattacks. Both Senator King and Representative Gallagher have provided invaluable leadership on the issue of cybersecurity. We are pleased to welcome them here this morning. Thank you both very much for joining us.

I especially want to thank our Ranking Member Capito this

morning for suggesting this hearing in the first place and for her work and the work of her staff in helping to put it all together.

All of us gathered here today understand the importance of protecting our Nation's critical infrastructure, yet in the past year alone, we have witnessed several major cyberattacks that have hobbled critical systems across our Country.

Unfortunately, no government agency or industry is immune to attacks from the vast array of bad actors who seek to undermine our security and profit from our vulnerabilities. We face threats from unscrupulous individuals, from criminal enterprises, and antagonistic state actors 24 hours a day, 7 days a week.

It is unclear that many of our Nation's vital transportation and water systems face especially serious challenges in dealing with cybersecurity vulnerabilities.

A 2019 report from FHA, the Federal Highway Administration, stated that, and I am going to quote, "the Department of Homeland Security considers the Transportation Systems Sector to be one of 16 critical infrastructure systems … so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, on national economic security, and our national public health and safety.

It is not hard to imagine how they came to that conclusion.

If we look at our highways, our tunnels, our bridges, we can see that they are dependent on vast inter-operating computer systems, each with their own vulnerabilities to cyberattacks.

We should also be increasingly concerned by the mounting cybersecurity challenges facing our Nation's drinking water and wastewater systems. According to a 2019 report by the American Water Works Association, cyber risk is the top threat, the top threat, facing the U.S. water sector today. Just one year earlier, the Department of Homeland Security and the FBI warned that the Russian government was specifically targeting the water sector and other critical infrastructure as part of a multi-stage intrusion campaign.

Cyber vulnerabilities in our water systems represent unique national security challenges. A major breach in our water infrastructure system could jeopardize the safety of our drinking water and impair communities' ability to safely dispose of harmful waste, threatening human health.

The cybersecurity of our inland waterways is yet another area that requires our attention. Approximately 15 percent of all domestic freight moves through our intra-coastal and inland waterway systems. The safeguarding of this system is vital, not only for economic activity, but also for effectively protecting our communities form flooding.

These threats are large in scale and require widespread

collaboration. I am looking forward to hearing from all of our distinguished witnesses today on how federal and State agencies can work together with industry and community leaders to strengthen the cybersecurity of each of these vital parts of our infrastructure, but before we do that, let me offer some observations upfront.

There is no one-size-fits-all solution to all of the different cyber threats facing our critical infrastructure systems. At the federal level, we should build flexibility into our solutions so that State and local leaders have the tools they need to effectively address their unique cybersecurity challenges.

At the same time, we must also recognize that many local government agencies and infrastructure systems face significant challenges in just fulfilling their core missions. Therefore, any Federal assistance in cybersecurity should be structure to help these entities remain focused on their core missions.

Finally, I believe it is incumbent on us to recognize that cybersecurity is a long-term, constantly evolving challenge. Addressing this challenge requires sustained Federal investment, not one-time solutions.

With that, I am happy to turn to our Ranking Member, Senator Capito, for her opening remarks. I want to thank her again, her and her staff, for coming up with this idea and

helping to make it happen. Senator Capito?

[The prepared statement of Senator Carper follows:]

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

Senator Capito. Thank you, Mr. Chairman. I want to thank all the witnesses that are here and thank my colleagues, Senator King and Representative Gallagher, for being here with us today.

We look forward to hearing from you on the best ways to protect our physical infrastructure from cyberattacks. I think it is a very timely hearing, as we have seen attacks here in the last several months, how the Federal Government can partner with industry, State, and local partners, and what gaps we have that are leading to our vulnerabilities.

This committee has a leading role in ensuring the safety and security of our Nation's core infrastructure system, and we are committed to being a strong federal partner in tackling the most challenging issues that cyber threats present.

We must work together, and I think we will, on this issue to find solutions that will safeguard the whole of our core infrastructure, which include our water systems, our port and inland waterways, flood control infrastructure, highways, bridges, and tunnels.

The speed of advancing technology and the improvements this has on our day-to-day lives of all Americans is extremely positive in a lot of ways. We are working toward a more modern and a more connected transportation system.

This does, however, create a level of urgency for implementing strong cybersecurity measures. On our roads and bridges, vehicles and infrastructures are becoming more connected and smarter. With these types of advancements, increased data and access to that data can result in safety and privacy threats. It opens our transportation system up to vulnerabilities that didn't exist in the past.

To help address these types of threats, our committee passed the Surface Transportation Reauthorization Act of 2021, in which we expanded eligibilities under the National Highway Performance Program, NHPP, and the Surface Transportation Block Grant Program, STBGP -- they all have little initials for everything -- for cybersecurity protections, and added a requirement for the Federal Highway Administration to develop tools to assist transportation agencies in protecting and recovering from cyber incidents. I think it is important that we have the capacity. A lot of our local systems don't have the capacity to really meet these challenges and need some assistance.

These provisions will help to protect our highways, bridges, and tunnels against emerging cyber threats and protecting our critical transportation infrastructure.

Cyberattacks are also a growing threat to our water and wastewater systems. We have seen a growing number of these

systems fall victim to these attacks, which have significant implication on public health and safety. These attacks are very scary for the public, when you think about your water system being invaded, when they occur and can leave us questioning the safety of our water systems.

I am proud of the work this committee has done so far to address cybersecurity vulnerabilities in drinking water and wastewater systems.

The Drinking Water and Wastewater Infrastructure Act, which passed out of this committee unanimously and was approved on the Senator floor by a vote of 89 to 2 --

Senator Carper. How much?

Senator Capito. Eighty-nine to two, includes provisions that provide funding for protections against cybersecurity vulnerabilities to our water systems all around the Country.

Though I am proud of our work, there is more work to be done, and the Chairman talked about this. I look forward to hearing from our witnesses on the ways the Federal Government can act as a better partner is protecting our drinking water and wastewater systems from cyberattacks without costly mandates that can distract from the core mission of providing safe, reliable, and affordable water service to the American Public.

The physical infrastructure of our ports, inland waterways, and flood control systems are also potential targets for foreign

adversaries and cyber criminals pursuing ransomware attacks.

Hacking of these systems can harm our economy and pose threats to human life, property, and the environment.

Providing the tools to the government agencies, industry partners, stakeholders responsible for protecting our critical infrastructure from cyberattacks is essential.

Maintaining resiliency against cyber threats is also an ongoing and ever-evolving process.

As the Chairman said as well, and a little bit differently, but it is not a one-and-done event. We cannot put blinders on and think we have finished everything when we come to envisioning potential threats, because we know those threats change daily.

Government agencies such as the Corps of Engineers have been partnering with other agencies and local communities to address cybersecurity for our infrastructure.

We need to continue to support training exercises and information sharing between agencies to protect our critical infrastructure, such as the electrical grid, our water systems, transportation systems, and emergency response systems.

I expect that the committee will continue to include cybersecurity in our WRDA bill, which we are beginning work on, that is the never-ending story water bill, and as we have in our transportation, drinking, and wastewater legislation.

I look forward to hearing from our witnesses today about the best practices and key challenges facing the security and safety of our transportation systems and how we can work together towards protecting all American's and that critical infrastructure through strengthened cybersecurity measures.

Thank you, Mr. Chairman.

[The prepared statement of Senator Capito follows:]

Senator Carper. Thank you, Senator Capito. Well said.

Now we are going to turn to our witnesses, our colleagues. We welcome our first panel, which is comprised of our distinguished colleagues, Representative Mike Gallagher, whom I don't know well. I am happy to see you again and welcome you today from the Badger State of Wisconsin.

I will never forget, as a 17-year-old freshman to Ohio State, I pledged to a fraternity, homecoming, we were playing Wisconsin at the homecoming football game. Football is a big deal at Ohio State, and we erected a two-story-high badger, a paper-mâché badger, in front of our fraternity, and I think I got to put the halo or something on top of it. I learned from an early day in my life what the Badger State was all about. Then we went out and crushed Wisconsin.

[Laughter.]

Senator Carper. No, I don't think so. Anyway, we are glad you are here and delighted that Angus is here. Senator King and I had the privilege of serving as governors together, and it is great to be able to work here on all kinds of issues that are important to our Country, especially this one.

These two gentlemen currently serve as co-chairs of the Cybersecurity Solarium Commission, which was established by the 2019 National Defense Authorization Act to develop a consensus National strategy to counter significant cyberattacks. Working

together, Representative Gallagher and Senator King have provided crucial leadership in defending our Nation from cyber threats, and so we are very pleased that they could join us this morning to share their insights with us, so thank you both.

I am going to ask Representative Gallagher, if you would lead off, and for Angus to follow in turn. Thank you both very much for joining us.

STATEMENT OF THE HONORABLE MIKE GALLAGHER, A UNITED STATES REPRESENTATIVE FROM THE STATE OF WISCONSIN

Mr. Gallagher. Well, thank you, Chairman Carper and Ranking Member Capito. It is an honor to be here. I won't spend any time talking about my college fraternity experiences, because they all make me disqualified for office.

[Laughter.]

Senator Carper. It is a PG audience.

Mr. Gallagher. Exactly. It is also an honor to be here with my good friend and fellow Solarium co-chair, Senator Angus King, whom I've worked incredibly close to with on this project over the last few years, and really learned about the importance of securing our Nation's water supply from cyberattacks.

In the course of our work, we paid special attention to our National critical infrastructure and the importance of securing that infrastructure from both criminal and nation state cyber threats.

It is my observation and the commission's observation that the 16 critical infrastructure sectors are not equally equipped when it comes to cyber security. There are leaders, like the financial services sector, and there are, quite frankly, laggers. Despite the importance of our water systems, the water and wastewater infrastructure sector lags behind many of its peers, posing a risk to our public health and safety.

In the report we submitted to Congress in March of 2020, the commission concluded that water utilities remain largely ill-prepared to defend their networks from cyber-enabled disruption. As we've continued our work on approving the Nation's cyber security, bolstering the ability of the water sector to detect, prevent, and withstand cyberattacks has emerged as a crucial priority.

Though 55 percent of utilities responding to a survey conducted by the Water Sector Coordinating Council rated cyber security as a high or top priority, the overall cyber security of our water sector remains immature.

A 2016 National Infrastructure Advisory Council report highlighted the wide disparity in the technical capabilities and resources of water utilities across the Country. Many of our Nation's nearly 70,000 community water and wastewater systems are small, publicly owned assets that are not equipped to deal with nation-state threats, and the National Infrastructure Advisory Council has described the Federal support for the resilience of the water sector as "fragmented and weak."

Municipalities have benefitted greatly from the enhanced efficiency and quality brought by automated and remote systems for treating water supplies, but those same systems introduce new risks when not properly secured, as can often happen when budgets are tight and must be balanced. Investments in security

can fall by the wayside. The Water Sector Coordinating Council reports that 38 percent of utilities dedicated less than 1 percent of their budget to the cybersecurity of information technology, and 44.8 percent allocated less than 1 percent of their budget to the cybersecurity of operational technology. This leaves the water sector vulnerable to nation-state and criminal adversaries and insider threats and gives them the ability to disrupt our critical infrastructure.

Against these threats, the water sector faces challenges ranging from maintaining awareness of threats to assessing risks to identifying and remediating vulnerabilities. A shortage of qualified cybersecurity professionals across the world compounds the problem, making it very difficult for resource-strapped organizations to attract and retain the talent necessary to protect our drinking water and our public health systems.

