S. HRG. 117–74

ADDRESSING CYBERSECURITY VULNERABILITIES FACING OUR NATION'S PHYSICAL INFRASTRUCTURE

HEARING

BEFORE THE

COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JULY 21, 2021

Printed for the use of the Committee on Environment and Public Works

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

45–752 PDF WASHINGTON : 2021

COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

THOMAS R. CARPER, Delaware, *Chairman*

BENJAMIN L. CARDIN, Maryland
BERNARD SANDERS, Vermont
SHELDON WHITEHOUSE, Rhode Island
JEFF MERKLEY, Oregon
EDWARD J. MARKEY, Massachusetts
TAMMY DUCKWORTH, Illinois
DEBBIE STABENOW, Michigan
MARK KELLY, Arizona
ALEX PADILLA, California

SHELLEY MOORE CAPITO, West Virginia, *Ranking Member*
JAMES M. INHOFE, Oklahoma
KEVIN CRAMER, North Dakota
CYNTHIA M. LUMMIS, Wyoming
RICHARD SHELBY, Alabama
JOHN BOOZMAN, Arkansas
ROGER WICKER, Mississippi
DAN SULLIVAN, Alaska
JONI ERNST, Iowa
LINDSEY O. GRAHAM, South Carolina

MARY FRANCES REPKO, *Democratic Staff Director*
ADAM TOMLINSON, *Republican Staff Director*

C O N T E N T S

ADDRESSING CYBERSECURITY VULNERABILITIES FACING OUR NATION'S PHYSICAL INFRASTRUCTURE

WEDNESDAY, JULY 21, 2021

U.S. SENATE,
COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS,
Washington, DC.

The Committee, met, pursuant to notice, at 9:51 a.m., in room 406, Dirksen Senate Office Building, Hon. Thomas R. Carper (Chairman of the Committee) presiding.

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

OPENING STATEMENT OF HON. THOMAS R. CARPER, U.S. 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 cyber attack. 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 cyber attacks 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 them, "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 cyber attacks.

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 1 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 from 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 up front.

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 structured 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.

OPENING STATEMENT OF HON. SHELLEY MOORE CAPITO, U.S. 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 cyber attacks. 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.

Cyber attacks 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 in protecting our drinking water and wastewater systems from cyber attacks 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 cyber attacks 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 policies 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 toward protecting all Americans and that critical infrastructure through strengthened cybersecurity measures.

Thank you, Mr. Chairman.

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 cyber attacks. 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 HON. MIKE GALLAGHER, U.S. REPRESENTATIVE FROM THE STATE OF WISCONSIN

Representative 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.

Representative 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 cyber attacks.

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 cybersecurity. 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 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 cybersecurity, bolstering the ability of the water sector to detect, prevent, and withstand cyber attacks has emerged as a crucial priority.

Though 55 percent of utilities responding to a survey conducted by the Water Sector Coordinating Council rated cybersecurity as a high or top priority, the overall cybersecurity 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 benefited 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 cyber attack 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 cyber attack on our water supply. Beyond the direct impact to drinking water, a cyber attack 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 Representative Gallagher follows:]

Thank you Chairman Carper, Ranking Member Capito, and distinguished members of the Committee for the opportunity to speak with you today. I appreciate the chance to appear along with my U.S. Cyberspace Solarium Commission co-Chair, Senator Angus King, to talk about the importance of securing our nation's water supply from cyberattacks.

The U.S. Cyberspace Solarium Commission was authorized through the National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."[1] In the course of this 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.

The sixteen critical infrastructure sectors are not equally equipped when it comes to cybersecurity: There are leaders—like the financial services sector—and there are 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."[2] As we've continued our work on improving the nation's cybersecurity, 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 cybersecurity as a high or top priority,[3] the overall cybersecurity 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:[4] Many of our nation's nearly 70,000 community water and wastewater systems[5] are small, publicly owned assets that are not equipped to deal with nation-state threats.[6] And the National Infrastructure Advisory Council has described federal support for the resilience of the water sector as "fragmented and weak."[7]

Municipalities have benefited 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 dedicate less than 1 percent of their budget to the cybersecurity of information technology, and 44.8 percent

---

[1] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (2018), https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf.
[2] U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission* (March 2020), 62, https://www.solarium.gov/report.
[3] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity 2021 State of the Sector* (June 2021), 18, https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf.
[4] National Infrastructure Advisory Council, *Water Sector Resilience: Final Report and Recommendations* (June 2016), 4, https://www.cisa.gov/sites/default/files/publications/niac-water-resilience-final-report-508.pdf.
[5] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity,* 3.
[6] National Infrastructure Advisory Council, *Water Sector Resilience*, 36-37.
[7] National Infrastructure Advisory Council, *Water Sector Resilience*, 97.

allocate less than 1 percent of their budget to the cybersecurity of operational technology.[8] Insufficient security investment leaves the water sector vulnerable to nation-state, criminal adversaries, and insider threats—disgruntled employees or former employees with specific knowledge of how to disrupt a utility's information technology or operational technology systems. Against these threats, the water sector faces challenges ranging from maintaining awareness of the threats to assessing risks to identifying and remediating vulnerabilities.[9] A shortage of qualified cybersecurity professionals across the globe compounds the problem,[10] making it difficult for resource-strapped organizations to attract and retain the talent necessary to protect our drinking water and public health systems.

Earlier this year, 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.[11] 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.[12] 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.[13] 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's why it's considered a lifeline sector.[14] 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, economy, public health, and safety.

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

---

[8] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity*, 8.
[9] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity*, 10.
[10] International Information System Security Certification Consortium, *Cybersecurity Professionals Stand Up to a Pandemic: (ISC)² Cybersecurity Workforce Study, 2020* (2020), 16, https://www.isc2.org/Research/Workforce-Study#.
[11] Peter Elkind and Jack Gillum, *America's Drinking Water Is Surprisingly Easy to Poison* (March 17, 2020), https://www.propublica.org/article/hacking-water-systems.
[12] Kevin Collier, *50,000 security disasters waiting to happen: The problem of America's water supplies*. NBC News (June 17, 2021), https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206.
[13] U.S. Department of Justice, U.S. Attorney's Office for the District of Kansas, *Indictment: Kansas Man Indicted for Tampering With a Public Water System* (March 31, 2021), https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system.
[14] National Infrastructure Advisory Council, *Water Sector Resilience*, 19.

Senator CARPER. Thank you, Congressman.
Senator King, please proceed.

STATEMENT OF HON. ANGUS KING,
U.S. 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 cyber space 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 cyber attacks, 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 cyber attack, but it was a kind 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 2 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 e-mail, 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 OK. 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 this issue. 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:]

Thank you Chairman Carper, Ranking Member Capito, and the distinguished members of the Committee for the opportunity to speak with you today. I am pleased to be here along with my Cyberspace Solarium Commission co-Chair, Congressman Mike Gallagher, to talk about how we might improve the cybersecurity of one of our nation's most critical sectors.

Congressman Gallagher paints a disturbing picture. Threatened by criminals and nation-state adversaries alike, as this Committee is aware, our water sector is at risk. Less than a decade ago, its disruption through cyber means seemed like science fiction, but in the last several years we have witnessed widespread and impactful cyber attacks on our critical water infrastructure from Florida to California. The time is now to explore solutions to the challenges we face in securing our water systems.

As the U.S. Cyberspace Solarium Commission details in its report, pushing back against bad cyber behavior is both an offensive and a defensive activity. On the offensive side, we possess the world's most capable cyber operators in our Department of Defense and National Security Agency. We must continue to enable these entities to defend forward against foreign threats and disrupt our adversaries at the source. On this front, the United States is making effective investments.

However, we have chronically underinvested in cyber defense for decades. The necessary investment can take many forms. We need to build capacity and provide better advice to less mature organizations, exchange better information with more mature organizations, and build a more integrated relationship between our largest, most mature—and often, most at risk—partners in the private sector and the federal government. This applies across the board with our sixteen critical infrastructure sectors, but is particularly salient in the context of the water sector.

Defense starts at the local level, where many smaller rural water utilities struggle to identify, assess, understand, and ultimately mitigate cyber risk. The Federal government has a duty to help these entities manage such risk. Two specific programs stick out as relevant in this context. First, the circuit rider program provides hands-on technical assistance to water system operators on a variety of issues. This program could be expanded to incorporate technical cybersecurity assistance. Second, the work of National Laboratories to identify cybersecurity vulnerabilities in the operational technology environments of the energy sector should serve as the groundwork for similar efforts and trickle out to other sectors, including the water sector.

Moving up the chain, mid-sized and more mature entities in the sector thirst for more knowledge and information regarding the threats that they and their counterparts face. In most sectors, Information Sharing and Analysis Centers (ISACs) serve as coordinating bodies to facilitate the sharing of cybersecurity information among entities in a given sector. The waterISAC provides free services to the water and wastewater sector but is under-resourced. An augmentation of their budget through a federal grant would allow them to expand their services to enhance the overall cyber readiness and resilience of the sector through risk assessments, advisory support, incident tracking and analysis, and training and sector-wide exercises.

Finally, at the top of the chain, the most mature and riskiest entities need to be brought closer to the Federal government. Reinvigorating this relationship should take two forms. First, we as a Federal

government must do a better job of assessing national risk and working with the entities that own and operate infrastructure that, if disrupted, could produce catastrophic consequences for our national security, economic continuity, or societal resilience. To do this, the U.S. Cyberspace Solarium Commission recommended the passage of legislation tasking the Department of Homeland Security with working with relevant sector risk management agencies to identify systemically important critical infrastructure and build more robust relationships with these entities, providing them with benefits—like enhanced intelligence sharing—and holding them to account for their cyber hygiene. Second, we must do more to ensure that mature companies are able to share with and receive information from the Federal government in real time. The creation of a cloud-based Joint Collaborative Environment would supply the Federal government and critical infrastructure owners and operators with a common, interoperable virtual environment to share and fuse threat information, insight, and other relevant data, allowing the federal government to give real-time warning of incoming threats.

These are important steps that we, as Congress, can take in the short-term to build greater cyber resilience in the water sector. In the longer term, we must consider how best to equip responsible Federal agencies, including the Environmental Protection Agency, with the resourcing and investment to set and normalize standards across the sector. Holding entities to a higher cybersecurity standard is, and will continue to be, crucial for ensuring that both systemically important critical infrastructure and the rest of the sector are fully prepared to defend the nation's water supply from the pressing threats that Congressman Gallagher eloquently described.

Thank you again to Chairman Carper, Ranking Member Capito, and the members of this Committee for the opportunity to speak with you today about this crucial issue. I look forward to working with all of you to improve the cybersecurity and resilience of our nation's critical water infrastructure.

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 our 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 Hickenlooper for whom you worked 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 John Sullivan.

Mr. Sullivan, good to see you. Chief Engineer for the Boston Water and Sewer Commission. Do you have a favorite baseball team?

OK, 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 5 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. Sophia 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 in 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 my 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 6 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, 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 mak-

ing cybersecurity 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, V-to-X, and other emerging connected vehicle technologies, autonomous and automated technologies, and mobility on demand.

While advances have made the transportation system more connected than 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 3 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 cybersecurity. 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 cybersecurity 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 cybersecurity 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 cybersecurity work force 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 cybersecurity 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:]

STATEMENT OF

SHAILEN P. BHATT

PRESIDENT AND CEO

INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA

ON

"ADDRESSING CYBERSECURITY VULNERABILITIES

FACING OUR NATION'S PHYSICAL INFRASTRUCTURE"

SUBMITTED TO THE

UNITED STATES SENATE

COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

JULY 21, 2021

Chairman Carper, Ranking Member Capito, and Members of the Committee on Environment and Public Works, thank you for the opportunity to provide the Intelligent Transportation Society of America's (ITS America) perspective on "Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure."

My name is Shailen P. Bhatt, and I am the President and CEO of the Intelligent Transportation Society of America (ITS America). I am honored to be here today – I appreciate the opportunity to talk about addressing cybersecurity vulnerabilities related to road and bridge infrastructure.