Earlier this year, for example, the City of Oldsmar, Florida suffered a cyberattack in which malicious actors attempted to change the level of lye in the city's drinking water. Though the attack was quickly detected and stopped, the situation could have been disastrous. In another incident, a malicious cyber actor compromised a California water treatment plant, deleting crucial programs meant to treat drinking water, and in April, Federal prosecutors unsealed a grand jury indictment of a former employee of a Kansas water utility who

remotely tampered with the utility's cleaning and disinfecting procedures. It was through sheer luck that none of these incidents affected customers.

A more sophisticated adversary could impact the safety of thousands of Americans through a cyberattack on our water supply. Beyond the direct impact to drinking water, a cyberattack affecting the water supply could have cascading impacts for other critical infrastructure sectors that rely on clean and safe water to function properly. That is why it is considered a lifeline sector.

These incidents underscore the importance of protecting our water systems and the need for more coordinated, consistent federal action to ensure that water utilities have the people, processes, and technology necessary to protect our public health and safety. Investment in the sector's cybersecurity must match the importance of the sector to our National security, our economy, our public health, and our safety.

With that, I just want to thank you again, Chairman Carper, Ranking Member Capito, and the members of this committee for the opportunity to discuss this pressing issue with you today. We appreciate your attention to this matter, and with that, I would like to turn it over to my Cyberspace Solarium Commission Co-Chair, Senator Angus King.

[The prepared statement of Mr. Gallagher follows:]

Senator Carper. Thank you, Congressman.

Senator King, please proceed.

STATEMENT OF THE HONORABLE ANGUS KING, A UNITED STATES SENATOR FROM THE STATE OF MAINE

Senator King. I once appeared before a middle school group with my friend, Stephen King, the other King from Maine. A little girl raised her hand and said, "Do you ever have nightmares?" Stephen King's response was, "No, I give them to you."

[Laughter.]

Senator King. That is my job today, to give you a nightmare about the vulnerability of our water systems. This is an extremely dangerous situation. I believe that the next Pearl Harbor, the next 9/11, will be cyber. We are facing a vulnerability in all of our systems, but water is one of the most critical and, I think, one of the most vulnerable, and that is why Mike Gallagher and I thought it was important to come and talk to you today.

We have to reimagine conflict. For a thousand years, we have thought of conflict and wars as army against army, navy against navy, battles out in some other place. Conflict now is almost entirely in the cyberspace area, focused on the private sector, on non-combatants, if you will. That is why we are in a different way of thinking about this kind of issue. We have to think about a new relationship between the government, particularly the Federal Government, and the private sector.

Eighty-five percent of the targets in cyberspace are in the private sector.

In this Country, I was on a panel recently with Kevin Mandia, who is one of the real private sector experts. He is the head of FireEye, the guy who really discovered the SolarWinds attack. He said we lived in a cyber glass house in this Country. We are the most wired Country in the world; that is good. But we are also the most vulnerable Country in the World.

North Korea, I don't think, has to worry too much about cyberattacks, because they don't have much in the way of connectivity. Everything in this Country is connected, and water is a target. As Representative Gallagher just mentioned, we know of attacks in Florida, in California, in Kansas. There was a serious one in Israel recently. Wherever there is an automated system for controlling chemical flow, which there is in virtually all water systems, there is a vulnerability.

Our adversaries, be they criminal syndicates or nation states, are never at rest, and Chairman Carper, in his opening statement, talked about how this has to be a sustained effort. There is no single solution. We have got to continue to up our game because our adversaries are upping their game.

In terms of the water systems, we have good news and bad news. The good news is our systems are fragmented and

scattered. In other words, it is not like the electric grid where an adversary could take down a whole region of a country. The bad news is because they are so fragmented, 70,000 of them, rarely do they have the wherewithal or the knowledge to fully protect themselves. So they can be picked off one at a time more easily than the grid, which has a high level of protection and a high level of sophistication.

The Ranking Member knows all about what can happen when a water system goes bad, as it did in Charleston some years ago. It wasn't a cyberattack, but it was a king of warning of what this can mean and how serious it can be for a community.

So, what are the solutions? I should mention that our commission worked, we are still at work, we had our appalling 44th meeting this past Monday, so we are still at it, trying to define what the solutions are. There are federal solutions in terms of organization. We just appointed our first national cyber director two weeks ago. There are a lot of those things that are going on, but in an area like this, protection begins at the desktop.

We could do everything right here in Washington, and goodness knows, we don't, but we could, but still be vulnerable if one official in one desk in Dubuque in the water office clicks on a phishing email, then we are sunk, and that is the danger. There has to be a system of tech support through the

Department of Agriculture, through your programs, tech support for these programs.

There have to be standards, and there has to be testing. There has to be somebody who, if I were running a water system, I would hire an outside group to try to hack me to show whether or not I am vulnerable. Most CIOs say yes, boss, we are okay. I don't think we are, and the only way to determine that is by what is called penetration testing, which is actually hackers for hire, friendly hackers, to determine where your vulnerability lies.

We need to talk about systemically important critical infrastructure and setting up an environment in our report, we called a joint collaborative environment where the private sector and the government can share information in real time with confidence and trust that will enable us to bring to bear the resources of the Federal Government and also to allow the private sector to have some liability protection if they are going to share information and have this relationship, because a week later doesn't work.

To go back to the beginning, there is an incipient nightmare here, and it involves all sectors of our critical infrastructure. But water, I think, is probably the most vulnerable because of the dispersed nature of water systems in the Country.

So I commend this committee for attending to these issues. I look forward to working with you as we try to work through the solutions and to have our game at the level of our adversaries. This is a potential nightmare, but it is one that we can wake up from if indeed we wake up.

Thank you, Mr. Chairman.

[The prepared statement of Senator King follows:]

Senator Carper. We should pay you for coming and testifying. That was terrific. That was just terrific.

Actually, we do pay you for coming and testifying. I would say to Congressman Gallagher, Senator Capito and I love working with your colleagues here on a lot of issues. Whenever I have the opportunity to cosponsor a bill with Angus, I always insist that his name goes first. That way people can describe the legislation as "King Carper."

[Laughter.]

Senator Carper. You think I am kidding.

Senator King. I always talked about it with Tom Cotton, King Cotton.

[Laughter.]

Senator Carper. All right, gentlemen. I know you don't have anything else to do today. No, I know you have got a lot of other things to do. Thank you so much for your leadership on this and for taking time to kick us off this morning. Thank you.

With that, I think our second panel is welcome to take your seats. I think I have had a chance to shake all of your hands this morning. Senator Capito and I have had a chance to personally welcome you. Some of you we know very well, Shailen, and others not as well, but we are delighted that you were able to find time in your schedules to join us. I will take a minute

or two to introduce the witnesses.

First, let me introduce Shailen Bhatt, who is not a native of Colorado. He is not a native of Delaware, but in the past, he has served as Secretary of Transportation for both of those States. We are grateful for his service. I know Hick, we call him Hick, Governor Hick, Senator Hick for whom you work is grateful for your service.

In addition to literally serving as a DOT head at two States, Shailen has also served as Associate Administrator at -- this is impressive; I learned some things I didn't know about Shailen -- he served as Associate Administrator at the Federal Highway Administration. It mentions the Secretary of DelDOT, as well as the Executive Director of the Colorado Department of Transportation. The list goes on. I won't go through everything. Thank you for your extraordinary record of public service.

Let me also introduce Mr. Sullivan. Mr. Sullivan, good to see you. Chief Engineer for the Boston Water and Sewer Commission. Do you have a favorite baseball team? Okay, thank you. Good. I think I know who it is. Mr. Sullivan is a 49-year veteran of the Commission. Is that true?

Mr. Sullivan. Yes, that is correct. I am in my 50th year, and I re-signed up for five more.

Senator Carper. I love that. Anyway, thank you for all

those years of service. I understand you serve on a number of other boards, leading National and regional organizations dedicated to the advancement of water delivery systems and pollution control.

Next, I want to introduce Ms. Oberton. Sophia, welcome. Public Works Department, Special Project Coordinator for the town of Delmar, Delaware. It sits right on, Ben Cardin knows, it sits right on the Delaware-Maryland line. Half of it is Delaware, and half of it is Maryland. We call it Delmar, the town too big for one State.

Ms. Oberton. That is correct.

Senator Carper. There you go. Delaware has a unique jurisdiction, with town departments that provide services to residents on both sides of the Delaware-Maryland State line. Ms. Oberton is a licensed water operator in both States who also serves as the Safety Coordinator for the town of Delmar. Welcome. Which side of the border do you live in?

Ms. Oberton. I live on the Maryland side.

Senator Carper. I am sorry.

[Laughter.]

Senator Carper. The lady's time has expired. Not really.

Finally, I want to introduce Mr. Evan Pratt, the Water Resources Commissioner and Washtenaw -- is it Washtenaw?

Mr. Pratt. Washtenaw, that is correct. The first peoples'

name.

Senator Carper. Oh, good. Washtenaw County, Michigan as Commissioner. Mr. Pratt oversees a range of programs and services, including design, construction, and maintenance of county drains, as well as emergency flood response and maintenance of lake water levels, to name just a few of his many duties.

Mr. Pratt is also the Chair of the Huron River Watershed Council Board of Directors and President of the Michigan Chapter of the American Public Works Association. One of the great thrills of my life was to throw the opening pitch at the Tiger Stadium the last week the Tigers played in Tiger Stadium.

Mr. Pratt. I was at that game.

Senator Carper. It was so exciting. I always wanted to be third baseman for the Tigers, and after I threw the pitch, I went over and I stood on third base, and I said, this is mine, and they closed the stadium that week. It has been some years since they could have used me on third base, but not this year.

Mr. Pratt. I spent six years drinking Mr. Sullivan's water, so I am kind of a Red Sox fan, as well.

Senator Carper. That is good, that is good. We are grateful you are all here. We look forward to an enjoyable hearing and informative hearing, and one that will maybe excite and get us on the right path so we address these really

significant challenges. Shailen, I am going to recognize you first for your statement, and then we will follow in order. Mr. Secretary, Shailen Bhatt?

STATEMENT OF SHAILEN BHATT, PRESIDENT AND CEO OF INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA

Mr. Bhatt. Good morning, Chairman Carper, Ranking Member Capito, and members of the committee. I am honored to be here today. On behalf of ITS America members working to secure transportation assets, thank you for recognizing the growing risk and making cyber security explicitly eligible in the committee's FAST Act Reauthorization bill.

For the past 100 years, surface transportation has primarily consisted of individual, independent vehicles traveling on asphalt. In other words, cars and trucks moving on, over, and through roads, bridges, and tunnels without the benefit of intelligent transportation technologies. Twenty years ago, in addition to causing a tragic loss of life, the 9/11 attacks were a wake-up call that focused our attention on the vulnerabilities of U.S. infrastructure.

When I was with the Kentucky Transportation Cabinet in 2005, we had deployed sensors and CCTV to monitor critical roads and bridges. At that point, data was still largely siloed and fragmented, but soon, these transportation data systems converged. Shortly after that, connected vehicles, along with faster and more reliable broadband entered the equation.

In the last decade, we have seen another convergence: the smartphones and other devices that have been so helpful in our

daily lives were introduced into transportation. State and local transportation agencies began to modernize their informational and operational technologies, overlaying their physical infrastructure with a digital layer. They began to use real-time data and predictive analytics to operate the systems with more efficiency and functionality, which led to safer roads.

Today, we are on the cusp of a digital transformation in transportation. The Internet of Things, electric vehicles, V2X, and other emerging connected vehicle technologies, autonomous and automated technologies, and mobility on demand.

While advances have made the transportation system more connected that ever, this connectivity brings increased cyber risks, and these risks have the potential to threaten the system, the economy, and people's lives.

In the last three years alone, we have seen a 900 percent increase in attacks focused on operational technology use in traffic management signaling systems across the Country. ITS technologies are making our system safer and more efficient by moving people, data, and freight. They support the U.S. economy. We must, however, secure our critical infrastructure assets and manage the vulnerabilities that come with a more complex system. ITS technologies play a critical role across the Country, in cities and suburban and rural areas, and not

just with passenger traffic.

Let me give you an example of the critical role technology plays in supporting our economy. Think about a truck delivering freight from South Carolina's Port of Charleston to West Virginia's capital city of Charleston. Traffic management software efficiently helps to drive or maneuver out of the port and through city traffic.

Automated enforcement allows inspections to happen at 30 miles per hour instead of the driver stopping. Smart truck parking helps the driver find a place to rest and maximizes his or her hours of service. Electronic logging devices collect those hours of service. GPS technology can adjust routing based on weather and traffic information.

These are just a few of these examples of technologies that improve safety and efficiency, and they must all be safeguarded.

Just as we have underinvested in roads, bridges, and tunnels over the last two decades, the same is true for cybersecurity. We have not made the necessary investments to protect our transportation system. Developing a resilient system begins with cyber security. We should take it just as seriously as we do with other industries.

As a former DOT director for two States, I am very familiar with making tough choices about how to spend scarce resources. Public agencies must take an enterprise risk management approach

by assessing and analyzing risks and making decisions accordingly. We recommend a more robust national transportation cyber security strategy to make the digital layer of our transportation system safer, much like how Vision Zero makes our fiscal infrastructure safer.

We can do this by ensuring transportation agencies meet certain marks determined by the National Institute of Standards and Technology and the Center for Internet Security. We should treat cyber security like other safety programs, funded at 100 percent and provide technical assistance and best practices. In addition, we should help rural transportation agencies and areas of persistent poverty or income inequality, and let's allow flexibility in how transportation funds are used to invest in future cyber security workforce capacity.

This is a critical opportunity. We have a playbook. If we provide the necessary resources, we can level the playing field and create a more safe and secure transportation network. We should give cyber security the same level of support that we give other safety programs. DOTs need resources to shore up their infrastructure.

Thank you again for the opportunity to testify today. I look forward to answering any questions you may have.

[The prepared statement of Mr. Bhatt follows:]

Senator Carper. Thank you, Secretary Bhatt.

Now, we are going to turn to Mr. Sullivan to provide his testimony. Ms. Oberton, you are batting on deck. Go ahead, Mr. Sullivan.

STATEMENT OF JOHN SULLIVAN, CHIEF ENGINEER, BOSTON WATER AND SEWER COMMISSION

Mr. Sullivan. Thank you, Chairman Carper, Ranking Member Capito, and members of the committee. Thank you for the opportunity to testify on cyber security challenges facing the Nation's critical infrastructure.

I am John Sullivan, Chief Engineer of the Boston Water and Sewer Commission. The commission is the largest and oldest water system of its kind in New England and provides drinking water and sewer services to more than one million people daily.

Today, I am testifying on behalf of the Association of Metropolitan Water Agencies, or AMWA, which is an organization representing the Nation's largest publicly owned drinking water systems. AMWA's members collectively serve more than 156 million Americans with quality drinking water.

In addition to serving on the boards of AMWA and other State and National groups as well as on the Water Sector Coordinating Council, I also chair the Water Sector's Information Sharing and Analysis Center, better known as the WaterISAC. AMWA operates WaterISAC on behalf of the water sector. It is a non-profit organization established in 2002 by national water and wastewater associations at the urging of EPA and the FBI to provide utilities with critical information on physical and cyber security threats and best practices for

prevention and response.

WaterISAC members currently serve 203 million people across the United States. While EPA and Congress provided some funding to get the service up and running, today, member dues support 100 percent of the WaterISAC's budget. We know that water utilities pose attractive targets for cyber attackers.

We are all aware of the well-publicized intrusion against the water utility serving Oldsmar, Florida earlier this year. While utility staff immediately observed the breach and took corrective action to prevent any impacts to water quality or public health, it is easy to imagine how the outcome could have been much worse.

The Boston Water and Sewer Commission had its own experience with a cyber security incident last year in the form of a ransomware attack. While it complicated day-to-day business and was costly to recover from, there was never any threat to public or environmental health due to precautions such as our business network being segregated from our control system. This is the best practice in any sector that uses industrial control systems, but this approach is not consistent across the sector of 50,000 drinking water systems and 16,000 wastewater systems.

With such a large universal water system across the Country, many are bound to have a lack of understanding of these

cyber best practices or a lack of expertise and equipment to implement them. This is where the WaterISAC can help. In Boston's case, the center was instrumental in our recovery from our incident. ISAC referred us to a firm specializing in ransomware incident response, which helped us navigate our way through the even. Expanding the reach of the WaterISAC would therefore enable more water systems to be better prepared to respond to their own incidents.

As Congress thinks about new oversight of cybersecurity at water utilities and critical infrastructure more broadly, we support an approach that incorporates the advice of subject matter experts from the water sector, as well as lessons learned from other sectors. The nature of cyber threats is they are revolving, and a binding requirement that makes sense with today's technology could quickly become outdated in years ahead.

Any regulatory oversight of the cyber sector and cyber activities must therefore remain as nimble as possible. One promising model for legislation could be found in the Energy Infrastructure Act approved by the Senate Energy and Natural Resources Committee last week. That proposal would encourage water utilities to bolster their cyber preparations and would seek to increase participation in the Electricity Information Sharing and Analysis Center, WaterISAC's counterpart for the electric sector.

A similar direction for the water sector would have EPA take steps to bolster water sector participation in the WaterISAC, especially among systems serving fewer than 100,000 people. This would help us get threat information and best practices into the hands of more small systems across the Country.

In closing, I want to note that my written testimony offers some feedback on water sector cyber security provisions in Senate 914, the Drinking Water and Wastewater Infrastructure Act approved by the Senate this spring. While AMWA believes these provisions were well-intentioned, we have identified a number of issues that could prevent the proposal from working as envisioned in its current form. We would be happy to work with you to address these issues.

Thank you for the chance to testify today, and I am happy to answer any questions.

[The prepared statement of Mr. Sullivan follows:]

Senator Carper. Mr. Sullivan, thank you, and thank you for your extraordinary service. Forty-nine years, that is very impressive.

Ms. Oberton, please.

STATEMENT OF SOPHIA OBERTON, SPECIAL PROJECTS COORDINATOR, DELMAR PUBLIC WORKS DEPARTMENT

Ms. Oberton. Good morning, Chairman Carper, Senator Cardin, and members of the committee. I am Sophia Oberton, the Special Projects Coordinator with the Town of Delmar in Delaware and Maryland. We have a population of approximately 4,500 persons.

I hold a Class 4 drinking water operators' license in both Delaware in Maryland. In addition to managing the town's public drinking water supply, I am also the town's Safety Coordinator.

I am honored to testify here today on behalf of small and rural communities in the United States through my affiliations with Delaware, Maryland, and National Rural Water Associations. I am joined by my mother, Mrs. Linda Anderson, and the Town of Delmar's Town Manager, Mrs. Sara Bynum-King.

Senator Carper. Could your mother just raise her hand? Ms. Anderson, thank you. I was going to see if we could see her lips move when you spoke, but that would be a lie.

[Laughter.]

Senator Carper. She is wearing that mask.

Ms. Oberton. Before getting into the substance of my comments, I want to personally thank Senator Carper and Senator Cardin for being such good friends and supporters of rural Delaware, Maryland, and rural USA. The rural and small-town

provisions in your recent legislation, DWWIA 2021, are very much appreciated. Senator Carper, you made us so proud when you chose to announce the legislation at Delaware Rural Water Association headquarters in Milford in April.

The Town of Delmar would like to sincerely thank Congress for the funding we received under the American Rescue Plan Act. We received $3.7 million for the entire town. Much of this funding will be earmarked for water and sewer projects.

My main messages here today regarding cyber security protection of small and rural communities' public drinking water infrastructure is, first, small communities only operate to serve the public interest. We are owned and governed by our local citizens through the elected local government. We only exist to serve the public and are eager to take all feasible and necessary actions to protect the cyber security of our public drinking water supplies.

Second, most U.S. community water systems are small, like my Town of Delmar. Ninety-one percent of the Country's just under 50,000 Community Water Systems serve populations less than 10,000 persons. Eighty-nine percent serve populations less than 3,300 persons. That means approximately 90 percent of the Country's public water supplies are smaller than my town, and I am about to explain the rudimentary nature of Delmar's water cyber security.

However, any successful cyberattack on a small community that results in drinking water contamination would cause psychological panic in a national scale. This is why small communities believe that protecting our water supplies from any cyberattack is just as important as protecting large communities.

In Delmar, we don't have a SCADA control system or interface with the internet regarding our water infrastructure. On the other hand, we do have automated well pumps, disinfection injection, corrosion control technology, and pressure monitoring systems. If one of the water treatment technologies is not functioning properly, we receive an alarm message on our cell phone, and we must get to the appropriate part of the treatment facility to directly adjust the system.

We want the committee to know that when towns like Delmar need help in operating our water utilities, understanding new and complex Federal water requirements, receiving the required training to maintain our licenses, and learning about the latest cyber security practices, we call on our rural water associates and ask for assistance from their circuit rider technical assistance providers. These circuit riders will travel directly to our town and focus on our particular issue with our specific water utilities.

Just this past April, a circuit rider from Delaware Rural

Water and another from Maryland Rural Water came to Delmar and spent the entire day helping us complete the very complicated EPA mandated risk assessment. I can't imagine how many days this approximately 50-page assessment would have taken us to complete without the direct technical assistance of the circuit riders. We may have been forced to pay a consulting engineer to complete the assessment for us, which would likely cost over $10,000, a massive unplanned expenditure for a town our size.

Our greatest threat identified within the EPA assessment is likely the physical disruption of the water supply. However, our most significant issue from our perspective is the lack of personnel to operate and maintain the public water supply, fulfill the mandatory compliance testing and reporting, and respond to the typical small-scale emergencies in the water system, such as line breaks and leaks.

We also need to replace our old and failing terracotta sewer lines, which are causing a severe I&I problem for the wastewater utility. The reality is that small towns have limited financial resources, which must be targeted to meet our greatest needs. Any cyber security program should be scalable, meaning it must recognize the complexity of water cyber security systems in small communities like Delmar is not remotely similar to a large community.

In closing, Mr. Chairman, I want to thank you again on

behalf of small and rural water communities for your continued help and assistance.

[The prepared statement of Ms. Oberton follows:]

Senator Carper. What is I&I?

Ms. Oberton. I&I is the inflow and infrastructure of water going into our sewer systems from manholes and our old terracotta pipes.

Senator Carper. Thank you. Okey-doke. Thank you for your testimony. Thanks so much for joining us.

Ms. Oberton. Thank you.

Senator Carper. Senator Cardin, I am sure he will want to welcome you personally when he is able to join us in a little bit.

I think that takes us to Mr. Pratt. Evan, we used to have a Congressman, a Senator named Evan, and a governor named Evan Bayh. It is a great name, great calling.