Before becoming ITS America's President and CEO in 2018, I served as Executive Director for the Colorado Department of Transportation. During that time, I also served as the national Chair of the Vehicle-to-Infrastructure Deployment Coalition and the Chair of the National Operations Center of Excellence. Before the Colorado Department of Transportation, I served as Cabinet Secretary with the Delaware Department of Transportation and Deputy Executive Director of the Kentucky Transportation Cabinet. I also served as an Associate Administrator at the Federal Highway Administration under U.S. Department of Transportation Secretary Ray H. LaHood.

ABOUT ITS AMERICA

ITS America is the nation's leading advocate for the technological modernization of our transportation system by focusing on advancing research and deployment of intelligent transportation technology.[1] Founded as an official advisory board on road technology to the U.S. Department of Transportation, ITS America represents state and city departments of transportation, transit agencies, metropolitan planning organizations, automotive manufacturers, technology companies, engineering firms, automotive suppliers, insurance companies, and research and academic universities.[2] Our members come to one table – ITS America – to shape the next generation of transportation and infrastructure driven by intelligent transportation technologies.

[1] Find out more information about ITS America here: https://itsa.org/

[2] The ITS America Board is represented by the following organizations: AAA, AECOM, Amazon Web Services, Arizona Department of Transportation, California PATH University of California Berkeley, California State Transportation Agency, Central Ohio Transit Authority, Cisco, Cubic, Econolite, Florida Department of Transportation, Ford Motor Company, General Motors, Google, PrePass Safety Alliance, HNTB, Iteris, Los Angeles Department of Transportation, MCity, Michael Baker International, Michelin, Michigan Department of Transportation, National Renewable Energy Lab, New York City Department of Transportation, Panasonic North America, Qualcomm, San Francisco Bay Area Metropolitan Transportation Commission, San Francisco County Transportation Authority, State Farm Insurance, Texas Department of Transportation, Texas Transportation Institute, Toyota, Virginia Department of Transportation, and Washington State Department of Transportation

ITS America's mission is to advance the research, development, and deployment of intelligent transportation technologies and solutions to save lives, improve mobility, promote sustainability, expand equity, and increase efficiency and productivity. Our focus is policy that accelerates the deployment of seamless mobility technology, connected and automated vehicle technologies, and smart infrastructure; policy that breathes new life into our transportation system by expanding investments in technologies that support smart communities; policy that encourages new models and modes of transportation, including micro-transit and Mobility on Demand, including ridesourcing, carshare, bikeshare, micro-mobility, and unmanned systems; and policy that does all of this while making our transportation system safer, greener, and smarter. Investments in these technologies should also address issues of transportation equity, so everyone gains access to mobility and opportunity, and the valid concerns of the transportation workforce.

As ITS America noted in our recently-released technology blueprint, enacting policies that deploy intelligent transportation technologies will ensure a safer, greener, smarter, and more equitable transportation system.[3]

My remarks will focus on three key areas.

- First, how intelligent transportation technologies have transformed transportation and are defining the way people, goods, services, and information move in the 21st century.
- Second, why cyber-attacks on transportation are a growing concern worldwide.
- Finally, much like Vision Zero, in regard to the national strategy to make our streets and physical infrastructure safer, ITS America calls on Congress and the Biden Administration to work with the United States Department of Transportation and other stakeholders to adopt a more robust national transportation cybersecurity strategy to make the digital layer of our transportation system safer.

INTRODUCTION

On behalf of ITS America members working to secure critical transportation assets, including road and bridge infrastructure, thank you for recognizing the growing risk and making cybersecurity explicitly eligible, for the first time, under federal highway formula programs in the Committee on Environment and Public Works approved Surface Transportation Reauthorization (STRA) Act of 2021.[4i]

[3] Find out more information about ITS here: https://www.transportation.gov/new-and-emerging-technologies

[4] STRA made cybersecurity explicitly eligible, for the first time, under the following federal highway formula programs: Sec. 1105. National Highway Performance Program. Makes eligible measures to protect

As vehicles and infrastructure become more connected, our nation's transportation system faces increasing cybersecurity risks. Given the ability to cause loss of life and inflict significant economic damage in a highly visible manner, cybersecurity attacks directed at those producing or operating technologies travelling over or connected to U.S. roadways will intensify. Infrastructure with Intelligent Transportation Systems (ITS) leverages modern communications systems to support transportation management and operations. As a result, intelligent transportation technologies no longer function as closed systems, thus exposing transportation facilities and infrastructure to cyber threats due to their connectivity.[5]

ITS support the U.S. economy and state and local economies by making our transportation system safer and more efficient. They allow U.S. cities to compete globally with cities in Asia and Europe in a technology-driven 21st century economy. But - we must manage the vulnerabilities that come with a more complex and connected transportation system. We need to stop thinking of cybersecurity as something to add to our infrastructure. We need to fully integrate cybersecurity as part of our infrastructure and make intelligent transportation systems secure by design.[6]

DEFINING THE WAY PEOPLE, GOODS, SERVICES, AND INFORMATION MOVE

For the past 100 years, road and bridge infrastructure has primarily consisted of individual, independent vehicles traveling on asphalt – in other words, cars and trucks moving on and over roads and bridges without the benefit of intelligent transportation technologies.

Twenty years ago, in addition to the tragic loss of life on 9/11, the attack was a wake-up call that focused our attention on the vulnerabilities of U.S. infrastructure. While I served as Deputy Executive Director of the Kentucky Transportation Cabinet in 2005, we had deployed CCTV and sensors to monitor roads and bridges. At that point, data was still largely siloed and fragmented, but over time these transportation data systems converged. Cybersecurity weaknesses in one system could jeopardize the safety of other systems in the converged data system. Shortly after that, connected vehicles communicating with the Internet, with transportation infrastructure, and with each other also created risks of those vehicles' systems being attacked by hackers trying to steal data, learn their locations, or take control of the vehicles' operations.

Around the same time, state and local transportation agencies began to introduce Information Technology (IT), including networked communications, and connect it to new and existing

---

segments of the National Highway System from cybersecurity threats. Sec. 1109. Surface Transportation Block Grant Program. Makes measures to protect a transportation facility otherwise eligible for assistance under this section from cybersecurity threats.

[5] Federal Highway Administration Office of Operations Guide on Transportation Management Center Information Technology Security, https://www.itskrs.its.dot.gov/sites/default/files/docs/fhwahop19059.pdf

[6] https://www.missionsecure.com/

Operational Technology (OT) such as traffic signals, cameras, and sensors. This created a new digital layer of road, bridge, and tunnel infrastructure overlaying their physical infrastructure. The state and local transportation agencies began to use real-time data and predictive analytics now available over their communication networks to operate their transportation systems with more precision, efficiency, and functionality, which led to safer roads. These agencies could respond to urgent events more quickly, change traffic signals in real time to reduce congestion, and even detect freezing and potentially dangerous road surfaces such as was done during and after my time in Colorado as executive director of the state's Department of Transportation.

Today we are on the cusp of digital transformation in transportation as dramatic as the period when the car supplanted the horse and buggy. The Internet of Things (IoT), autonomous and automated technologies, artificial intelligence and machine learning, electric vehicles, Mobility on Demand, advanced air mobility, and many other technologies have the potential to save lives, and make surface transportation safer, greener, smarter, and more equitable.

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 guides traffic movement, so the truck moves through the city traffic more efficiently. Automated enforcement allows inspections to happen at 30 miles per hour instead of the driver pulling over and remaining idle during the inspection. Smart truck parking helps the driver find a place to rest and maximizes their hours of service. Electronic devices log hours of service. GPS technology adjusts routing based on weather and traffic information.

It is important to speak about multi-purpose evolution when discussing technology – some things designed for singular purposes often produce additional applications. For example, with trucks, ITS America member WSP points out that electronic logging technology in the previous example also creates data that can be further analyzed and combined with vehicle sensors to flag unusual patterns or unexpected events for further security investigation or action. This is similar to how electronic toll collection data can also identify traffic congestion, an additional benefit realized through interconnected systems.

ITS is transforming how we maintain and build new roads and bridges by integrating technology into the infrastructure, including sensors and advanced monitoring systems that can track roadway and bridge conditions, which will alert state and local transportation agencies of any disruptions or extreme weather conditions.

An example of this is the Star City Bridge in West Virginia. The Star City Bridge is outfitted with more than 700 sensors that monitor measurements on the triaxial state of strains on the concrete, concrete crack initiation and growth, opening of joints at the bridge edges, steel girder bending/stresses, axial forces on the bracing members, and the angles and inclination of abutments. The bridge sensors also collect data on traffic weight, dynamic strain, temperature profiles of the bridge and climate data. West Virginia University, located near the bridge, uses the

bridge as a teaching tool, particularly in regard to the data on "deflection," the stresses placed on it at various locations and how loads, such as two trucks approaching each other from opposite directions, affect it.

The Indian River Inlet Bridge in Delaware is another example of a bridge instrumented with smart technology. It is equipped with 119 fiber optic sensors built into the pylons and support cables. The sensors measure stress on structural components, wind-related movement, and the penetration of road salt into the concrete. Each sensor has its own wavelength that will change due to stressors and alert the Delaware Department of Transportation, allowing it to make changes to traffic patterns or make targeted repairs to alleviate stress. This bridge was the first in the country to utilize this technology.

While advancements in technology have made the transportation system more connected than ever, this connectivity brings increased cyber risk – and these risks have the potential to threaten the system, the economy, and people's lives.

CYBER ATTACKS ON TRANSPORTATION

The nation's transportation assets and infrastructure are now as vulnerable to cyber threats as are other connected systems. Cybercriminals may have the opportunity to disrupt the American economy by targeting transportation systems and infrastructure due to these vulnerabilities.

U.S. Transportation Secretary Pete Buttigieg described the Colonial Pipeline attack as a "wake up call" that highlighted significant vulnerabilities in U.S. critical infrastructure. The Department of Homeland Security considers the Transportation Systems Sector to be one of 16 critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." The cybersecurity threat landscape is constantly evolving, and new vulnerabilities are discovered every day.[7]

Cyber threats are becoming increasingly sophisticated and target transportation's interconnected data systems, monitoring physical and digital networks. As cyber technology becomes more sophisticated, the threat from attack is moving from data breaches to interrupting physical critical infrastructure, exposing transportation operators to economic and reputational damage.[8] More important than these harms or damage to infrastructure is the potential harm to the nation's

[7] Federal Highway Administration Office of Operations Guide on Transportation Management Center Information Technology Security, https://www.itskrs.its.dot.gov/sites/default/files/docs/fhwahop19059.pdf
[8] https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf

transportation system. The figure here illustrates common cyber incidents within the transportation sector.

According to ITS America member Mission Secure, in the last three years alone, the United States has seen a 900 percent increase in attacks focused on Operational Technology used in traffic management signaling systems. ITS America member Southwest Research Institute (SwRI) notes that phishing emails, malware, and Denial-of-Service, as well as ransomware, are some publicly known and heavily used cyberattacks against state and local transportation agencies. Compromised Dynamic Message signs displaying various messages (e.g., "Zombies Ahead," "Hacked by Sun Hacker") have targeted state transportation agencies. As state and local transportation agencies migrate systems to the cloud, more vigilance is needed. More prevalent cloud attacks include stolen credentials, typically via phishing, exploitation of cloud misconfigurations, and vulnerable cloud application hacking.

ITS America member AECOM notes that the use of GPS to adjust routing based on weather and traffic information might have an associated threat of being spoofed via a cyberattack. If a related vulnerability were successfully exploited, a simple denial of service attack could be performed on a wide scale, causing delays to shipments and traffic flow on the highway. This could also be used as a targeted means of causing valuable freight to be re-routed to a specific road where police protection, traffic volume, and CCTV camera coverage are not as prevalent as on the main route. Sensors and monitoring systems on roads and bridges could be susceptible to similar attacks, with a malicious actor intentionally hiding the fact that a structural problem exists. Other vectors of attack could be the interception of transmitted sensor information (e.g., if weak or no encryption existed) or having stored diagnostic data leaked from compromised monitoring system databases. In the worst case, if not properly secured, this sort of information could get into the hands of a

malicious actor who is actively planning physical attacks on U.S. infrastructure and assessing potential targets.

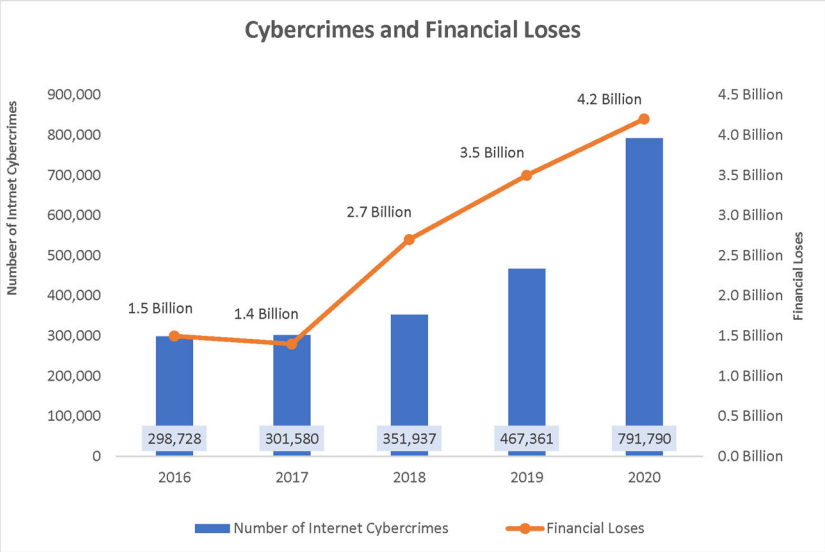
The number of attacks made on public and private organizations is growing at an alarming rate and becoming more sophisticated, notes ITS America member C. Douglass Couto, Senior Fellow, Center for Digital Government, and chair of the Transportation Research Board Cybersecurity Subcommittee. There are estimates in the millions per day. "We can defend against them day after day, but it only takes one vulnerability exploited to create havoc. The use of artificial intelligence thwarts these attacks," notes Couto. Investments in research to identify the next generation of cyber tools to defend against attacks is critical. The word cloud below from Couto illustrates the numerous cybersecurity concerns for transportation agencies and government leaders at all levels.

The COVID-19 public health emergency forced many organizations, including state and local transportation agencies, to rely more heavily on technology as people worked from home. More

than a third of U.S. households reported working from home more frequently than before the pandemic.[9]

Based on a report released by the Palo Alto Networks threat intelligence team Unit 42, organizations expanded their cloud workload deployments following the onset of the pandemic, but they also saw more cloud security incidents. Such incidents in the retail, manufacturing, and government industries rose by 402%, 230%, and 205%, respectively. These industries were among those facing the greatest pressures to adapt and scale in the face of the pandemic – retailers for basic necessities and manufacturing and government for COVID-19 supplies and aid.[10]

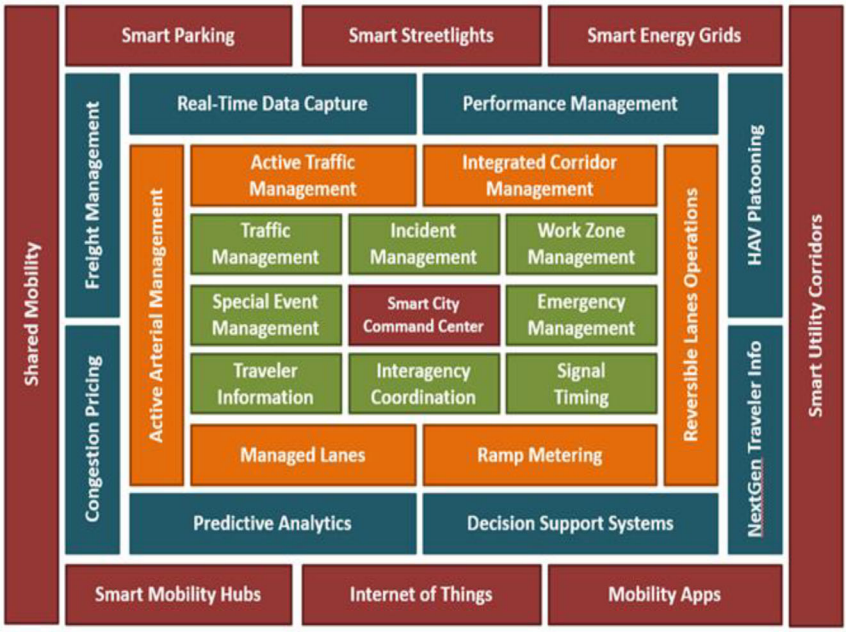
The chart below, based on the FBI 2020 Internet Crime Report data, illustrates a record number of cyber incidents in 2020 exceeding $4.1 billion in financial losses, which represents a 69% increase from 2019.



The following chart from AECOM illustrates all the functions and interfaces that need to be secured to protect transportation, and its users, from cyber threats. To reduce transportation's susceptibility to cyber threats, the transportation sector needs to ensure security not just for each

[9] https://www.census.gov/library/stories/2021/03/working-from-home-during-the-pandemic.html
[10] https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21 Find out more information about how malicious cyber actors have exploited the COVID-19 here: https://us-cert.cisa.gov/ncas/alerts/aa20-099a

of these boxes on their own, but also interconnectedly for when these functions interface with each other or interface with a command center.



According to Mission Secure, the increasing prevalence of connected, autonomous, and automated assets in our systems further exacerbates this problem. For example, connected and autonomous vehicles will increasingly rely on real-time, accurate data from traffic controllers, interacting directly with the entire traffic system. Any potential compromise to the car or controller would have adverse impacts on safety.

ITS America member Texas Department of Transportation points to an integrated city in the not so distant future in which automated and autonomous vehicles, including Personal Delivery Devices (PDDs), connected bikes and scooters, and other systems not yet developed will be operating in the same areas – sidewalks, bike paths, roads, intersections. Directly above them will be drones delivering packages, and potentially people, along managed low-level air corridors. Future urban traffic management will incorporate all these elements and it is critial that the entire system integrates strong cybersecurity systems.

Intelligent transportation technologies are making our country safer and more efficient - by moving people, data, and freight, they support the U.S. economy. We must, however, manage the vulnerabilities that come with a more complex system by meeting cybersecurity benchmarks that

increase adoption of security best practices, including by employing a zero-trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multifactor authentication and encryption.[11] Outdated security models and unencrypted data have led to compromises of transportation assets and infrastructure. Any potential vulnerability could have adverse impacts on safety.

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 investments necessary to protect our transportation system. Developing a resilient system begins with cybersecurity. As a former DOT director for two states, I am well acquainted with making tough choices about spending scarce resources. State and local transportation agencies must analyze their systems to identify where the greatest risks and weaknesses exist. A risk management plan is used to determine courses of action to mitigate and manage those risks.[12] The transportation sector needs to secure network infrastructure devices[13] and enforce domain security.[14]

ITS America member Michigan Department of Transportation (MDOT) notes that cybersecurity crosses several governmental jurisdictions and can be justified as part of several department missions. These include state and local DOT's, law enforcement, and others such as the National Guard or anti-terrorism agencies. When these agencies work together, it is important that new cyber vulnerabilities are not created by lack of coordination.

MDOT also notes that cybersecurity for transportation interests and providers is more challenging because the consequences are public and immediately affect people regardless of whether they are connected to a system, business, or process. A hospital under a ransom attack is threatened, but that threat does not affect people who are not connected in some way. An attack on a bank concerns people with savings there, but not necessarily the general public. An attack on an ITS roadside network access point can affect the personal safety of nearby pedestrians and all vehicles and their passengers communicating with that network.

[11] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/
[12] Federal Highway Administration Office of Operations Guide on Transportation Management Center Information Technology Security, https://www.itskrs.its.dot.gov/sites/default/files/docs/fhwahop19059.pdf
[13] https://us-cert.cisa.gov/ncas/tips/ST18-001
[14] https://www.circleid.com/posts/20210709-domains-a-critical-component-of-your-enterprise-risk-management/

A NATIONAL TRANSPORTATION CYBERSECURITY STRATEGY

ITS America and our members, in particular the New York City Department of Transportation, recommend a more robust national transportation cybersecurity strategy to make the digital layer of our transportation system safer, much like how Vision Zero strategies in New York City and elsewhere have saved lives and prevented serious injuries through engineering, education, and enforcement to make our streets and physical infrastructure safer.

Commercial aviation has long embraced a safe systems approach, and since 1997, the risk of a fatal crash has fallen 95 percent. In fact, in 2017, there were no passenger jet crash fatalities anywhere in the world – a previously unimaginable achievement. The same principles, applied to road traffic and focused on data-driven policy, have the potential to significantly reduce the burden in death, disability, and property damage from crashes in the United States

A more robust national transportation cybersecurity strategy should see all cyber attacks as defendable, provided we make the necessary investments before they occur. The strategy should include risk assessment, network security controls, and updated Information Technology – Operational Technology cyber-physical systems.

Adopting a national strategy can be achieved by ensuring that state and local transportation agencies and other transportation bodies adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework for cyber risk management and the Center for Internet Security (CIS) Critical Security Controls to improve their network cyber defenses as recommended in the Federal Highway Administration's Transportation Management Center Information Technology Security Final Report, September 2019. Specifically, we call on the federal governement to:

1. Provide state and local transportation agencies or other bodies funding at up to a 100% federal share, technical assistance, and best practices to modernize intelligent transportation systems, so they can adopt the NIST Cybersecurity Framework for risk management, CIS Critical Security Controls to improve network security, and upgrade or replace IT-OT cyber-physical devices and systems;

2. Establish a Department of Transportation grant program to provide grants to rural transportation agencies and areas of persistent poverty or income inequality to modernize intelligent transportation systems and adopt the NIST Cybersecurity Framework and CIS Critical Security Controls;

3. Reimburse state and local transportation agencies or other bodies that have been proactive and used state, local, or other funding sources to modernize intelligent transportation systems and improve cyber defenses according to the NIST Cybersecurity Framework for risk management and CIS Critical Security Controls; and

4. Allow flexibility in how transportation funds are used to invest in future cybersecurity workforce capacity. We see marked improvements in threat reduction when agencies hire full-time staff to manage their cybersecurity programs. However, there is a skyrocketing demand for cybersecurity-trained people making it harder to hire these skills across all sectors of our economy, including transportation.

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

***

ITS America acknowledges the contributions of members AECOM, C. Douglass Couto, HNTB, New York City Department of Transportation, Michigan Department of Transportation, Mission Secure, Southwest Research Institute, Texas Department of Transportation, and WSP.

Please email ITS America's Vice President of Public Policy and Legislative Affairs Ron Thaniel at rthaniel@itsa.org with testimony questions or comments.

---

[i] **ITS America's FAST Act Reauthorization Platform** Moving People, Data, Freight: Safer. Greener. Smarter. **Cybersecurity Policy**

1. POLICY: SAFEGUARD CRITICAL TRANSPORTATION INFRASTRUCTURE FROM CYBERSECURITY THREATS

As vehicles and infrastructure become more connected, our nation's transportation system faces increasing cybersecurity risks. Given the ability to cause loss of life and inflict significant economic damage in a highly visible manner, cybersecurity attacks directed at those producing or operating technologies travelling over or connected to U.S. roadways will intensify.

ITS America Recommendation

- Support policy that would provide states and localities funding and technical assistance to safeguard critical transportation systems that are more reliant than ever on connectivity to communicate and exchange data from cybersecurity threats.
- Amend 23 U.S. Code § 119 National Highway Performance Program, 133 Surface Transportation Block Grant, 167 National Highway Freight Program, and 148 Highway Safety Improvement Program to explicitly authorize that funds made available may be used to implement measures to protect highways, roads, bridges, and tunnels against cybersecurity threats to transportation infrastructure by allowing system access only as authorized and preventing malicious activity.
- Amend 49 USC Chapter 53 of Subtitle III Public Transit to protect public transportation systems from cybersecurity threats – Amend § 5302 definitions to explicitly include measures to protect against cybersecurity threats under the definition of Capital Project to allow system access only as authorized and prevent malicious activity.