I am happy you are here. Welcome. Please proceed.

STATEMENT OF EVAN PRATT, MEMBER OF GOVERNMENT AFFAIRS COMMITTEE, AMERICAN PUBLIC WORKS ASSOCIATION

Mr. Pratt. Thank you very much, Chair Carper, Ranking Member Capito, and members of the committee. I am Mr. Pratt. On behalf of the American Public Works Association and our more than 30,000 members across America, I do appreciate the opportunity to provide this testimony today with some wonderful peers at this important hearing on cyber security vulnerability for America's physical infrastructure.

As background, I spent my career in public infrastructure. I have a fancy degree from MIT, and I have been a licensed engineer for 30 years.

Senator Carper. What was your degree in? What was it, engineering?

Mr. Pratt. Civil and environmental engineering.

Senator Carper. We have a mechanic in our family from there.

Mr. Pratt. Oh, there you go.

Senator Carper. I can barely spell MIT. To have a kid go there is pretty amazing.

Mr. Pratt. Just remember, it is TIM backwards in the mirror.

Senator Carper. That is great; that helps a lot.

Mr. Pratt. Little mnemonic device, right?

I am a frontline person. I currently serve as the Water Resources Commissioner for Washtenaw County, Michigan with about 370,000 people. But today, I am testifying on behalf of APWA, the only association to serve and represent all areas of public works, both public and private sector and providing expertise at the local, State, and federal levels. A lot of smarter people than me, I would say.

Cyber security is an increasingly important part of protecting our critical infrastructure assets and our citizens, and I am embarrassed to say today, I am here because I and many of my peers know we are behind on cyber security, and we need help from you. You are going to hear some things that Representative Gallagher said, and I don't think either of us hacked into our systems to steal our speeches, but boy, he had a lot to say, and he is right here.

We are first responders in public works. We embrace our responsibilities on the front line preparing for, responding to, and recovering from disasters, all while protecting that critical infrastructure that is out there. I think you all understand critical infrastructures is the roads and the bridges, sewer plants, water plants, flood control devices, drainage systems, and, of course, the cyber systems that are sometimes used as controls to operate these. For the purposes of today's hearing, I kind of want to focus on that area.

We heard about the industrial controls in the water business. They are known as SCADA systems, which stands for Supervisory Control And Data Acquisition. We use this stuff to manage systems and to make decisions, so it is pretty important to a lot of systems.

We all know flood control systems are critical too, from mitigating severe weather, and it is essential for Congress to consider shared strategies to save our communities from potential attacks on these increasingly automated and connected systems. As we do appreciate, as many have thanked you, Congress can and has supported America's critical infrastructure through continued and flexible Federal funding, financing, and regulatory streamlining to help ensure that our agencies have the resources to protect against cybercrime.

In 2016, 17, I was part of a governor's bipartisan task force to assess the condition and funding needs of all infrastructure in the State of Michigan using a RiskLens. To be clear, the overall purpose of the report was to bring that ROI that infrastructure brings right into focus, right to our State economy and to community quality of life, and that report is still used today, but there was not a single recommendation about cyber security, nor did we ever discuss it in talking about all the needs for infrastructure.

The bottom line is, we are trying to play catch-up right

now, and again, I will talk a little bit later about where we could get help.

As Sophia said, I have learned and observed since then. Cyber security is a big issue. On the one hand, not all utilities have remote sensing and controls. On the other, the wide range of SCADA solutions for the many who do may result in weak points when deployed, particularly with varied levels of agency cyber awareness that you have heard about today, and even more especially in the very common situation where agencies like mine can only meet their SCADA needs by stitching together several different tools, having homemade applications. And then there is gentleman or lady who is on call at home, and they might be operating this from a bring-your-own device type of situation. My county will give people $80 a months for the phone, and you are on call, and you got to operate the system. That is how you are going to be doing it, so you can picture, there is a lot of, the more hand-offs, the more fumbles, let's just say how that goes.

At the end of the day, you have heard about the Nation having its fair share of attacks, whether it is SolarWinds, Colonial Pipeline, or other intrusions attacking those SCADA systems like Oldsmar and Post Rock, Kansas that have been talked about today. I would just like to summarize the risk. You have heard about the 50,000 water systems, nearly 70,000 water and

sewer plants across the U.S. I will say that again: that is 70,000. I don't know what .1 percent is of that, even though I got a fancy degree, but it is a number that affects people, like in Delmar. One of those goes bad, and as was mentioned, that can cause nationwide panic, just with one of those 70,000 systems, so there is a lot of vulnerability there.

In closing, APWA recommends the following, and again, we appreciate this committee has supported many of these things. First, the Federal Government must share threat information and provide inter-agency technical support, perhaps by establishing voluntary national cybersecurity guidelines, something to supplement the Water Rights Act that has been talked about.

Second, let's standardize and utilize important tools to protect these critical areas, including SCADA systems. Third, comprehensive cybersecurity training for old guys like me and my peers is really essential. That is something that we need to have more of out there so the awareness is greater.

Fourth, please continue to fully fund FEMA's Emergency Management Performance Grant Program. Fifth, let's encourage effective asset management strategies to help deliver best taxpayer value. That is why we use these controls, because we can more efficiently operate these systems and get more bang for the buck.

Sixth, let's continue to ensure that cybersecurity is

specifically eligible for all the funding this wonderful committee provides. My agency has a history of more than 30 revolving loan funds for resilience and flood control, water quality, infiltration, and all of that.

Our seventh thing is to basically lift that cap on private activity bonds for water infrastructure and restore advanced refunding of tax-exempt municipal bonds. This helps both local cybersecurity funding as well as taxpayers when we can get better interest rates.

My last one that APWA requests is, I hope Congress continues to ensure State and local control regarding public works projects. Locals are experts on their community needs.

We do thank this committee for holding this important hearing and allowing me to provide testimony and, like everyone here has said, APWA stands by ready to help, however you need us. Thank you.

[The prepared statement of Mr. Pratt follows:]

Senator Carper. That was great. Thank you so much, Mr. Pratt.

Senator Capito is going to lead us off on our questioning, so shall we?

Senator Capito. Thank you. Thank you, Mr. Chairman. Thank all of you. Very interesting.

I want to start with just kind of a quick question to Ms. Oberton. You mentioned in your testimony that you hold a Class 4 Drinking Water Operators License in Delaware and Maryland. Is there any cybersecurity training that goes along with obtaining one of those licenses?

Ms. Oberton. None.

Senator Capito. None. So there is a gap right there, and that is probably, I don't know, Mr. Bhatt, or maybe Mr. Pratt, do you know other licenses, other levels, is there ever any cyber training that goes along with any of the licensors?

Mr. Pratt. I have gone to lots of training; I have given lots of training with various professional organizations. I have never attended a cybersecurity class, and I can't recall seeing one on an agenda. Perhaps they are out there, but it is not typically required in licensure situations that I am familiar with. I don't know everything, but it is rare today.

Senator Capito. Okay. Let me ask too, then, another basic question, Mr. Sullivan or Ms. Oberton, and Mr. Pratt would

probably know this issue from operating local systems. If you were to see that a cyberattack is occurring, or you made note, you had the ransomware attack, right?

Who do you go to first? Do you go to Homeland Security, do you go to your State? I know you went to your -- I can't remember what the organization was that helped you solve your problem, but is there a response that is laid out for you to be able to react to something like that?

Mr. Sullivan. Under AWEA, we had already had an emergency plan, should we be attacked. We received on all printers at 3:00 in the morning, every printer printed out the ransomware demand of $2 million and told us that we were encrypted.

We immediately shut down the entire system. We notified the FBI immediately; we notified the EPA; we notified our State.

Senator Capito. FBI, EPA, and your State.

Mr. Sullivan. We turned to the WaterISAC to say, we were just attacked. What do you do? Who are the experts? Because cyber is a different thing. None of us have trained in it. All of us know about it; we know about the threats and all that, but what to do?

So, there are experts out there, and we were able to immediately contact the ISAC, who knew of companies that immediately came in and helped us bail out.

Senator Capito. Ms. Oberton, if you were to get sent

something, get something on your printer at 3:00 o'clock in the morning, who would you go to first?

Ms. Oberton. I think we would contact our State and local governments. It is not necessarily like this gentleman said, Mr. Sullivan said, it is not directly laid out. It is not a training that we have had, or hopefully it is coming forward to let's know as a small and rural area.

Senator Capito. Right, which is my entire State.

Let me ask you this: you mentioned the Circuit Rider Program, which is great for our States.

Ms. Oberton. Yes, absolutely.

Senator Capito. Did they have any expertise, or did they bring anything to you on cyber security?

Ms. Oberton. Not as of yet. But the tons of educational information, I am sure that is coming down the pipeline.

Senator Capito. Yes. Mr. Pratt, do you have anything? Where would you go if you were attacked?

Mr. Pratt. FBI first, and the WaterISAC, plus our State has some support in that area. I do want to echo what Representative Gallagher said, though. Many government agencies have historically viewed IT infrastructure as an optional buy-out versus necessary investment. We are playing catch-up, and that SCADA marketplace is much less mature on cyber security than say, I had it written down, the financial or medical

software market.

My county was hacked, not in our control systems, but they got in and got some HIPAA records from an internal type of pathway, and we have had a Chief Information Security Officer since that time. Fortunately, I was able to speak with him prior to coming here to get his insight on things. But FBI, WaterISAC, and State SSO Agency.

Senator Capito. Mr. Bhatt, let's talk about transportation a little bit because I think, obviously, with autonomous vehicles and electric vehicles, I mean actually, I saw, I call it a lamppost. It was an enormous post that they were going to be installing along one of our major arteries interstates, and my husband looked over, and he was like, what is on the top of that? It was some kind of sensor.

I don't know what it was. It could have been a weather sensor; it could have been a who-knows-what, but it was something tied to the internet. It was pretty obvious there. I think that we are going to see this more and more. It may have been something to sensitize when and how often the light went off and on or whatever.

In transportation, where would a transportation facility go? Because I am the Ranking Member on Homeland Security, on the Appropriations Committee. There is an organization there, SISA, that is supposed to be helping all State and local in a

lot of areas in terms of cyber security. We are putting a lot of money into that, because I think this could help our Circuit Riders, it could help our State and locals, it could help everybody. But where would you go in a transportation incident?

Mr. Bhatt. So, I think that you have correctly identified the major vulnerabilities, and many vulnerabilities that exist, because as we introduce more of these sensor systems, active traffic management, VMS signs, variable message board signs, closed circuit television cameras, tolling systems, these are all potential vectors, or entry points.

You want to delineate between operational technologies, vulnerabilities, like I just listed out, the IT, that is in there where somebody was opening up a phishing email, and then all the data that is out there.

Colorado DOT experienced a ransomware attack. The playbook there was to go to the State resources first, but it quickly became apparent that it was a state-sponsored attack. So we had to bring in Federal resources from Colorado Springs, or they did; I was not there at that time, but from Colorado Springs and other places.

So I think that that is one of the reasons for providing federal support, to bring all of these States and other transportation agencies up to a level playing field, so no matter whether you are the most sophisticated State or one that

is just discovering this, you kind of know exactly where to go.

Senator Capito. Thank you.

Senator Carper. Thank you. Senator Whitehouse, thanks for joining us.

Senator Whitehouse. Thank you, Chairman. Thanks to all the witnesses for being here.

Just a quick opening question. Ms. Oberton, what federal standards must Delmar adhere to with regard to cybersecurity?