- Amend 23 USC § 503(c)(4)(E) Advanced Transportation and Congestion Management Technologies Deployment Program to explicitly include measures to protect against cybersecurity threats as an eligible use of grants.
- Explicitly provide funding for risk assessments and planning services; developing best practices supporting cyber protection of legacy infrastructure, software and hardware solutions; implementing active and predictive threat monitoring services; deploying continuous monitoring and attack mitigation cyber security technologies and devices to harden traffic management systems and operations centers, creating Security Operations Centers (SOCs); and providing cybersecurity training to cybersecurity staff and other staff.
- Eligible activities include operating Intelligent Transportation System networks (ITS Networks) that enable infrastructure owner-operators to actively manage and protect transportation system such as secure traffic signal and sensor networks; secure wireless, wired, and fiber-optic networks; toll lane devices and systems; secure devices and systems to provide reliable and authoritative traveler information (VMS, websites, handheld device applications, in-vehicle information systems, etc.); active traffic management systems (lane use signals, variable speed limits); camera networks; weather-incident management systems; rock fall, flood, and avalanche detection systems; seismic detection systems; connected vehicle systems (Vehicle-to-Everything: infrastructure, other vehicles, people, cyclists, etc.); and Security Credential Management System (SCMS) that ensures connected vehicle technologies operate in a safe, secure, and privacy-protective manner.

Senate Committee on Environment and Public Works
Hearing Entitled, *"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"*
July 21, 2021
Questions for the Record for Shailen Bhatt

Senator Kelly:

1. With predictable weather, easily navigable terrain, and sunny-days year-round, Arizona is a leader in self-driving vehicle technology. There are more than 600 automated test vehicles on Arizona roads, and increasingly companies in Arizona are looking to test integrate traffic management systems with self-driving vehicles on surface streets. These advancements are exciting, but as you mention in your testimony, deploying these technologies must be done correctly. What additional guidelines or regulations do you believe are necessary on the state or federal level to ensure that we can deploy more integrated traffic management technologies, while accounting for the cyber threats these systems could be exposed to?

    a. How should the federal government, and states like Arizona, balance the need to protect infrastructure from physical threats, without stifling innovation?

RESPONSE: When we talk about cyber infrastructure, we are talking about the devices, signs, signals, cameras, and sensors along the highway that are included as part of the layer traffic management systems. In my written testimony, there is a chart from ITS America member AECOM. It illustrates all the functions and interfaces that need to be secured to protect transportation, and its users, from cyber threats. To reduce transportation's susceptibility to cyber-threats, the transportation sector needs to ensure security not just for each function within the box, but also each function with which the box interfaces. Imagine adding 10,000 autonomous and automated vehicles to the system that need to be connected to the infrastructure and managed by a traffic management system.

The evolution of automated and autonomous vehicles will increase the number of devices and communication systems along our roadways. Connected and autonomous vehicles will increasingly rely on real-time, accurate data from traffic controllers, interacting directly with the entire traffic system. Any potential compromise to the cyber infrastructure would have adverse impacts on safety.

ITS America supports more robust national transportation cybersecurity guidelines and regulations, including risk assessment, network security controls, and updated Information Technology and Operational Technology cyber-physical systems. We can achieve more robust national guidelines and regulations by ensuring that state and local transportation agencies and other transportation bodies adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework for cyber risk management and the Center for Internet Security (CIS) Critical Security Controls to improve their network cyber defenses as recommended in the Federal Highway Administration's Transportation Management Center

Information Technology Security Final Report, September 2019. Specifically, ITS America calls on the federal government to:

- Provide state and local transportation agencies or other bodies funding at up to a 100% federal share, technical assistance, and best practices to modernize intelligent transportation systems, so they can adopt the NIST Cybersecurity Framework for risk management, CIS Critical Security Controls to improve network security, and upgrade or replace IT-OT cyber-physical devices and systems;
- Establish a Department of Transportation grant program to provide grants to rural transportation agencies and areas of persistent poverty or income inequality to modernize intelligent transportation systems and adopt the NIST Cybersecurity Framework and CIS Critical Security Controls;
- Reimburse state and local transportation agencies or other bodies that have been proactive and used state, local, or other funding sources to modernize intelligent transportation systems and improve cyber defenses according to the NIST Cybersecurity Framework for risk management and CIS Critical Security Controls; and
- Allow flexibility in how transportation funds are used to invest in future cybersecurity workforce capacity. We see marked improvements in threat reduction when agencies hire full-time staff to manage their cybersecurity programs. However, there is a skyrocketing demand for cybersecurity-trained people making it harder to hire these skills across all sectors of our economy, including transportation.

While resources available from NIST, research organizations, and peer exchanges among DOTs, are raising awareness and improving their cyber resilience, solving the funding question will go a long way. ITS America appreciates the Senate Committee on Environment and Public Works for recognizing the growing risk and making cybersecurity explicitly eligible in the Committee's Surface Transportation Reauthorization Act, a centerpiece of the Infrastructure Investment and Jobs Act.

ITS America supports a federal framework to facilitate the safe testing, deployment, and integration of automated and autonomous vehicles into our transportation system. Key to this is robust cybersecurity of AVs. The federal government should be in the driver's seat on cybersecurity for AVs, working closely with automakers, the Auto-ISAC, top AV research institutions, and other cybersecurity experts. ITS America firmly believes that connected, automated, and autonomous vehicles have great promise. We also believe there should be national safety standards, including cybersecurity, for these vehicles and the infrastructure that connects to them.

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 cybersecurity 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 1 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 cybersecurity 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 cybersecurity 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's 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, as it referred us to a firm specializing in ransomware incident response, which helped us navigate our way through the event. 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 evolving, 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 electric 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 cybersecurity 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:]

Testimony of John P. Sullivan, P.E.
Chief Engineer, Boston Water and Sewer Commission

On Behalf of the
Association of Metropolitan Water Agencies

Senate Environment and Public Works Committee

"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"

July 21, 2021

Chairman Carper, Ranking Member Capito, and members of the committee: I appreciate the opportunity to represent the Association of Metropolitan Water Agencies (AMWA) at today's important hearing on "Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure."

I am John P. Sullivan, and for many years I have served as the 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. In addition, I currently serve on the board of directors of AMWA, as well as other state and national groups. I also chair the Water Information Sharing and Analysis Center, better known as WaterISAC, and serve on the Water Sector Coordinating Council, comprising the national water and wastewater associations,[1] which advises the U.S. Environmental Protection Agency and the Cybersecurity and Infrastructure Security Agency (CISA) on their security programs.

I testify today on behalf of AMWA, an organization of the nation's largest publicly owned drinking water systems. AMWA's members collectively serve more than 156 million Americans with quality drinking water. AMWA also operates WaterISAC – the water sector's Information Sharing and Analysis Center – on behalf of the sector. The center is a non-profit organization established in 2002 by the national water and wastewater associations, at the urging of EPA and the FBI, to provide utilities with critical information on physical and cybersecurity threats and

[1] The Water Sector Coordinating Council consists of the American Water Works Association, the Association of Metropolitan Water Agencies, the National Association of Clean Water Agencies, the National Association of Water Companies, the National Rural Water Association, WaterISAC, the Water Environment Federation, and the Water Research Foundation.

best practices for prevention and response. The designated information-sharing arm of the Water Sector Coordinating Council, WaterISAC is the most comprehensive and targeted single point source for data, facts, case studies, and analysis on water security and threats from intentional contamination, terrorism, and malicious cyber actors. WaterISAC member utilities currently serve 203 million people across the United States – about 60% of the U.S. population.

We commend the committee for holding today's hearing because protecting the nation's critical infrastructure against a growing range of cyber threats is an issue of increasing urgency. My testimony will provide an overview of the cyber risks faced by water systems, the sector's response thus far, and how Congress can help us move forward. I will also offer feedback on water sector cybersecurity provisions that the Senate approved in April as section 113 of the Drinking Water and Wastewater Infrastructure Act, commonly known as DWWIA (S. 914).

Water Systems' Cyber Risks

Like all critical infrastructure sectors, the water sector is an attractive target for cyber attackers. However, it is important to distinguish between two different types of cyber-attacks against water systems. The first are attacks against utilities' information technology systems, also known as business or enterprise systems. These include email systems, websites, and billing databases. In recent years water systems have reported a variety of such attacks, which include ransomware incidents, email compromise scams, and social engineering and phishing attempts. And while these attacks, if successful, can disrupt day-to-day business and compromise sensitive data, they, alone, would not have any impact on the treatment or management of drinking water or wastewater.

A more concerning type of cyber-attack would be that against a utility's industrial control system. Industrial control systems operate treatment processes, sensors, valves, pumps, and other utility infrastructure.

A demonstration of these risks played out this past February at the water system serving the city of Oldsmar, Florida. In this well-publicized case, an unknown malicious actor infiltrated the city's water treatment plant and made changes to chemical levels in the treatment process. According to the Pinellas County sheriff, the attacker accessed a computer in the treatment plant's control system using an application called TeamViewer. A plant operator observed two intrusions that were hours apart. In the second intrusion, which lasted about five minutes, the operator saw the mouse moving around as the malicious actor accessed various functions. One of these functions controls the amount of sodium hydroxide in the water, which the actor changed from about 100 parts per million to 11,100 parts per million. The operator in Oldsmar observed this change and immediately reversed it.

If the intrusion had not been detected in real time, reports say that it would have taken between 24 and 36 hours for the affected water to reach the distribution system, and prior to that point it most likely would have been detected by redundancies that are in place to check water quality before release. But this incident is emblematic of how bad actors can take advantage of cyber vulnerabilities that may be present in many of the nation's roughly 50,000 drinking water systems and 16,000 wastewater systems, and it is easy to imagine how the outcome might have

been far worse. What if, for example, the intruder was not immediately detected, and was able to manipulate pumps to drain a water tower, or restrict distribution to certain areas? Such an outcome not only would have undermined the public's confidence in their drinking water, but would have carried severe impacts on the community's infrastructure and public health.

It is important to recognize that organizations – from federal agencies to large and small businesses – can implement every best practice in the book and still suffer a cybersecurity attack. Notwithstanding that nation states have sophisticated methods of gaining unauthorized access to even the most secure systems, compromises can also be caused simply by one employee clicking on a malicious link in an email. So not only is it critical to implement the best technologies, but it is also critical to educate employees and to have incident response plans in place should attacks occur.

The Boston Water and Sewer Commission had its own experience with a cybersecurity incident in the form of an Egregor ransomware attack last year. While it complicated day-to-day business for many weeks and was costly to recover from, there was never any threat to public or environmental health, due to our business network being segregated from our control system, among other precautions. This saved the utility from suffering much greater impacts and is a best practice in any sector that uses industrial control systems, but this approach is not consistent across the sector. This is likely due to a lack of understanding of its importance and a lack of expertise and equipment to implement it.

WaterISAC was instrumental in helping us recover from this incident. The center referred us to a firm specializing in ransomware incident response, which helped us navigate our way through the event. In situations such as these, WaterISAC has access to a field of subject matter experts at other utilities and at private firms that it can tap in support of its members.

Water and Wastewater Systems Cybersecurity: State of the Sector

We know there is more the water sector could be doing to prepare for cyber attacks. According to a cybersecurity survey on water and wastewater systems - *2021 State of the Sector*[2] - released in June by the Water Sector Coordinating Council, adoption of cyber best practices varies across the sector. For instance, the Council found that while cybersecurity is an element of most water utility risk management plans, that is not the case for nearly 40% of respondents, which included many water systems serving less than 500 people, but in some cases those serving hundreds of thousands. On the whole we found that larger utilities – with more resources – have fewer challenges to implementing cybersecurity practices, while many smaller utilities lack funding and expertise.

The survey also found that the number one challenge for systems serving more than 100,000 people is creating a cybersecurity culture within the utility. For smaller systems, awareness of threats and best practices was the top challenge.

[2] waterisac.org/2021survey

Sector Efforts to Improve Cybersecurity

One resource available to the sector is WaterISAC, established in 2002 with seed money from EPA and subsequent congressional appropriations. A critical component of cybersecurity preparedness is having access to the latest cyber threat and vulnerability information and to best practices from subject matter experts. One of two dozen other ISACs across critical infrastructure sectors, WaterISAC annually issues hundreds of advisories, maintains a secure portal for members and hosts webinars and threat briefings. The center also receives incident reports and conducts threat analyses to help utilities stay ahead of the threat curve.

In more recent years, in collaboration with EPA, through the Government Coordinating Council, the water sector as a whole has recommended that utilities implement best practices and has offered resources to that end.