Ms. Oberton. Whatever is put out there for us to follow. We don't have any specific standards at this point for cyber security.

Senator Whitehouse. I think that is my point, thank you.

Ms. Oberton. Yes

Senator Whitehouse. Mr. Sullivan, Boston Water, what federal standards are you obliged to follow regarding cyber security?

Mr. Sullivan. The only federal requirement was we needed the follow AWEA, and we needed to self-certify that we looked at our systems, we came up with a plan. That is the only standards that I know of.

Senator Whitehouse. Mr. Pratt, your county?

Mr. Pratt. No mandates.

Senator Whitehouse. I think that is a pretty open situation. My view of this is that the Federal Government, by

and large, has done a pretty good job of defending its cyber systems. When there is a hack, it is a big one, because we have boatloads of info, but by and large, federal agencies have been fairly good.

The Defense Industrial Base has done quite a good job at defending itself, because it is put under immense pressure by the Department of Defense to make sure that it does defend itself. The financial system is heavily regulated, and as a result, the financial system has done a very good job of defending itself.

Local government has very mixed views. The Town of East Greenwich in Rhode Island sustained a ransomware hack, but it was prepared. They quickly shut down their systems. They had backups that were current that they could roll right in quickly. They had a disaster recovery plan, and it took a lot of work, but they were able to pay no ransom and get back up and operating and lose no data because they were prepared. Paid no ransom because they were prepared.

One of the reasons they were able to do that was because another Rhode Island municipality had very bad luck, and it had to pay. Our Rhode Island State Police Cyber Unit did a very good job of going and banging on the doors of our 39 municipalities and saying, look guys, this just happened. Everybody has to be ready. So that change happened, and East

Greenwich was ready and did a very, very good job.

The worst place in the Country that I can think of right now is privately owned critical infrastructure because they have successfully defended against being under anything other than the voluntary NIST Framework Program, which is totally voluntary.

It is immensely frustrating to me, having worked in this space since my time on the Intelligence Committee a long time ago, that we have known about ransomware for over a decade, right? We have known that critical infrastructure was the prime target for cyber hackers for more than a decade. We spent billions of dollars to defend critical infrastructure through Homeland Security, through the Department of Defense and other places, and what did we get? We got a ransomware attack on critical infrastructure, and it succeeded. Why people didn't get fired over that, I do not know.

But part of the deal has to be that we have got to be less reticent about a company's critical infrastructure, making sure that they are doing their job of defending themselves. We can't just have the Chamber of Commerce, the U.S. Chamber of Commerce come in here and say, no, we are against all this stuff, and roll over backwards when it is critical infrastructure.

So, you guys are kind of in the middle. You are not privately owned, but you are not much supported, either with

resources or with regulations. I hope very much that in this committee, we will start to develop things that will help you work through this, so you are more like East Greenwich when you get hit. It sounds, Mr. Sullivan, like you all did a pretty good job of getting back online.

Mr. Sullivan. We did not pay any ransom. We immediately shut down. We didn't even communicate with them, and we sought the resources, but we had a plan already, because we were required to do that. The problem we have, we got the ransomware because an employee opened up an email, despite the training we had, and it takes constant training. That is the biggest problem for the large utilities. Cyber security, the element of people watching out all the time. Everyone assumes that email comes in, it looks good, let's open this attachment.

Senator Whitehouse. You click the attachment, and immediately they are in.

Mr. Sullivan. Yes.

Senator Whitehouse. Yes. If I could mention just one additional thing that doesn't really bear on this committee, but I am hoping we can get it done bipartisan and maybe even by unanimous consent.

Senator Graham, Senator Tillis, Senator Blumenthal and I have a bill to help with criminal enforcement of people who attack our critical infrastructure. It makes hacking qualify

for a bunch of predicates, like RICO and money laundering, and so forth. It deals with bots and botnets. In my view, there is no good bot, and there is no good botnet, but the authority to go after them before they become --

Senator Carper. Maybe a Shailen Bhatt?

Senator Whitehouse. -- before they become, sorry, B-O-T, not B-H-A-T-T, but the authority to go after them before they become actively harmful is unclear, and we need to fix that.

We have a bunch of enhanced penalties that we could add once people go after critical infrastructure. I am hoping that is something that we can move quickly, unless there is some, like, botnet caucus out there that I haven't heard about. These are things that the Department of Justice has long asked for and would provide some additional backstopping for all of you, because there is nothing like people going to jail to help knock behavior down.

Thank you, Chairman, for drawing our attention to this. Thank you to the Ranking Member for making this a good bipartisan hearing, and I look forward to working with you all on this subject. Terrific witnesses.

Senator Carper. Thank you, Senator Whitehouse. You spent a lot of time on this, and we appreciate it very much.

Mr. Pratt, I think you shared with us eight or nine recommendations from the APWA. Did you do that in your

testimony?

Mr. Pratt. We will be providing those in writing. Are you saying you would like to hear them again?

Senator Carper. No, no. You already went through them.

Let me just ask of our other witnesses, I think that may be the first time I have heard those, are you all familiar with what he shared with us, the eight, I think there are eight PWA recommendations that were part of your testimony? I'm just asking if you are familiar with those recommendations.

Maybe it is something you are familiar with, maybe not. Anybody? Ms. Oberton, is this something that has come to your attention?

Ms. Oberton. No, not to my attention.

Senator Carper. Okay. Mr. Sullivan?

Mr. Sullivan. I heard them, and I would like to add that there needs to be funding for the small systems. There is too much pressure between our problems with PFAS, with affordability issues, and the intensity of existing regulations. People can say they have a problem with their cyber. They need a way to fix them. The smaller ones have the biggest problems.

Senator Carper. Thank you. Secretary Bhatt, is this something you have heard of?

Mr. Bhatt. Yes. Obviously, from an APWA perspective, it is not a direct analog for transportation, but many of the same

principles on the SCADA devices, when he was talking about the bring-your-own device, this is an issue that affects all of these industries. So as I was listening, I was thinking, there are a lot of items that we could also support from that as well for transportation.

Senator Carper. Mr. Pratt, would you just walk through those recommendations and I add that they are very good.

Mr. Pratt. I am happy to go through them one more time, just to note that our association president and our government affairs staff are here and have traded cards with each of the organizations that these folks represent. We totally understand that we want to be singing from the same hymnal.

So, the first was to have the Federal Government sharing threat information and providing interagency technical support to local governments to enhance cyber security, perhaps by establishing Voluntary National Cybersecurity Guidelines. That would help us with that certification and including public works folks and all these organizations and crafting those to supplement that WaterISAC.

The second one was to standardize and utilize important tools to protect these critical assets, so we use that CyberLens to maybe get a little more consolidation in that SCADA industry. Third was comprehensive cyber security training for me and my peers. I believe this is essential, because again, this has

been said. This is not a thing that no matter how good we are at our technical jobs, at physical infrastructure, this is just as new to us as any of you here. We all are trying to hire young staffers.

Fourth, please continue to fully fund FEMA's Emergency Management Performance Grant Program. Fifth, let's continue to support asset management. So, that really is something that can be done with revolving loan funds. We want to deliver that best taxpayer value when we do make infrastructure investments, and we want to absolutely make sure that my seventh one was related to that, that cybersecurity is fundable in any program that flows through this wonderful committee.

The sixth one was talking about that specifically, I guess, so I had those back to back. I am sorry. My seventh one was more related to taxpayer value. APWA does support lifting the cap on private activity bonds for water infrastructure and restoring the advanced refunding of tax-exempt municipal bonds.

Again, that will help give us a little bit better interest rates and provide a little more space for that cybersecurity piece of things. Whether that should be 2 percent or 1 percent, I am not an expert, but it needs to be something percent, right, when we invest in intelligence systems.

My last one was just that we hope Congress continues to ensure State and local control regarding public works projects,

because locals are experts on their community needs. I am very sympathetic to Senator Whitehouse's point of perhaps a little bit better checking on how we are doing with cybersecurity, and do we know what we are supposed to be doing. I appreciate the opportunity to restate that.

Senator Carper. That was worth hearing again, and thank you for sharing it with us.

Anybody want to react here, any of the other three witnesses want to react to anything that he has mentioned in those nine recommendations, please? Secretary Bhatt?

Mr. Bhatt. Yes, in hearing them again, I think the one thing that jumped out at me that I think is shared from infrastructure from an infrastructure owner-operator perspective, as many of the transportation agencies are, was the comprehensive cyber training. We talk a lot about workforce in transportation and making sure that we are training people to create a culture of cybersecurity within State DOTs and other transportation agencies.

I think that is something that would be valuable to share across all organizations, because we are already tasking them to be responsible for whatever their core mission is. You can't just then say, in addition to that, also be mindful of cybersecurity. You have got to train them; you have got to create that culture, and so I think that was something that

really resonated, as well.

Senator Carper. Thank you. Any other reactions? Ms. Oberton, and then Mr. Sullivan.

Ms. Oberton. In saying that, I would also just say that remember that rural water, these smaller communities, most don't have the opportunity to get the information. So making sure that we hit these small mom-and-pop communities, like the trailer parks and things, making sure that even though we say funding and low interest rates, they may not be able to afford that.

So cybersecurity and training and everything that is necessary should be affordable to them, if not at a free cost, as our Delaware Rural Water, Maryland Rural Water, and National Rural Waters provide that training.

Senator Carper. Good. Thank you.

Mr. Sullivan, any thought?

Mr. Sullivan. Yes. There are some excellent sources out there. SISA puts out unbelievable stuff. Yesterday, we were alerted that they put another item up on the website about industrial control systems. The problem is people don't have time to go to all these sources and collect them all and see if it pertains to their particular system, which is the reason that I have been emphasizing the WaterISAC can collect all this. It partners with everybody: EPA, SISA, all Federal Government, all

the associations.

We can consolidate, and we can get it to the smaller systems, telling them what is important for them, because it is important that we weed out some of this extraneous stuff. There is so much information out there that our analyst could take a look at it, bring it down, and get it to them. We would just need funding so that we can get to these particular systems, because they can't afford to join the WaterISAC.

Senator Carper. Thank you. We have been joined by Senator Padilla. He hails from a State, a big State where I used to live when I was in the Navy, and we are honored that he joined us in the Senate and on this committee. Senator Padilla, you are right on time. Go ahead.

Senator Padilla. Thank you, Mr. Chairman. I appreciate the discussion.

I am going to continue in a minute, here, on the cyber theme that we are discussing right now, but just a little bit of a preface. As the former Secretary of State from California, I am all too familiar with the risks posed by cyberattacks and the importance of security and modernization of our critical infrastructure, whether it is voting systems or water systems, transportation systems, et cetera.

Unfortunately, we are getting constant reminders of not just the importance, but the urgency with which we need to act.

Just last month, a hacker accessed a computer system of a water treatment plant in California and deleted several programs that are designed and put in place to treat drinking water. Thankfully, the hack did not result in harm to the public, but again, the most recent reminder of the importance and the urgency with which we need to act.

SolarWinds was not that long ago, the Colonial Pipeline, on and on and on. We have begun the discussion, but if I can ask just Mr. Sullivan maybe, for a few more thoughts on what role should municipalities play in preparing their employees for this now constant stream of phishing emails and now texts, phishing text messages, other efforts to undermine security systems that are in place and what else the Federal Government can do.

I heard you reference SISA. If there is anything else that they are not doing that you think they could or should be doing to add value for State and local governments or system operators, that would be helpful.