Among these is WaterISAC's free *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*, a set of best practices for the protection of information technology and industrial control systems. First published in 2012 and most recently updated in 2019, the *15 Fundamentals* provide straightforward but sometimes overlooked tasks like enforcing user access controls and performing asset inventories. Other recommendations in the guide address vulnerability management and creating a cybersecurity culture.[3]

Another key sector resource is the American Water Works Association's *Cybersecurity Guidance & Tool,* which is based on the NIST Cyber Security Framework. The AWWA guidance offers a sector-specific approach for implementing applicable cybersecurity controls and recommendations and is widely used.

WaterISAC and the sector associations also promote EPA tools and those offered by CISA, as well as small-system resources.

---

[3] The complete list of 15 water sector cybersecurity fundamentals, available at waterisac.org/fundamentals, consists of:

1. Performing Asset Inventories
2. Assessing Risks
3. Minimizing Control System Exposure
4. Enforcing User Access Controls
5. Safeguarding from Unauthorized Physical Access
6. Installing Independent Cyber-Physical Safety Systems
7. Embracing Vulnerability Management
8. Creating a Cybersecurity Culture
9. Developing and Enforce Cybersecurity Policies and Procedures
10. Implementing Threat Detection and Monitoring
11. Planning for Incidents, Emergencies, and Disasters
12. Tackling Insider Threats
13. Securing the Supply Chain
14. Addressing All Smart Devices
15. Participating in Information Sharing and Collaboration Communities

Congress took a step toward recognizing the importance of water sector cybersecurity in 2018 with the passage of America's Drinking Water Act, or AWIA (P.L. 115-270). That legislation updated section 1433 of the Safe Drinking Water Act, which was originally enacted following 9/11 with the goal of helping drinking water systems secure themselves against physical threats and terrorist attacks. Under AWIA, the program was revised to have utilities take an "all-hazards" look at potential threats, including risks to "electronic, computer, or other automated systems." June 30 of this year was the AWIA-imposed statutory deadline for all community water systems serving more than 3,300 people to certify to EPA their completion of a risk and resilience assessment that identifies such risks posed to the system, and within six months of this certification each community water system is further required to prepare an emergency response plan that outlines how the system will protect against the identified threats. The association views AWIA as a strong and useful step toward a more secure water sector, but more must be done.

A New Approach to Water Sector Cybersecurity

Many water systems are implementing best practices to safeguard their information systems and industrial control systems from attacks and fulfilling their missions to protect public health and the environment. However, the water sector is large and diverse, and we see room for improvement, as demonstrated by the *State of the Sector* report noted above. We recognize that the current, purely voluntary approach leaves utilities vulnerable to cybersecurity attacks that could endanger health and the environment.

AMWA believes more rigor and accountability is necessary in the adoption of best practices. Our members recognize that utilities can and should do more to, for instance, assess their systems, implement access restrictions, development response plans, and exercise those plans.

AMWA is eager to work with the committee, and the other sector associations to come up with a fresh approach – one that takes into account the urgency and complexity of cybersecurity and the diversity of the sector.

The association is aware of the interest in water sector cybersecurity by the Cyberspace Solarium Commission. AMWA looks forward to working with the commission as it engages on this topic.

We urge Congress to move carefully toward a solution that incorporates the advice of subject matter experts from the water sector and as well as lessons learned from other sectors. The nature of cyber threats is ever-evolving, and a requirement that may make sense with today's technology could quickly become outdated in years ahead. Any regulatory oversight of the sector's cyber activities must therefore remain as nimble as possible.

How Congress Can Help

One of the most effective ways for Congress to help the nation's water systems withstand cyber threats is to provide more resources to both water systems themselves and to EPA in its capacity as the Sector Risk Management Agency (Sector-Specific Agency) for the water sector. These resources could come in the form of additional grant funding to help individual water systems

implement actions to improve their cyber posture, initiatives to expand the reach of WaterISAC to all water systems nationwide, training and technical assistance to help water systems comply with best practices, and aid that facilitates access to sector-based resources that are available. Indeed, the *State of the Sector* survey cited resources such as these among utilities' top needs.

One promising model that this committee may wish to explore is based on provisions included in the Energy Infrastructure Act, which was approved by the Energy and Natural Resources Committee on July 14. Subtitle B of this legislation focuses on cybersecurity in the electric sector and includes direction for the Energy Department, in conjunction with the Department of Homeland Security and other federal agencies and sector stakeholders, to:

- Carry out a program to encourage electric utilities to implement maturity models, self-assessments, and auditing methods to assess their own cybersecurity posture;
- Establish an Energy Cyber Sense Program to test the cybersecurity of products and technologies intended for use by electric utilities;
- Offer financial incentives to encourage electric utilities to adopt advanced technologies that improve cyber defenses; and
- Implement a grant and technical assistance program to help electric utilities prepare for and respond to cybersecurity threats.

Perhaps most notably, the legislation would authorize $250 million over five years to support an Energy Sector Operational Support for Cyberresilience Program, which would include among its objectives efforts "to expand industry participation in E-ISAC," the Electricity Information Sharing and Analysis Center, WaterISAC's counterpart for the electricity sector. As the EPW Committee considers cybersecurity legislation for the water sector, a similar program, at EPA, aimed at increasing participation in WaterISAC, should be a key component.

As previously mentioned, WaterISAC currently counts among its members water and wastewater utilities that serve about 60% of the U.S. population. Some members serve as few as 2,000 people, but most members serve larger populations. However, only about 400 of the nation's nearly 50,000 community water systems and 16,000 wastewater systems are paying WaterISAC members that enjoy full access to all of the nonprofit's threat and vulnerability alerts, subject matter expertise, and other information.

Congress provided funding to get the center up and running in the first decade of the 2000s, but since that time the center has been funded exclusively through member dues. These dues are structured on a sliding scale - beginning at $270 per year - so as to be affordable for smaller utilities, but nevertheless many utilities are not able to take advantage of the resources available. At the same time, many thousands of utilities are simply unaware of WaterISAC. Unless more utilities are part of WaterISAC, then lack of awareness of threats will prevail.

WaterISAC member utilities have more and better information with which to build a security and resilience program than those that don't belong to the center.

Therefore, federal assistance to underwrite membership fees for systems serving fewer than 100,000 people and a federal program to increase awareness of the center would help get threat

information and best practices into more hands across the country. As noted in the *State of the Sector* report, the greatest challenge for smaller systems is awareness of threats and best practices.

We estimate that federal assistance at a level of just $6 million over three years would enable WaterISAC to expand service to cover thousands of additional water and wastewater utilities nationwide.

The Drinking Water and Wastewater Infrastructure Act

Finally, I would like to offer some reaction to the water sector cybersecurity provisions approved by the Senate in April within section 113 of DWWIA (S. 914). While AMWA believes these provisions were well-intentioned, we have identified a number of issues that could prevent the proposal from working as envisioned should it be enacted into law in its current form.

Section 113 would add a new "Cybersecurity Support for Public Water Systems" section to the Safe Drinking Water Act. The provisions would require EPA to work in conjunction with CISA to carry out several activities, including developing a "prioritization framework" to identify public water systems that "if degraded or rendered inoperable due to an incident, would lead to significant impacts on the health and safety of the public." But as drafted the provision raises a number of questions.

Most significantly, it is difficult to envision any public water system in the U.S. that, "if degraded or rendered inoperable" due to a cybersecurity incident, would not result in "significant impacts on the health and safety" of members of the public who are customers of that water system. Even if the affected system is a small utility serving only several dozen customers, those individuals would face significant health and safety impacts if their water service became unavailable for any length of time. As a result, the prioritization framework language does little to narrow down the focus to a meaningful subset of the nation's 50,000 community water systems. If the intent of the provision is to highlight public water systems where an incident could lead to the most widespread health and safety impacts, or impacts that would affect the greatest number of people, that should be specified.

The provision's reliance on the 44 U.S.C. 3552 definition of "incident" is also questionable. An "incident" is defined in that section of code as such:

> "means an occurrence that—
>
> (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
>
> (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

This definition does not limit "incidents" to those related to industrial control system vulnerabilities, or even cybersecurity in general. Therefore any "occurrence that constitutes a violation or imminent threat of violation of law, security policies, security procedures, or

acceptable use policies" would have to be captured in the prioritization framework – meaning that any focus on cybersecurity would be lost.

When developing the prioritization framework, EPA and CISA would be directed to consider "whether cybersecurity vulnerabilities for a public water system have been identified under Sec. 1433." However, EPA and CISA would have no way of knowing what has been identified by a water system under section 1433 of SDWA, because the Risk and Resilience Assessments and Emergency Response Plans completed by community water systems pursuant to that section are not forwarded to or shared with any federal entity. Instead, each community water system only certifies to EPA that the assessments and plans have been completed.

Should the prioritization framework succeed in accurately identifying a subset of water systems where a cyber attack could lead to the most significant public health impacts, nothing in the legislation would prevent this list from public disclosure. This means that nation states or individual actors who may wish to do harm to water systems could have access to a federal assessment of where a successful attack is likely to result in the greatest damage to public health.

Section 113 would elsewhere require EPA and CISA to develop a Technical Cybersecurity Support Plan that would identify public water systems in need of prioritized cybersecurity support, and report to Congress with "a list describing any public water systems identified . . . as needing technical support for cybersecurity during development of the Support Plan." But like the documentation produced during development of the prioritization framework, this list of public water systems in most need of cybersecurity assistance would not be protected against public disclosure, providing bad actors with information indicating where a targeted cyber attack is likely to result in the most damage.

Finally, section 113 would direct EPA and CISA to use their existing authorities "for providing voluntary support to public water systems and the Prioritization Framework." However, section 113's rules of construction only specifies that nothing in the section "alters the existing authorities of the *Administrator"* or "compels a public water system to accept technical support offered by the *Administrator"* (emphasis added). The rules of construction should also make clear that the language does not alter any existing authorities of the CISA director, and that public water systems are not compelled to accept technical support offered by CISA pursuant to this provision.

Overall, we understand the Senate's intent in attempting to develop a greater awareness of cyber risks to water systems through section 113 and providing mechanisms for selected water systems to voluntarily access aid. But AMWA believes the language as approved by the Senate is in need of significant revision to truly accomplish this objective without introducing new risks that could leave some water systems even more vulnerable to cyber threats. AMWA would be eager to work with the committee and the Senate to improve these provisions or draft a new version of a proposal through which water systems could be offered effective cyber assistance.

Conclusion

AMWA appreciates the opportunity to share our views on the cyber threat landscape facing the

nation's drinking water systems, and strategies Congress can take to help utilities respond to these challenges. I am proud of the work the water sector has done on its own to spread awareness of sound cyber practices, but additional resources and assistance from the federal government would go a long way toward ensuring the greatest number of water utilities are as prepared as they can be. AMWA stands ready to work with you to make this a reality.

Thank you again for the chance to testify today. I am happy to answer any questions you may have.

Senate Committee on Environment and Public Works
Hearing Entitled, *"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"*
July 21, 2021
Questions for the Record for John Sullivan

Senator Kelly

1. I wanted to discuss the security of water and wastewater infrastructure. As has been discussed in this hearing, the events earlier this year in San Francisco and Oldsmar, Florida underscored the real life and safety threats that cyberattacks pose to water infrastructure. In Arizona, any similar incident could be even more catastrophic – with water users all over the state cutting back on their water reserves as a result of water shortages along the Colorado River. That's why I was incredibly proud to support the Drinking Water and Wastewater Infrastructure Act earlier this year, which expands grant funding opportunities to help water and wastewater systems and also creates a new requirement for EPA to establish a Technical Cybersecurity Support Plan for water and wastewater systems. You addressed this briefly in your testimony, but can you expand upon why additional guidance from EPA for public water systems for how to prepare for cyber threats is so critical?

   RESPONSE: The nation's drinking water and wastewater systems serve cities and towns with a wide range of resources and capabilities. In fact, roughly 97% of the nation's 50,000 community water systems serve fewer than 50,000 people, meaning that they have relatively small ratepayer bases and are likely operated with minimal staff. It would be reasonable to expect that these smaller-utility workers would be primarily focused on keeping the water flowing and may not have the resources or expertise to stay apprised of the ever-evolving cyber threat landscape facing critical infrastructure.

   However, just because a small water system may not be focused on cybersecurity does not mean that a cyber-criminal will not focus on them. We know that utilities make attractive targets to hackers who wish to sow discord or undermine public institutions, so a cyber-attack that interrupts or interferes with the water supply of even the smallest water utility could have national implications for the public's confidence in their drinking water, not to mention the public health risks that would impact the customers of the affected water system.

   This is why additional guidance and resources for water systems on cybersecurity is so important. For small community utilities, even having a basic understanding of the threats – and suggested steps to mitigate those threats – can make a difference. After all, the Oldsmar incident involved outdated versions of software and less than robust password protections. With greater access to resources that promote cyber best practices, such as WaterISAC's *15 Cybersecurity Fundamentals for Water and Wastewater Utilities,* more water systems would be prompted to think about taking relatively basic steps to improve their security practices.

Just as valuable as the *15 Fundamentals* are the hundreds of water sector cyber advisories WaterISAC disseminates each year, along with alerts on vulnerabilities in the equipment and software our members use. The information that WaterISAC disseminates to the sector and maintains in its secure online library comes from many sources. In addition to the material produced by WaterISAC's analysts, WaterISAC identifies, analyzes, and shares relevant information from CISA, the FBI and other intelligence community sources, not to mention expert resources from subject matter experts in the private sector, the American Water Works Association, and from ISACs in interdependent sectors. As a nonprofit, we would like to be able to expand access to this critical information to thousands of utilities across the sector.

As my testimony noted, AMWA appreciates the rationale behind provisions in the Drinking Water and Wastewater Infrastructure Act that seek to identify and offer assistance to water systems that may be least prepared to withstand a cyber-attack. We do believe the language could be improved to ensure that any lists of at-risk water systems are protected from public disclosure, as that could direct hackers as to where to direct their attention. AMWA is eager to continue to work with the committee on this issue, both to promote helpful cyber guidance from EPA, and to increase water systems' access to existing, sector-based security resources like WaterISAC.

a. Once EPA completes this guidance, do you believe that the existing federal funding streams, both through the state revolving funds and through other discretionary grant programs, that water systems will have the resources needed to harden their infrastructure to cyber threats?

   RESPONSE: AMWA believes that a dedicated source of federal cybersecurity funding assistance for drinking water and wastewater systems is an idea that should be explored. While EPA does consider water security projects to be eligible for funding through the Drinking Water State Revolving Fund, that program is primarily used by water systems to help fund projects that have a direct correlation with public health improvements or that address the $472.6 billion in investments that are needed to maintain and improve the nation's drinking water infrastructure over the next twenty years, as estimated by EPA. Against these competing needs, many individual water systems may not choose to utilize these funds to support cyber improvements.

   AMWA supports the Drinking Water and Wastewater Infrastructure Act's creation of a new Midsize and Large Drinking Water System Resilience and Sustainability Program that will offer grants to help community water systems serving 10,000 or more people pay for projects to help withstand natural hazards or reduce cybersecurity vulnerabilities. This new funding

will be valuable to these water systems. However, the legislation will also reauthorize a similar Drinking Water Infrastructure Resilience and Sustainability Program that serves small (fewer than 10,000 people) or disadvantaged community water systems, but funds through that existing program cannot be used to address cyber vulnerabilities. As a result, the smallest water systems that are likely to have the least sophistication in preparing for and responding to cyber threats will have fewer cyber grant funding opportunities than larger water systems.

Additionally, America's Water Infrastructure Act of 2018 (P.L. 115-270) authorized $25 million in each of fiscal years 2020 and 2021 for an EPA Drinking Water Infrastructure Risk and Resilience Program to help water systems address identified security risks, including through "improvements to electronic, computer, financial, or other automated systems and remote systems." While these funds would certainly be able to be used by communities to address known cyber weaknesses, to date Congress has not appropriated any funding for the program, and no grants have been awarded.

In sum, AMWA would support the creation of a dedicated federal program to improve the cybersecurity of the nation's drinking water and wastewater systems, to ensure they suffer no lack of resources to harden their infrastructure to cyber threats. Additionally, because information sharing and threat awareness must be a key part of this effort, we believe funding should also be available to subsidize WaterISAC membership fees, particularly for drinking water and wastewater systems serving fewer than 100,000 people. A modest federal investment in this area, we believe, would make great strides toward improving the cyber resilience of the water sector at large.

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 and 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 cybersecurity 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 cybersecurity 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 cybersecurity.

However, any successful cyber attack 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 cyber attack 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 cybersecurity 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 cybersecurity program should be scalable, meaning it must recognize the complexity of water cybersecurity 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:]

Testimony of:

Sophia Oberton, MBA

Special Project Coordinator

Representing the:

Town of Delmar, Delaware and Maryland
Delaware Rural Water Association
Maryland Rural Water Association
National Rural Water Association

Before the:

U.S. Senate Committee on Environment and Public Works

July 21, 2021

Subject: *Cybersecurity of water infrastructure of small and rural local governmental authorities.*

Good morning, Chairman Carper, Senator Cardin and members of the Committee. I am Sophia Oberton, the Special Project Coordinator with the Town of Delmar in Delaware and Maryland. We have a population of approximately 4,500 persons. My title means I am the lead drinking water operator for the town. I hold a class 4 drinking water operators' license in both Delaware and 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 all small and rural communities in the United States through my affiliations with the Delaware, Maryland and National Rural Water Associations. I am joined by my mother, Ms. Linda Anderson, and Delmar's Town Manager, Ms. Sara Bynum-King.

Before getting into the substance of my comments, I want to personally thank you, Senator Carper, for being such a good friend and supporter of rural Delaware and rural USA. The rural and small town provisions in your recent legislation, "The Drinking Water and Wastewater Infrastructure Act of 2021," are very much appreciated and you made us so proud when you chose to announce the legislation at the 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 $1.9 trillion COVID-19 Stimulus Package otherwise known as the American Rescue Plan Act (ARPA).

We received $930,000 from Delaware and $2.8 million from Maryland. A significant portion of this funding will be earmarked for water and sewer projects by our local government - we are very appreciative of the assistance.

My three main messages here today regarding cybersecurity protection of small, rural and tribal communities' public drinking water infrastructure are:

First, small communities only operate to serve the public's interests. We are owned and governed by our local citizens through their elected local governments. We only exist to serve the public and are eager to take all feasible and necessary actions to protect the cybersecurity of our public drinking water supplies. This means that any federal initiative to protect the country's public water supplies should be assistance-based. We need help in the form of technical assistance on how to best implement the newest and most advanced cyber protection actions for our specific water infrasource as opposed to a regulatory construct. Additional federal regulation of cybersecurity in water supplies is not the appropriate policy because local governments are eager to adopt the best cyber policies. Again, we need help, not enforcement.

Second, the country's public drinking water supplies are different from other critical infrastructure sectors because we are local governments and nonprofits and because of the very large number of public water supplies; there are 49,775 Community Water Systems (CWSs) in the U.S. and 146,839 Public Water Systems (PWSs).[1]

And third, most U.S. Community Water Systems are small like my town of Delmar. 91percent (45,350) of the country's 49,777 Community Water Systems serve populations of less than 10,000 persons; 89 percent (40,332) serve populations of 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 cybersecurity system. The water cybersecurity systems of cities like Baltimore and Philadelphia are completely different from the systems of small communities like Delmar that are typical of over 90 percent of the U.S. water public water supplies. Large cities have very complex cybersecurity and SCADA systems to operate and protect their utilities. Because of their complexity, they also have many more potential targets for hostile actors and cyberattacks. On the other hand, their size and economies of scale provide them far greater financial and technical resources to protect their complex systems - and they are doing a very good job of protecting their water supplies. However, any successful cyberattack on a small community that results in drinking water contamination would result in causing psychological panic on a national scale as communities fear their own drinking water supply could be threatened. This is why small communities believe that protecting our water supplies from any cyberattack is just as important as protecting large communities. Large and small communities have a shared mission to protect and enhance the health and safety of our citizens.

We believe that any federal government policy for water cybersecurity must treat small and large communities very differently while recognizing the fundamental differences in the complexity of the water systems, financial resources, and technical capability. For a town the size of Delmar, a $1,000 dollar cost is a significant expenditure. We only have three licensed drinking water operators who need to implement all safety measures, manage all treatment of the water, read the meters, be on call at night for line breaks, manage the wells, the pumps, and our two water towers, take all the required U.S. Environmental Protection Agency (EPA) tests including the lead tests, operate the chlorine disinfection and pH adjustment processes which require constant monitoring, submit all the test results to the state, exercise our pumps and valves, sample the water for a variety of water quality parameters every day, complete and mail the federally mandated public water quality report every year, respond to any problems that can occur at any time, and keep the water safe and flowing to every citizens' tap every second of every day - including during the pandemic of the last year and half.

[1] U.S. EPA, Attachment 1.

In Delmar, we don't have a SCADA (supervisory control and data acquisition) control system or any interface with the internet regarding our water infrastructure assets and fixtures. On the other hand, we do have automated well-pumps, disinfection injection, sodium carbonate mixing technology and pressure monitoring systems. We have to be at the water treatment facility, however, to directly adjust the technological systems to maintain our water safety parameters. Suppose one of the water treatment technologies is not functioning properly. In that case, we receive an alarm message on our cell phone and we must get to the appropriate part of the treatment facility to fix the situation. These urgent messages are a common occurrence. We do have personal computers (PCs) in the office connected to the internet. However, these PCs do not interface with any of the water treatment technologies or our customers' records. We take precautions to protect any data and information on these PCs from potential cyberattacks.

Our wastewater utility does have a rudimentary SCADA system to adjust our secondary wastewater treatment process and ultraviolet light disinfection. Still, that SCADA system is not connected in any manner to the internet, and the operator must be at the wastewater treatment facility to use that SCADA system.

We want the Committee to know that when towns like Delmar need help in operating our water utilities, understanding new and complex federal Clean Water Act (CWA) and Safe Drinking Water Act (SDWA) requirements, receiving the required training to maintain our licenses, and learning about the latest cybersecurity practices, we call our rural water association 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. They have been essential to almost every small and rural community in Delaware, Maryland, and the other states. Circuit riders are funded by Congress each year through the appropriations process - and I would like to express deep gratitude on behalf of every rural and small community for this Committee's support of the funding for our circuit riders every year.

Just this past April, a circuit rider from Delaware Rural Water and another from Maryland Rural Water came to Delmar and spent an entire day helping us complete the very complicated EPA mandated Risk and Resiliency Assessment (RRA) that was authorized in the 2018 America's Water Infrastructure Act (AWIA). 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 rural water 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. This assessment included a review of our cybersecurity plans and every other possible threat (cyber, natural, terrorism, disgruntled personnel, etc.) to our water infrastructure. We certified the completion of the assessment to EPA on April 22nd (the deadline was June 30, 2021).

This exercise did reveal some vulnerabilities to the community, which I will explain shortly. However, it was not the mandated assessment that allowed us to focus on the greatest threats to the public water supply in Delmar - it was the time and experience of the circuit riders that educated us on possible vulnerabilities. It is relevant to note that cybersecurity is a very low to non-existent risk to our town. What the circuit rider did help us realize was that our simple hard-water infrastructure assets were likely our greatest vulnerability. Items like fencing and secure locks on any access to our storage towers, well-houses, pump-houses, and the water treatment technologies in the water treatment facilities' buildings are what we need to monitor and enhance constantly. We do have security and protection for all these assets, but they are likely our most significant vulnerabilities. Also, the circuit riders' assessment allowed us to observe that physical disruption of our drinking water supply is what we need to be most vigilant in preventing and planning for all contingencies. We rely on a series of pumps to keep the distribution system pressurized, the wells pumping, the storage tanks full, the town supplied with drinking water. Any physical harm to this system could leave the town without water, and we assessed this to be our significant threat as opposed to a cyberattack. Our nearest neighboring water supply is the City of Salisbury, Maryland, which is likely too far away to establish

any emergency inter-connection. Therefore, we are planning on all types of contingencies should any worst-case scenario occur.

Again, cybersecurity is not high on the list of potential threats to our community due to our size, limited use of the SCADA systems, and lack of connectivity to the internet. Our greatest threat identified within the parameters of the EPA RRA 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 a water distribution system such as line breaks and leaks. We also need to replace our old and failing terracotta sewer lines which are causing a severe inflow and infiltration (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. We would not want to see any new federal cybersecurity initiative or regulation result in the reprioritization of these limited resources to compliance with a new federal cyber program. And we simply can't just increase water rates to cover the cost of new federal requirements. Increasing water rates on our low-income residents can have the unintended consequence of forcing them to go without something they desperately need like food, housing, medical needs, etc.