Mr. Sullivan. I think the most important thing is that they have to play a role in testing with their own employees, what happens if we were attacked, if this is shut down. Who do you contact, how do you contact them.

One of the things that goes on at our facility now is that randomly, each week, 20 employees get phishing emails from the IT department, and we test to see who hits them. Invariably,

somebody opens up an email, and they do very well at massaging them, making them look real. Some of them look like they are bank accounts, some of them look like you just won a prize, some of them, and yet people still fall for it.

So, one of the things that has to be done is the culture that cyber is very important, and you can bring down an entire city if you are not careful.

We also now limit what people can do at their computers. We used to be wide open. People would bring in their own USBs, hook them in, download. You can't do that anymore. We totally shut that off. We do not allow people to use their own private phones in order to access anything, which we used to before. That is shut down. You have got to use a commission; it has got double authentication on it. So we have really tightened it up.

Senator Padilla. Even some of those latter dynamics, complicated by the COVID pandemic, with more remote working, for example, so whether it is a personal device versus an official device, how you are accessing private networks, et cetera. Cyber hygiene, constant training of employees, these tabletop exercises led by DHS in the election space, we found tremendously helpful and important.

Like you are saying, running through simulation exercises, what-if, what-if, what-if, so that staff, top to bottom is best prepared in the event of a threat or the event of an actual

incident.

I don't mean to cut you off, but in my limited time, I raise a specific question as it pertains to some of the smaller and rural systems, particularly in the water in different parts of the Country. Organizations like the Rural Community Assistance Corporation, which is a non-profit organization based in West Sacramento, provides training and technical assistance to Tribal and rural communities across California and in 13 other Western States. Small and rural water systems face particular challenges in operating water systems, since income from a small population of ratepayers may not be enough to cover the actual providing the water service itself, let alone a robust cyber security infrastructure.

So, these challenges are obviously compounded by the drastic reduction in federal funding in water infrastructure over the course of several years.

Ms. Oberton, how can Congress ensure small and rural water systems are not left behind, and that under-served communities served by these systems are also protected from cyber threats?

Ms. Oberton. I think by making sure that the information is out there. Again, I speak to the small, small rural areas like we live in. If we know it is there and the training is available and easily funded, then it won't be such a burden for our rural community.

Sometimes, we have people that have a trailer park, like I spoke earlier. You have a community of 25 or 30 people, but they don't get the information like we get it. So it is very important that however we get it out there, those communities and our small communities are recognized. We do that through our Rural Water Associations.

Senator Padilla. Mr. Chairman, I know my time has expired. If I could just squeeze in one more question about transportation.

Senator Carper. No, I can't. I am sorry. I skipped over Senator Boozman, and I will come back to you soon, but he needs to be someplace else, so if you will just let.

Senator Boozman. Mr. Chairman, it is okay, go ahead.

Senator Carper. Are you sure? All right, go ahead. Just briefly please, thank you.

Senator Padilla. I just want to recognize that continued research development and deployment of smart infrastructure and automated vehicle technologies has the potential to save lives, to reduce congestion and emissions and improve equity and economic growth. When I was in the State Senate in California, I authored the law to provide for the safe operation of autonomous vehicles in California, but we have also seen an increase in connected transportation system raise new challenges, like cyber threats.

As with other sectors, we must ensure that transportation agencies are equipped to handle these threats and prevent disruptions to critical infrastructure. Mr. Bhatt, given your experience as a State and Federal official, what resources do transportation agencies uniquely need to protect infrastructure from these threats and to promote a safer, cleaner, more efficient transportation system?

Mr. Bhatt. Thank you, Senator Padilla. In fact, all of your words are consistent with the mission of our organization at ITS America, and in fact, California Department of Transportation, CalSTA is a member. David Kim, Secretary Kim, sits on our board of directors.

I think what is really important in terms of what is needed is just getting all of the States, all of the agencies up to the standards so that everybody is on a level playing field, because you can't have a vehicle, whether it is driven by a human or in the future, autonomous vehicles, drive from California to New York and go through 20 different jurisdictions and have 20 different protocols. So I think that what would be great from a Federal perspective is the funding.

I have had lots of conversations with USDOT. I think they get the severity. The President had an executive order on cyber security. Committees like EPW are showing the importance of cyber security in infrastructure. I think there is the

opportunity for leadership, and then providing the funding because State DOTs have so many other things that they have to do that you can't make cybersecurity one of the things that they have to pick between. You have got to provide the funding, and I really appreciate the efforts of this committee to make that funding eligible.

Senator Carper. Thank you, Senator Padilla. Senator Boozman, please excuse me for skipping over you. You are very kind. Thank you for being so gracious.

Senator Boozman. Thank you. Oh, no, Mr. Chairman. I apologize for being late

Senator Carper. You are recognized for the next 30 minutes.

[Laughter.]

Senator Boozman. I apologize for being late and having to sneak out. There are about six hearings going on all at the same time right now, but thank you, Mr. Chairman, for having this really important, timely hearing.

Senator Carper. I wish I could say it was my idea. It was actually Senator Capito's idea, so we are happy you are here.

Senator Boozman. Well, it is a joint venture.

Mr. Sullivan, in your testimony, you stated the larger utilities with more resources have fewer challenges to implement cyber security practices, while many smaller utilities lack

funding and expertise. In your opinion, is this an issue of a lack of resources and tools for small and medium systems, or is it a lack of awareness of the tools already available? Are there any recommendations to help promote available tools among the smaller providers who often have fewer resources, dollars, and people than the larger entities, or do we need to actually do something in addition?

Mr. Sullivan. I think the biggest problem is the lack of awareness. I am not sure if the smaller systems, if they have a system that is running and working, and they hear someone else gets attacked, and they just say, who is going to attack me, but they don't know their vulnerability. They don't really know how it could be. So, lack of awareness is, I think, the biggest problem.

Then, once they are aware of it, they need to be able to take a look at it, and say, what would it take for me to do it? It may be inexpensive, a couple of minor adjustments could be okay, but in many cases, I think people are dealing with legacy systems. They put them in, they work fine, there haven't been any patches to the industrial control systems. The devices have been sitting there. No one has looked at them for security purposes, and that is where the real problem lies, and I think we need to educate them, make them aware, and then, in some cases, get them funding to replace them.

Senator Boozman. Very good. Mr. Pratt, how do you balance cybersecurity with functionality? What types of water resources infrastructure should be prioritized?

Mr. Pratt. When I go through the pecking order, I think of, as far as the prioritization goes, I think of large holding ponds of contaminated water are probably a very high priority. Drinking water systems, sewage systems, and drainage and flood control are certainly important. That is the core of my operation. But the ability for that to cause harm to a wide range of people is somewhat limited because generally, the hazards are as related to weather as anything else.

As to how to balance those, what I talk to my team about, I have about 725 miles of infrastructure, three dams, a whole bunch of other odds and ends that go along with that. I have a team of about a dozen people that work on that.

What I talk to people about every day is, you need to decide what you are not going to do today because we don't have the bandwidth. Many of these small operations, that 89 percent that is very small utilities, you might have a single operator with a license who is the licensed operator for three of those facilities. That person is not there every day, and that person is relying even more when they have the opportunity on the remote side of things.

As Mr. Sullivan said, being able to thin out, weed out, and

provide a direct push of information to folks about stuff in their particular situation, that would be the most important to deal with cybersecurity is the most important thing I think, because it is really difficult to balance that. The pressures of day-to-day operations are difficult.

I think the last thing I would say is regarding upping everybody's game. We have all mentioned the tens of thousands of agencies there, and you know, in cybersecurity, you don't have to be faster than the bear, you just got to be faster than everybody else.

There are a lot of weak links, is the problem, and those links can be connected, and they all affect people, even if only one of 56,000 or 70,000 agencies, however many we want to say there are, public and private, just one of those, that can cause a real stir publicly that creates pressure, so there is the stick approach, but there is also the carrot.

Asset management is an excellent way to ensure that local units of government who have pressure to not raise rates are looking to do regular investing and having a long-range plan and having -- what Canada does is, our friends at the Canadian public works, they gave out $180 billion to municipalities. They announced it in 2016, and these folks require you to be eligible for a grant to, number one, you have to show how you are going to take care of the new stuff or the old stuff you are

fixing. You have to stick to that plan or you have to give that grant money back.

My last point would be forgiveness for cybersecurity would be a wonderful thing to weave into all of the programs. Let's put a carrot out there, along with whatever sticks you folks think is necessary. I appreciate the question, sir.

Senator Boozman. Thank you, and thanks to the panelists, and thank you, Mr. Chairman.

Senator Carper. Thank you again for your patience and for being so gracious.

Senator Cardin?

Senator Cardin. Thank you, Mr. Chairman. Let me thank all four of our witnesses. I am very proud of the work of our committee in providing the resources, and I appreciate the acknowledgements today, to allow our public works to have the capacity to respond to current challenges. We very much appreciate your testimony. We appreciate this hearing on cybersecurity challenges.

I really want to, first, welcome Ms. Oberton to our committee. Thank you for your service in Delmar, particularly on the Maryland side of that particular community.

[Laughter.]

Senator Cardin. I have a running battle with the Chairman. I really think that we should be calling it Mardel, but he will

not allow us to change the name of the city.

Thank you for being here.

Ms. Oberton. Thank you for having me.

Senator Cardin. I want to just talk a little bit about the challenges that we have in our rural communities in public works. You have mentioned some, but the rate base is challenging for people to be able to afford their water.

You have a broadband access issue in rural communities. You have a climate change challenge that you are now trying to deal with, so as we talk about being able to deal with the challenges of cybersecurity or the challenges of these other issues, let's talk a little bit about the local capacity and how much it is important for partnerships with the State and Federal Government.

Ms. Oberton. I think that we do very well with having those partnerships. I think that it would be more necessary for yourself and the Chairman and people to come down and see.

I think what happens is, when we look at the larger positions, people don't see what is going on in our small towns, and to know and to walk through and get the feel of what we actually go through on a day-to-day basis. We, in small areas, we don't have enough employees to cover some of the day-to-day things that need to get done. We have to prioritize, and some things that need to get done get pushed back on the back burner,

maybe because of funding, because we just don't have it.

So I think that when you look at the local government, the State government, and the Federal Government, you need to come down off that chair and come see what is really going on in our areas and sit down and have conversations and know what the specific needs are, because each utility is different. Each utility is not that same. We don't offer the same, we don't do the same things. I think that is very important.

Senator Cardin. I have visited the facilities in our rural areas, as well as the urban centers. As I look at current challenges, climate change has really presented a challenge for our water infrastructure. We have invested billions and billions of dollars to deal with the impact of climate change, whether it is storm runoff issues, erosion issues, pollution issues.

In rural communities, the problems might be big, but your rate base, your rate group, is small. So, these issues become magnified in communities that don't have the same fiscal capacity as our larger jurisdictions have.

Could you just share with us how you go about dealing with those types of challenges that are becoming more pronounced as we are dealing with the realities?

Ms. Oberton. Well, we are grateful for the funding that you guys provide for us, and so we make it a priority to figure

out what needs to happen first. Our I&I is first on the list because it is causing problems not only with our water, but also with the sewer, and that is where a lot of our money goes in.

Trying to keep our rates down so our residents can be comfortable is a challenge, but when you have old terracotta pipe, you have to fix them, or you going to continue to have issues. I think funding is very important, and we are grateful for the funding that you guys have given us. It is absolutely necessary for small town communities like ourselves.

Senator Cardin. Again, I want to thank all of our witnesses, and I can tell you, this committee is very mindful of your challenges. We work together in a very strong bipartisan way, and we are going to continue to do that.

Senator Carper. Thanks for joining us, Senator Cardin. We have been joined by Senator Markey.

Mr. Markey, I don't know if you know Mr. Sullivan. There are several John Sullivans in Massachusetts, but this is an extraordinary person, and his years of service rival our own. That is saying a lot.

Senator Markey. Thank you, Mr. Chairman. I will tell you something about the Sullivans. My mother is a Sullivan.

Senator Carper. No.

Senator Markey. Oh, yes. My mother always would say, the Sullivans are a superior group of people, so Mr. Sullivan just

reflects this whole tradition of superior Sullivans.

She had an Uncle John Sullivan, and we may be related, although John Sullivan is not the most uncommon name in Boston, I would say. There are a lot of Jack Sullivans and Jake Sullivans and J.J. Sullivans, to distinguish all of themselves, but this Sullivan, just from his testimony thus far, is clearly superior.

Senator Carper. He is good. He is first-rate.

Senator Markey. On the other hand, my mother was afraid that that had been watered down by the other side of the family, and she used to say that Eddie, your father and I, we are going to donate your brain to Harvard Medical School as a completely unused human organ. You are part Sullivan. Learn how to work smarter, not harder.

So, Mr. Sullivan, and we might need a translator, so other people can understand what we are saying to each other, is it a matter of money? Do you just need money to be able to invest in the technologies which are needed to protect against cyberattacks?

Mr. Sullivan. Well, Senator, there is money needed. However, the larger cities are able to, because of their workforce and because of their rate base, they are able to take care of most of the issues that are facing them.

What they need is more information, timely information.

They need to know about the innovations others are using so that they can implement them, and also the larger, greater than 100,000 cities.

When you get down smaller, there are so many competing interests on the smaller groups, including the affordability issue that is on their rate base, that they have got to look at, is climate change more important now? Is it the flooding that is occurring, what about a wildfire? Where do I put my resources?

Senator Markey. Can I ask a question? In this modern era, is it just part of the cost of doing business? In other words, there is Dickensian quality to the internet. It is the best of technologies, and the worst of technologies, simultaneously. The best of technologies can like, make so much money that we have a race to go to outer space, amongst all the people who made a lot of money, but then you leave behind these unattended to problems, which also exist, which is the vulnerability of every device which we use and all these utilities.

Do you think that our consciousness in the Country has to just switch to the fact where, you get the benefits of it, on the one hand, as a municipality, but at the same time, you have to adjust up what you are willing to pay in order to protect against the sinister side of cyberspace, or should the Federal Government be providing the funding, or State governments, to

smaller communities, especially?

Mr. Sullivan. I think we may be in a catch-up mode because we all went to this great technology. It was wonderful in the 1990s, and we could actually do more with less, because we could use technology. But no one worried about, is someone bad out there going to take me down with this?

So, now we are in the point, yes, someone is going to take you down, and the catch-up to the bigger cities, like I mentioned, have been taking care of their problems. The little ones are just stymied. First, they don't even know what the problems are, so we have got to get more resources to them and let them understand what is wrong, and some of them may need additional funds.

I can't speak for every utility and how they would get it or what their infrastructure needs are, or the sewer overflow.

Senator Markey. So, you are just saying, we have to provide the resources to those smaller communities?

Mr. Sullivan. Yes.

Senator Markey. And maybe ensure, on a regional basis, that this is an ongoing, educational process for those communities, so they are brought up to speed, and know that this risk is real, because we are deep into it now. All around the world, they can see what they can do to the Quabbin Reservoir, to other facilities, so thank you for that.

Mr. Bhatt, I have a piece of legislation: The Security and Privacy In Your Car Act, or the SPICar Act. I have introduced that with Senator Blumenthal, and the Chairman has been good enough to include it in the surface transportation bill approved by this committee. What that legislation does is it instructs the Federal Highway Administration to create a cybersecurity tool and appoint a cyber coordinator that will help transportation authorities identify, detect, protect against, and respond to, and recover from cyber incidents.

Do you support that legislation moving forward and passing this year so that the Federal Highway Administration has that instruction and those tools to being to implement?

Mr. Bhatt. Yes, Senator Markey. I know you have been very passionate on this issue, and to me, I think the whole tone and tenor of this hearing is about the need for Federal leadership in cybersecurity. So, to the extent that Federal Highways has more resources, the only caveat I would say is just making sure that whatever USDOT or Federal Highways is doing is tied in which DHS to make sure that they are all working in coordination.

Senator Markey. Thank you. I was the chair of the Energy and Environment Subcommittee in the House back in 2009, 2010. The FBI, CIA, they all came to me. They said, we have a great vulnerability in our utility sector. We can be attacked at any

time.

So I worked with Congressman Upton. We got the bill passed and on the Floor to mandate that utilities had to update. Mandates, okay, and we could give them some assistance.

What happened here, over in the Senate, a single Senator, actually from Arizona, just put a hold on that bill and killed it. It was, now, 11 years ago. Otherwise, we would have already had a mandate out there that utilities have to do something about this.

My own belief is that it is not a new issue. The CIA and FBI wouldn't have been coming to me in 2009 if it was a new issue. They said their hair was on fire 12 years ago, okay?

So, it is an issue that just hasn't had the funding or attention paid to it, and actually, I started with just looking at the utilities. They just don't like the cost of doing it. It is not like it is some mystery that they are the only ones who don't read the front page and say, these facilities are vulnerable, China or Iran or North Korea are attacking them. It is all out there in the public domain.

So I just think it becomes kind of the job of the government to say, you have to do it. We will help to fund it for you, but otherwise, we are going to have a catastrophe.

I am so glad that we are having this hearing, and I thank you, Mr. Chairman, for including in the surface transportation

bill my SPICar legislation. I hope we can get that deal out on the Floor in the next week or so, because I think those tools are going to help, especially in the automotive sector, where these things are just computers on wheels, and the internet is now in the red light. It is in all the traffic control systems.

There are so many pathways in now, to kind of disrupt our way of life, and as people drive these autonomous vehicles, just some kid sitting on his bed wants to just start playing games, he won't have to be on an overpass anymore, throwing a rock at a car. You just do it from sitting in a car, sitting in his living room, and create a disaster, so I thank you, Mr. Chairman, for your help in including that legislation.

Thank you.

Senator Carper. I am happy to do it. Thank you. SPICar, I like that. SPICar.

I have some questions I want to ask now, and I think Senator Capito may have an additional question or two, and then I think we are going to wrap at that point in time.

Coming back to Secretary Bhatt, a question with respect to interoperability and cybersecurity. As I am sure you are aware from your experience both at the State level in Colorado and Delaware and at the federal level of transportation, when looking to address a National problem, there is no one-size-fits-all solution.

In your testimony, you state that a national strategy that extends to State and local transportation agencies will be the key to helping address some, not all, but some of these vulnerabilities. My question would be, given that every State and local agency is not on the same level of technical expertise, as we have been reminded here today, as well as the financial capability, how do you suggest that we get just about everybody to agree to a baseline that will not prevent an inoperability between systems already in place?

Mr. Bhatt. Thank you, Senator, and again, I really appreciate the committee's focus on this issue.

I think that there are efforts underway in this space. We have talked about USDOT and their focus, AASHTO has a committee on transportation system security and resilience and also transportation system operations that is trying to bring everybody up to a baseline. From a federal perspective, based on my experience, the way I would approach this would be to say, let's make the funding 100 percent eligible from a federal perspective, as we do for many of the safety programs.

Then the playbook that I would recommend is the NIST Framework for all of the stakeholders. Their framework for cybersecurity talks about identifying the threats to your system, protecting against those vulnerabilities, detecting attacks on your system, responding to them, and then recovering.

We have heard, even, on the water side how folks have been able to respond quickly if they have got the proper backups, if they have got segmentation of their systems. So I think the simple answer is to have all of these agencies by a date come back and say, yes, we have adopted the NIST Framework. You have to walk before you run, and that would get everybody walking, and then we can kind of have a level playing field.

Senator Carper. All right. Good, thank you.

Mr. Sullivan, a question for you, if I could. If the Federal Government provided funding assistance to support the Water Information Sharing and Analysis Center operations, WaterISAC, what expanded services would the center be able to offer?

Mr. Sullivan. Well, we would work with our partner agencies, the EPA, et cetera, to identify all the agencies that needed us, all the water utilities, et cetera. We already work with them and the partners with SISA, et cetera. We would take that information they have and boil it down so it is understandable to our audience.

They put out a ton of information all over the place, a plethora of information on IT. We would take it and make it so that people would understand how it impacts their system. With that knowledge, we would do additional training. We would have the training that is available already through either National

associations that we could publicize that to them, because not every operator knows all of this is out there, so we would centralize it, put it to them through daily alerts, weekly alerts, monthly.

In addition, we have a huge library of all types of information, including chemical analysis, and what do you do when. We would be able to direct resources when there was a response that could call the ISAC, and we could put them in touch with subject matter experts.

Senator Carper. All right, thank you.

A question, if I could, for all of you, all of our witnesses, dealing with cross-modal integration. As we have seen and heard in this hearing today, cybersecurity is not an issue that exists in one, singular place or in one specific mode of transportation. How do we ensure that, as we look to address these ever-growing vulnerabilities, we do so in a way that addresses all modes of infrastructure, including transportation?

Secretary Bhatt, would you go first on this one, and then we will ask the others to comment, if they wish?

Mr. Bhatt. Yes. I think that that is part of the challenge in transportation and for all of these different agencies is, we have historically been very silent. So, our buses are part of our transit systems. Our trains are part of our rail system.

Our highways operate independently, and the problem is, as you get into this IOT environment, the cameras that are providing feeds into a transportation management center are also receiving signals from buses that are relying on traffic signals, to move to optimize that bus route. You have got micromobility coming in, scooters and automated vehicles.

So it is incredibly important that, and again, this is part of the discussion we have had with USDOT is, how do you bring in all of these disparate modes. The ITS Joint Program Office is providing a lot of leadership in this space, but it is critical that we do not view this as mode by mode, but as a system of systems, and I think that that is really critically important to these efforts.

Senator Carper. All right, thank you. Any of our other witnesses want to comment on this question? You don't have to, but if you would like to, go ahead. Mr. Pratt?

Mr. Pratt. I just have a comment to just make an analogy, just kind of looking around at maybe our average age profile. I remember when it you wondered if the printer was going to print the thing. When they first had printers, and the software didn't talk to each other, and everything was all goofed up.

So I just kind of want to bring that down to the more simple analogy of, eventually, that got figured out, and now my computer is going to automatically find the nearby printer, let

me know which ones.

It is getting those sort of protocols and standardization where, even if we have got a ramshackle set of connections of five different pieces of software, their ability to connect securely to each other quickly without the users having to be some sort of brilliant IT scientist. That is the direction, and that is where we need to head.

I believe, like the transportation systems in my neighborhood is the American Center for Mobility. One of their primary missions, it is a Federal testing center to attempt to provide more and more standardization. IT is, the fellows there and the ladies there have like, well, geez, the headlight thing is in a different place on every car. Good luck with getting all the computer stuff to work out.

Just a more plain-spoken way of trying to say for all of us, just back in the day of printers. We need to get back in that direction where the software is going to figure it out, but we are also secure. I think that second part is a lot trickier than it was in the day of printers.

Senator Carper. Anyone else before I yield to Senator Capito?