Our Current Water Rates and Financing Information:

- **Drinking Water (based on meter readings)**: Water usage per 1,000 gallons: $4.00 for residential units and $5.00 for commercial units. In addition, there is an availability charge flat rate (based on Equivalent Dwelling Units): $17.45 for residential units and $17.45 for commercial units.
- **Sewer (based on meter readings)**: Per 1,000 gallons: $5.50 for residential units and $7:00 for commercial units. In addition, there is a sewer front footage charge (based on Equivalent Dwelling Units): $35.00 for residential units and $35.00 for commercial units.
- **Current Debt to Federal Funding Program** (U.S. Department of Agriculture, Drinking Water State Revolving Fund or Clean Water State Revolving Fund): $3,316,740.00

Two Essential Issues in Advancing Any New Cybersecurity Initiative in Rural and Small Communities:

Small, rural and tribal communities support the model that Congress adopted in crafting the Risk and Resiliency requirement in AWIA 2018 that (1) limited the federal government's authority to review the content of RRAs and (2) only required that communities "certify" completion of the RRA and not submit the content of the RRAs for review or federal cataloguing.

Any potential new federal cybersecurity program for U.S. public water supplies should use this model as the starting point and make additional improvements by adopting two essential principles or characteristics.

> One, any cybersecurity program should be very "scalable," meaning it must recognize that the complexity of water cybersecurity systems in a small community like Delmar is not remotely similar to a large community. Again, Delmar, with a population of 4,500 people, does not have a SCADA system or internet access for our drinking water systems. As we are larger than over 90 percent of the approximately 50,000 U.S. Community Water Systems, this situation is typical among many small communities. Like those of my colleague testifying with me today, large metropolitan drinking water utilities are immensely more complex and their communities have vastly more resources to take the necessary protective actions for their SCADA and cybersecurity systems. And as my colleague testifies, they are responsibly taking those precautions without any current federal mandate because that is their purpose - to provide for the public welfare.

> Second, any new federal initiative should also provide new technical assistance to help small communities with implementation. For the smallest communities, the burden of performance should be far less than the RRA program. Again, the scalability of the degree of commitment is essential to limit the federal program from resulting in the unintended consequence of wasting precious and limited local public funds. Over 54 percent of the approximately 50,000 U.S. Community Water Systems serve populations of less than 500 persons.[2] Many will not have full-time operators, will definitely need technical assistance to manage any new program, are fundamentally different in their complexity compared to a large city, and cybersecurity enhancement will very rarely be their priority for protecting their public.

The most successful approach for making progress in environmental compliance for small and rural Community Water Systems and overcoming their lack of technical resources has been the circuit rider concept, created by Congress, which provides all small communities with the shared technical resource of an expert with experience in water utility operations and compliance. This expert can travel directly to small, rural and tribal communities, as needed, to assist with rule compliance and generally eliminate the need for civil-enforcement. Additionally, the circuit riders only act in the community's interest which allows them to identify the most economical solution and provide the best advice for local decision-makers. What small and rural communities want and need is to know how to comply simply and affordably – and similarly, how to operate and maintain their water utilities. Consistent with our request that any new federal cybersecurity regulation not circumvent local priorities and result in unnecessary costs to limited public funds, we are likewise are concerned that any new mandate could distract the existing circuit riders' time and resources away from what small communities in Delaware, Maryland and the rest of states see as their most pressing concerns. We urge you to be mindful of this dynamic when considering any new federal policies for cybersecurity plans in the water sector.

The National Rural Water Association (NRWA) has urged Congress to adopt a plan that relies on these two essential principles or characteristics in any federal cybersecurity initiative.[3] Additionally, by collaborating the water sector, and utilizing the existing state rural water associations' network that water supplies rely on for security initiatives and education, the federal government could (1) rapidly assess all of the water supplies efficacy in protecting their cyberinfrastructure, (2) develop reasonable protocols to enhance protection, (3) provide assistance to any inadequate cyber protection plan, and (4) document the state of the cyber protection in all water supplies. Upon adoption/completion of a cybersecurity proposal, each community will have a documented security plan that could be verified and open to review as appropriate. Federal, state, and local authorities could easily track which communities have taken the initiative to secure their cyberinfrastructure. The contents of each plan could be combined with each community's RRA and Emergency Response Plans. Such an approach would promote local support for security initiatives essential to ensure security protection because only local experts can identify the most vulnerable elements in the community and detect immediate threats.

In closing, Mr. Chairman, I want to thank you again on behalf of all small and rural communities for your continued help and assistance. Moreover, I want to thank all the Senators on the Committee for your consideration of our issues. This Committee is very important to rural and small town America; every federal dollar that has been granted to the many thousands of small towns to build, expand, and maintain their drinking water and wastewater infrastructure through the state revolving funds was authorized by this Committee. Also,this Committee likewise authorized every federal regulation under the Safe Drinking Water or the Clean Water Act.

We are grateful to testify today and thankful for the numerous opportunities this Committee has provided rural America to testify and be included in the crafting of water and environmental legislation.

---

[2] U.S. EPA, Attachment 1.
[3] NRWA, May 12, 2021, Attachment 2.

Attachment 1.

U.S. EPA, Government Performance and Results Act Data (June 2021)

GPRA Inventory Summary Report

Population Size Category	<=500		501-3,300		3,301-10,000		10,001-100,000		>100,000		**# of Systems**	**Population Served Count**
	# of Systems	Population Served Count	# of Systems	Population Served Count	# of Systems	Population Served Count	# of Systems	Population Served Count	# of Systems	Population Served Count		
PWS Type Code												
CWS	26,977	4,548,387	13,355	19,229,892	5,018	29,511,268	3,960	114,113,454	445	147,693,996	**49,755**	**315,096,997**
NTNCWS	15,030	2,074,858	2,466	2,637,868	164	908,392	38	812,466	1	203,375	**17,699**	**6,636,959**
TNCWS	76,326	7,092,346	2,972	2,786,182	75	387,952	12	247,616			**79,385**	**10,514,096**
Grand Total	**118,333**	**13,715,591**	**18,793**	**24,653,942**	**5,257**	**30,807,612**	**4,010**	**115,173,536**	**446**	**147,897,371**	**146,839**	**332,248,052**

SUBMISSIONYEARQUARTER is equal to **2021Q1**
and NPM_CANDIDATE is equal to / is in **Y**

Attachment 2.

NATIONAL RURAL WATER ASSOCIATION
NRWA America's Largest Utility Membership

May 12, 2021

The Honorable Gary Peters
Chairman
Committee on Homeland Security & Governmental Affairs
U.S. Senate
Washington, DC 20510

The Honorable Rob Portman
Ranking Senator
Committee on Homeland Security & Governmental Affairs
U.S. Senate
Washington, DC 20510

The Honorable Bennie Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

The Honorable John Katko
Ranking Member
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Peters, Ranking Senator Portman, Chairman Thompson and Ranking Member Katko:

The National Rural Water Association's (NRWA) over 30,000 small and rural community members with drinking water and/or wastewater supplies are very eager to initiate a partnership with the U.S. Department of Homeland Security (DHS) to secure small and rural community water utilities from cyber-attacks. The U.S. has approximately 50,000 community water supplies and 16,000 wastewater supplies - typically under various forms of local governments.

Approximately 90 percent of these water utilities are small, serving fewer than 10,000 persons. As the two most recent water cyber-attacks in Florida and Kansas have indicated, small communities can be a target of cyber-criminals including international actors. By implementing a few relatively simple actions, these water utilities could greatly decrease their vulnerability to future cyber-attacks. With a small additional cost for system infrastructure, many water utilities can take immediate essential actions such as removing insecure remote access (SCADA protection), performing a risk assessment, raising awareness of the issue, applying firewalls, providing multi-factor authentication, securing user accounts, limiting access to accounts, inventorying mobile access devices, and implementing protective policies for former employees.

By collaborating with small and rural communities and utilizing the existing network that water supplies rely on for security initiatives and education, the department could (1) rapidly assess all small water utilities efficacy in protecting their cyberinfrastructure, (2) develop reasonable protocols to enhance protection, (3) provide assistance to any inadequate cyber protection plan, and (4) document the state of the cyber protection in all small water supplies. Upon adoption/completion of a cybersecurity plan, each community will have a documented security plan that could be verified and open to review as appropriate. Federal, state, and local authorities could easily track which communities have taken the initiative to secure their cyberinfrastructure. The contents of each plan could be combined with each community's vulnerability assessment and emergency response plan.

In the past, similar types of security initiatives have been uniquely successful because they expeditiously advanced measurable security initiatives in water systems with the support of the local communities. For compliance with the Bioterrorism Act of 2002, for example, over 90 percent of small community water supplies relied on the rural water cooperative approach for completing security vulnerability assessments (VA) in a matter of months – at no cost to the communities. The 2018 America's Water Infrastructure Act (AWIA) requires updating these assessments by June 30, 2021. However, no federal funding has been provided to assist with compliance. The compliance rate for the revised assessments should be dramatically higher due to the existing network and outreach. The AWIA requirement for communities to adopt revised VAs was appropriately crafted by Congress in such a way to allow each community to address and prioritize their own vulnerabilities. This type of local tailoring is essential to crafting the most protective security plans because every community has a unique set of vulnerabilities. It also has the additional benefit of promoting local support for security initiatives versus a uniform regulatory approach, which is often costly and results in local resistance because it forces communities to dedicate limited funding and resources to something they see as unnecessary.

We urge you to initiate a similar approach with the Department of Homeland Security to rapidly evaluate and improve the cybersecurity measure in all small water utilities. We have recently partnered with the Mission Critical Global Alliance (MCGA) to develop the necessary protocols for a comprehensive continuous cyber assessment and education program and we would be eager for DHS collaboration on the content of the protocols and support to implement the protocols. With DHS support, we believe we could assess, measure, and improve every small and rural community's water infrastructure in a matter of months.

Small and rural water utilities want to take all necessary precautions to protect their utilities and the public. What is needed is to know how to take the most appropriate actions and make them simple and cost-effective. Local support and responsibility are essential to ensuring security protection because only local experts

can identify the most vulnerable elements in the community and detect immediate threats. A national collaborative cybersecurity water supply protection initiative should result in communities focusing enthusiastically on enhancing local security based on local risks. The best cybersecurity protection of a water utility is an educated and responsible local governing structure and operator.

Again, we are eager to partner with DHS in assessing the needs of every small water utility. Together, we can provide the appropriate education and technical assistance to ensure all necessary protective actions are conducted in a timely manner. We can also provide the federal government and Congress with the documented baseline assessment of the cybersecurity statutes and corresponding corrective actions in all small water utilities in the U.S.

Thank you for your consideration,

Sincerely,

Matthew Holmes, CEO

CC: Senators Warner and Rubio, Select Committee on Intelligence
Senator King and Representative Gallagher, CyberSpace Solarium Commission
Anne Neuberger, Deputy National Security Advisor for Cyber & Emerging Technologies
Brandon Wales, Acting Director of the Cybersecurity and Infrastructure Security Agency

Image 1

Image 2

Image 3

Image 4

Image 5

Image 6

Image 7

Image 8

Image 9

Image 10

Image 11

Image 12

Image 13

Image 14

Image 15

Image 16

Image 17

Image 18

Image 19

Image 20

Image 21

Image 22

Image 23

Image 24

Senate Committee on Environment and Public Works
Hearing Entitled, *"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"*
July 21, 2021
Questions for the Record for Sophia Oberton

Senator Kelly:

1. I wanted to discuss the unique challenges smaller rural and disadvantaged communities face when it comes to cyber threats. In February of this year, the City of Kingman Arizona, which is a city of approximately 30,000 people in north-eastern Arizona, was the victim of a cyber-attack which disabled their water and wastewater utility's online bill pay system and the entire City's IT infrastructure was offline for days. Fortunately, the City of Kingman was able to receive quick support in responding to the attack. In addition to the FBI and Department of Homeland Security, the City of Kingman relied on support from the Arizona National Guard's Joint Cyber Task Force – which has received training from federal agencies on how to respond to cyber threats, but has a better understanding of the on-the-ground needs of local communities. Months after the attack the scope of the attack is still not fully understood. In a time of crisis, what advantages do you believe there are in having state-based teams – like the Arizona National Guard's Cyber Task Force – able to support communities during a cyber-attack?

    a. As this committee considers ways to help smaller communities prevent and respond to cyber threats, should the emphasis be on additional federal response teams, like FBI or DHS, or would state-based teams be more helpful to communities like Delmar?