Mr. Sullivan. One real comment would be, the water systems are all independent. We all use the same equipment; we all do the same type of work, and similar, but we don't interconnect

like your electrics, like your communications, like your transportation systems across the board. We deal in a turf and a territory individually.

But we need standards so that we all know how we all should be taking care of our same types of equipment. We don't necessarily have those exacting standards. The bigger companies do; the bigger cities do, but the smaller ones, they don't know what the standards are.

Senator Carper. All right.

Senator Capito, go right ahead, and then I am going to ask one or two more questions, and we will be done.

Senator Capito. Yes, thank you. Thank you all very much. I think this has been a great hearing and eye-opening in some ways, because of the challenges, but also some of the gaps. We know this is an issue that is going to grow. It is not like it is going to shrink and go away. We know it is going to grow, so I thank you for being in the arena.

I did say, I thought Mr. Pratt, when you went to the average age of the folks in the room, one of the concerns that I have had and that we have actually in our water bill is the next generation workforce. For some reason, this career, which I think is very obviously, Mr. Sullivan has been in it for a very long time, holds a lot of promise to raise your family with and to have great expertise and respect, as you all do in your

community. But for some reason, our younger generation is not getting in there.. I know in our State of West Virginia, a lot of people are aging out. They want to retire, but to find replacements has been really, really difficult.

So I am hoping that by shining a light on how folks have managed their systems for so long, because I think Ms. Oberton said 70,000 rural water systems, I mean, that is a lot of people. That is a lot of jobs.

I just have one question of Mr. Bhatt. I had to step out a bit, so I don't know if this got addressed in any way.

Obviously, we have got a lot of big internet companies that gather a lot of data. That is a subject for a whole, bigger debate. I am not asking you to have that debate.

I was just wondering if there are any ideas on the table to partner with some of these private technology entities to be able to help meet the challenges, not just on prevention, but also on detection and other areas of cybersecurity? Are you aware of any of those?

Mr. Bhatt. Yes, Senator Capito, and I think one thing on the workforce piece. I think this is incredibly important, because State DOTs, I remember in my time having to struggle to compete for mechanics, because we would pay a certain wage, and private sector companies would pay more. Well, that problem is exacerbated on the technology side, and I think this idea of

creating these workforce cultures is really important, and I would look forward to working on that.

From a large internet perspective, we have Google and AWS that are members of ITS America. What used to happen was, back in the printer day, you were talking about one device. Now, you introduce the cloud, and something that Mr. Pratt said, the more hand-offs, the more fumbles.

I think that is critical to working with those partners to ensure that as data is going from a vehicle to the infrastructure up to the cloud, back, and lots of hand-offs, working with those technology partners to ensure that all levels are layers are secure is really important.

Senator Capito. All right. Thank you. I am going to go vote.

Senator Carper. Do you want to make any closing statements on this hearing?

Senator Capito. No, I just thank you, Mr. Chairman, and you all. I think this has been a really good hearing, and we will just have to keep the conversation going.

Senator Carper. Amen. Thanks again to you and your staff for bringing up the idea and for making it real.

One last question, if I could, for Mr. Pratt. One of the things you said was more hand-offs, more fumbles. People say to me, well, my wife will say to me, what did you learn today at

this hearing? I got a great line from a guy from Michigan.

Mr. Pratt. Actually, the term would be knock-ons, but since nobody else here probably plays rugby, I just went with the old football thing. Thank you, sir.

Senator Carper. Mr. Pratt, it is clear that the challenges are cybersecurity vary from large communities to smaller communities. As I said earlier, too, I think, to Mr. Sullivan, even within community categories, a one-size-fits-all approach may not be the best way to effectively manage and to address cybersecurity threats.

My question to you, Mr. Pratt, would be: aside from funding, what primary role should the Federal Government play in addressing cybersecurity so that the solutions are flexible, but also effective?

Mr. Pratt. You have hit the nail on the head, certainly. Flexibility, but we have got a lot of variety and diversity out there, so how do we get standardization at the same time as flexibility?

I am going to go with two most important things off of that list that we provided. One is that clearing house type of concept that Mr. Sullivan has talked about. How can we help filter so that rural water really has something that is cleaned up that they can push out to folks, and at the same time, agencies that are working more on the large scale have messaging

that is more tailored to them, and it is that training.

How do we get the training to acknowledge some of that need for standardization and having people recognize that we are in the process of moving forward? The thing about working with the private sector, I think the companies have quit calling me. But the market is so dispersed in the water infrastructure, it is a low barrier to entry, to startup, to do electronic sensing and controls.

So I would say my first five years in office, I probably got two or three calls a week from various different companies about hey, would you buy our doohickey to help you do that what, measure things, monitor things, control things. So I am sure I heard from a good 50, 60 different companies. It is a very fractured market is my point.

Senator Carper. All right, thank you.

I am just going to ask, sometimes I do when we have a minute or two at the end of a hearing, I will ask the panel is there one thing that you would like to add or really reiterate? Just very briefly, one more thing. You can come back to something that you have already said yourself or heard someone else say that you think is worth repeating, just something you would like to underline, put an exclamation point behind.

Ms. Oberton, would you do that, please?

Ms. Oberton. I just think that it is very important that

the training and the accessibility for the rural areas for the cybersecurity be top priority because we make up the majority of the water systems across the Country.

Senator Carper. Okay, thank you, ma'am.

Mr. Sullivan?

Mr. Sullivan. I know you have heard me say it many times that we need to get to the WaterISAC to be the central. I want to reiterate that the WaterISAC was formed for physical security problems in 2002. We then developed all hazards, and now we are working deeper in cyber, so anybody that joins it gets not only the cyber issues, but they get all the hazard and all the climate change issues and everything else. It is all available already, and we have it selected just for the water and wastewater systems.

Senator Carper. Thank you, sir.

Secretary Bhatt, the last closing thought?

Mr. Bhatt. I would say that the transportation system in the United States was what allowed us to "win the 20th century," and there are a lot of negotiations now about a generational investment that you all are trying to make. I think cybersecurity is an incredibly important part of ensuring that this digital confluence of physical infrastructure and digital overlay is secure so that we can have 21st century infrastructure that helps us in the 21st century.

Senator Carper. Mr. Pratt, one last thing you would like to emphasize?

Mr. Pratt. I am going to echo Mr. Sullivan, that WaterISAC is wonderful. It is an association of associations. It does connect somewhat at the federal level, but a little bit more input in that direction would really help.

I would say, my county is 370,000, but it is 40 percent rural. I can ride a bicycle 15 minutes from where I live in Ann Arbor any direction and be in a cornfield, so we have several rural operators in our area. I made the note of, I need to reach out to all those folks about the WaterISAC, because it has got great stuff for them.

Senator Carper. Thank you all. I presume you all have stores called Home Depot not too far from where you live. Their ad campaign for years was, you can do it, we can help.

When I think of responsibilities that we have, the people we are privileged to serve and represent across the Country, it is a shared responsibility. The Federal Government can't do everything. It can't be all on the States; it can't be all on the local governments or school districts. It can't be all on non-profits and so forth.

But you can do it, we can help. When you think about what the Federal Government might be doing a little better job at, we might want to put some emphasis to be a good partner. What

comes to mind, just briefly, Mr. Pratt?

Mr. Pratt. As a Federal Government partner, I am going to take a little bit of a different tack and go back to the asset management piece of things and start to, you know, it would be great to see asset management as a lot more carrot there, and having that whole cybersecurity is a part of keeping your stuff in good shape.

Whether you have leaky pipes or bumpy roads or signals that aren't optimized, at the end of the day, asset management is a mindset that requires quite a bit of training, just like cybersecurity, but it is really no different than having that maintenance schedule for your car. Everybody does the oil changes, but a lot of people say, well, that brake job is a lot. How long can I wait?

But it seems like America's infrastructure has been treated like, I am going to buy a car and I will drive it until the brakes fail, and then we will see what happens next. That is really the situation we are in.

So encouraging that asset management mindset and helping us develop workforce in that area is one of the best things I believe the Federal Government could do, and federal governments in most of the commonwealth countries are a good 5 to 10, 15 years ahead of the U.S. in that.

Senator Carper. All right, thank you. Thank you.

Secretary Bhatt?

Mr. Bhatt. I would say that one thing that the Federal Government is really good at doing is focusing attention on issues and then providing resources. So, to me, this hearing, the efforts going on with the Administration and other committees, it is an ability to bring focus, and then an ability to bring funding.

I think that making the cybersecurity eligible is a great first step. Now we need to identify funds so that these organizations that have to make tough choices don't have to choose between cybersecurity and potholes and other things, so asset management, incredibly important. But if you want the cybersecurity, that is what the Federal Government can play a critical role in.

Senator Carper. Okay, thank you.

Mr. Sullivan, how can we better help at the federal level?

Mr. Sullivan. I believe all of us have the same goal, and that is to improve the lives of the American people. The water utilities protect the public health of the American people, and we have a responsibility to do what we can.

We are a little bit behind the eight ball, and right now, we need to do catch-up. So what we need is a little more guidance on the rules, so we have a set of rules across the boards. Not regulations that you must mandate, because they are

going to be outdated by the time we pass them, because the technology is moving faster than we are. What we need is a little more guidance like that, and funding where it is needed.

There is a responsibility at the local level to do what you can do, but some people don't have the resources. So we could work with the Federal Government and partner with everyone, as we should on all things we do.

Senator Carper. Thank you.

Ms. Oberton?

Ms. Oberton. I think the Federal Government could help with providing us with more circuit riders, that type of assistance that can be targeted towards the cybersecurity and focus that specifically to each water community for the rural areas.

Senator Carper. Say that last sentence again.

Ms. Oberton. Say again?

Senator Carper. Just repeat your last sentence.

Ms. Oberton. Having more circuit riders come out to train us on the cyber security and it be specific for our particular needs.

Senator Carper. Thank you. I want to thank you for coming today. I want to thank your mom for having your back, and Mr. Sullivan, Secretary Bhatt, and Mr. Pratt, thank you. Thank you all.

I want to thank Senator Capito again, and her team, for working with my team and others to plan for this hearing and to hold this hearing. I want to thank you for your time and for your testimony today. I said earlier, cybersecurity is a constantly evolving challenge, much like climate change, no silver bullet, no single policy or one-time solution to address the cyber threats to our Nation's critical infrastructure.

I like to say there is no silver bullet, but a lot of silver BBs. Some are bigger than others, but my hope is that today's hearing will shed some light on the urgent need to protect our physical infrastructure and will help spur further action as we consider infrastructure legislation.

Just a little bit of final housekeeping. I would like to ask unanimous consent to submit for the record a number of reports and articles related to today's hearing. Hearing no objection, so ordered.

[The referenced information follows:]

Senator Carper. Additionally, Senators will be allowed to submit questions for the record through close of business on August the 4th. We will compile those questions. We will send them out to our witnesses, and we ask our witnesses to reply by August 18th, which was my mother's birthday, and her mother's birthday. How about that?

Last thing I would say, my mother was a deeply religious woman, and she was always reminding my sister and I to take seriously the admonition of Matthew 25, which starts off with, when I was thirsty, did you give me to drink? When you guys are up at the heavenly gates and trying to get in and talking to Saint Peter, and he says, what did you do about making sure people had some healthy water to drink and so forth, you can say, we did a pretty darned good job, and he will let you in.

Thank you all. With that, this hearing is adjourned.

[Whereupon, at 11:53 a.m., the hearing was adjourned.]