Response, August 24, 2021 (Mike Keegan, Analyst and Sophia Oberton, Witness, on behalf of the National Rural Water Association).

What is needed in any crisis (natural disasters and intentional attacks) regarding a small community's public drinking water supply is immediate access to technical personnel and equipment. We need immediate help and know-how to fix the problem. The assistance has to be available when the community needs the help which is often nights, winters, after natural disasters, weekends, etc. Also, the assistance must be non-regulatory to gain the trust of the local communities. Every small community wants to provide safe water to protect their citizens and the environment, but they need to know, often with hands-on demonstration, just how to operate their water systems and respond to a natural or cyber crisis. The most beneficial type of assistance to build resilience against future cyber-attacks in small and rural communities would be expansion of the circuit rider-type statewide technical assistance positions to work under the direction of state rural water associations that are governed by small communities, as opposed to regulators, academia or consultants, to ensure the assistance best meets small communities' needs.

The most successful approach for overcoming the lack of technical capacity in rural America has been the "circuit rider" concept, created by Congress, which provides all small communities with the shared technical resource of an expert with experience in water utility operations and compliance. This expert can travel directly to small and rural communities, as needed, to assist with rule compliance, training, governance, O&M, etc. - and generally eliminate the need for civil-enforcement. What small and rural communities want and need is to know how to comply simply and affordably – and similarly, how to operate and maintain their water utilities. This model should be expanded under the Department of Homeland Security to address cyber-security in small community drinking water supplies.

Approximately 90 percent of these water utilities are small, serving fewer than 10,000 persons. As the episode in Arizona indicates, small communities can be a target of cyber-criminals including international actors. By implementing a few relatively simple actions, these water utilities could greatly decrease their vulnerability to future cyber-attacks. With a small additional cost for system infrastructure, many water utilities can take immediate essential actions such as removing insecure remote access (SCADA protection), performing a risk assessment, raising awareness of the issue, applying firewalls, providing multi-factor authentication, securing user accounts, limiting access to accounts, inventorying mobile access devices, and implementing protective policies for former employees.

By collaborating with small and rural communities and utilizing the existing network that water supplies rely on for security initiatives and education, the department could (1) rapidly assess all small water utilities efficacy in protecting their cyberinfrastructure, (2) develop reasonable protocols to enhance protection, (3) provide assistance to any inadequate cyber protection plan, and (4) document the state of the cyber protection in all small water supplies. Upon adoption/completion of a cybersecurity plan, each community will have a documented security plan that could be verified and open to review as appropriate. Federal, state, and local authorities could easily track which communities have taken the initiative to secure their cyberinfrastructure. The contents of each plan could be combined with each community's vulnerability assessment and emergency response plan.

In the past, similar types of security initiatives have been uniquely successful because they expeditiously advanced measurable security initiatives in water systems with the support of the local communities. For compliance with the Bioterrorism Act of 2002, for example, over 90 percent of small community water supplies relied on the rural water cooperative approach for completing security vulnerability assessments (VA) in a matter of months – at no cost to the communities. The 2018 America's Water Infrastructure Act (AWIA) requires updating these assessments by June 30, 2021. However, no federal funding has been provided to assist with compliance. The compliance rate for the revised assessments should be dramatically higher due to the existing network and outreach. The AWIA requirement for communities to adopt revised VAs was

appropriately crafted by Congress in such a way to allow each community to address and prioritize their own vulnerabilities. This type of local tailoring is essential to crafting the most protective security plans because every community has a unique set of vulnerabilities. It also has the additional benefit of promoting local support for security initiatives versus a uniform regulatory approach, which is often costly and results in local resistance because it forces communities to dedicate limited funding and resources to something they see as unnecessary.

We urge you to initiate a similar approach with the Department of Homeland Security to rapidly evaluate and improve the cybersecurity measure in all small water utilities.

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, 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 Evan 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 cybersecurity 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 mechanical 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 backward 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.

Cybersecurity 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 cybersecurity, 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 recov-

ering 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 cyber crime.

In 2016, 2017, 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 cybersecurity, 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. Cybersecurity 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 the 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 month 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:]

Written Testimony for the Record

Senate Committee on Environment and Public Works

"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"

Wednesday, July 21, 2021

Submitted by Evan Pratt, , American Public Works Association

Chairman Carper, Ranking Member Capito, and members of the Committee, on behalf of the American Public Works Association (APWA), I appreciate the opportunity to provide testimony during this important hearing on **Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure.** It is our intention that the testimony provided will serve as a resource for the Committee.

As background, I currently serve as the Water Resources Commissioner for Washtenaw County, Michigan, with a population of approximately 370,000, and I am a member of the APWA Government Affairs Committee. Today I am testifying on behalf of APWA and our more than 30,000 members across North America. APWA is the only association to collectively serve and represent all areas of public works responsibilities with members working in both the public and private sectors, providing expertise at the local, state, and federal levels. Cybersecurity is an increasingly important part of protecting our critical infrastructure assets and our citizenry. I'm a little embarrassed to say I am here today because I and many of my peers know we are behind on cybersecurity and we need help.

In 2016-17, I was part of a bi-partisan task force to assess the condition and funding needs of all infrastructure in Michigan. To be clear, the overall purpose of the report was to bring ROI (return on investment) of infrastructure investment into focus relative to the state economy and quality of life, and that report is still used today. I admit there was no discussion of cybersecurity at that time, nor were any recommendations included. I have learned and observed since then that cybersecurity is an issue that still has a very unclear risk assessment profile.

Public works professionals are first responders and have been recognized as such through Homeland Security Presidential Directive (HSPD) 8 signed by President George W. Bush in 2003. This is a designation that APWA members embrace with great pride especially when we prepare for, respond to, and assist in disaster recovery. We are responsible for protecting our critical infrastructure. Critical infrastructure includes all modes of transportation, water and sewage treatment plants, dams, reservoirs, pumps, stormwater drainage facilities, other flood control systems, and often a variety of electronic controls for these systems.

Electronic sensors and controls for water utilities are known as SCADA systems, which stands for Supervisory Control and Data Acquisition systems. SCADA systems serve as the "nerve center" for a multitude of public works facilities and functions. In the private sector, such as industrial plants and pipelines, similar systems are often called Industrial Control Systems (ICS). For the purposes of today's hearing this is where I will focus my testimony.

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 vulnerable points when deployed, especially with varied levels of agency cyber-awareness. And particularly in the common situation where agencies can only meet their SCADA needs by stitching together products from multiple vendors and/or internal app development.

Public works agencies across the country are also responsible for building, operating, upgrading, and maintaining our nation's water infrastructure. This can include dams, reservoirs, stormwater drainage facilities, and other flood control systems. These systems are critical for preventing severe floods, and any attack that compromises them could endanger nearby communities. As technology advances and these systems become increasingly automated and connected, it will be critical for Congress to consider various strategies that safeguard our communities from potential cyberattacks on critical infrastructure. APWA's water resiliency policy priorities outline specifically how Congress can work with public works agencies to safeguard our infrastructure and protect public health.

Flood control systems are critical for mitigating severe wet weather. It is essential for Congress to consider strategies to safeguard our communities from potential cyberattacks on these increasingly automated and connected systems. Congress can support our flood control and other water infrastructure through continued and flexible federal funding, financing and regulatory streamlining to help ensure public works agencies have the resources to protect against cyberattacks.

About 52,000 community water systems operate in the United States, providing water to more than 286 million people year-round. Most systems are run by local governments; many are very small. Small water utilities often do not have their own IT or cybersecurity staff. They typically are part of city or county governments, but those too may not have the staff or resources to ensure that cybersecurity is strong.

I could spend hours specifically describing how far behind hundreds of agencies are, including a breach at my county. In the interest of time, I will just say that we can find an APWA member in your district with a story closer to home. In short, many, many government agencies have historically viewed IT infrastructure as an optional buy-up versus necessary investment. Further, the SCADA marketplace is less mature on cybersecurity than say the financial or medical software markets.

The challenges public works professionals face today have grown to include the responsibility of safeguarding the nation's critical infrastructure from cyberattacks. Public works professionals must be prepared to not only mitigate potential damage, but they simultaneously may also be called on to respond to and or repair any damage caused physically or otherwise from a cyber breach. Recent incidents around the nation have raised red flags therefore we must remain vigilant in protecting these valuable assets that keep our nation operating. Today I look forward to sharing with you APWA's recommendations to address cybersecurity protection for our physical infrastructure. APWA understands our infrastructure and cybersecurity are interconnected and function as one on many occasions. I have included copies of APWA's public policy priorities for the 117th Congress with this testimony for the Committee's reference. These priorities, drafted by our Government Affairs Committee and approved by our Board of Directors, are reviewed and updated prior to each new Congressional session.

APWA offered strong support of the Disaster Recovery Reform Act (DRRA) when it was initially offered as a stand-alone bill during the 115th Session of Congress. Becoming law on October 5, 2018, as part of the Federal Aviation Administration Reauthorization Act of 2018, Public Law No: 115-254, the federal government now has additional tools to emphasize what public works professionals have long identified as the most important aspect of dealing with disasters – mitigation efforts. Particularly efforts to safeguard our nation's critical infrastructure such as water treatment facilities and SCADA systems. A key provision of DRRA amended the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), modifying the Pre-disaster Hazard Mitigation Grant Program. The modification permits the use of technical and financial assistance to establish and carry out enforcement activities to implement codes, specifications, and standards that incorporate the latest hazard-resistant designs – a valuable tool for public works professionals.

Efficient and effective communication between emergency responders, public works included, is critical for preparedness, response, and recovery operations. Public works agencies depend on reliable interoperable emergency

communications systems that connect them to other responders during response and recovery operations--including law enforcement, fire, and emergency medical professionals. APWA has been an active partner with FirstNet and provide an APWA member to the Public Safety Advisory Committee (PSAC).

With respect to this hearing, APWA believes the following aspects of our policy priorities should be highlighted and considered by this Committee to enhance our nation's ability in both the public and private sectors to address disaster readiness and strengthen our cybersecurity:

- The federal government must share threat information and provide technical support to state, local and tribal governments in order to protect computer networks and other related critical infrastructure during times of disaster governments to enhance cybersecurity. One way may be by establishing Voluntary National Cybersecurity Guidelines and include public works in crafting these recommendations. APWA fully supports the use of interagency and organization task forces to coordinate implementation of Stafford Act rules and programs, as well as issues related to critical infrastructure protection. This would include maintaining the use of cross-sector task forces and study groups. APWA looks forward to continuing to be involved in federal task forces and other groups committed to preparing for, responding to, and recovering from disasters.
- Standardize and utilize important tools to protect these critical assets, including SCADA systems, possibly consistent with tools for other ICS system protections.
- Comprehensive cybersecurity training for public works professionals to prevent and mitigate cyber intrusions, including increasing training opportunities to provide first responders with the tools to harden their facilities against potential breaches and or failures caused through malicious or accidental actions
- Continue and fully fund the Federal Emergency Management Agency's (FEMA) Emergency Management Performance Grant Program (EMPG). This program assists state, local, tribal, and territorial governments by providing direction, coordination, and guidance to ensure that an emergency preparedness system exists for all hazards.
- Encourage effective asset management strategies. More coordinated, cooperative, and communicative infrastructure management strategies that utilize comprehensive planning, data, and analytical methods will ensure that municipalities can effectively work with federal and state partners to respond to cyberattacks.

- Provide robust federal funding through programs including the State Revolving Funds, Water Infrastructure Finance and Innovation Act (WIFIA) loans, and Rural Utilities Service loans & grants, Public Water System Supervision grants, and the Public Works and Economic Development program making cybersecurity specifically eligible for funding.
- Financing mechanisms for water infrastructure investment at the local level should be preserved and enhanced, to allow local governments to better invest in cybersecurity. Lifting the cap on Private Activity Bonds for water infrastructure and restoring advance refunding of tax-exempt municipal bonds can assist this goal.
- While APWA supports efforts to encourage state and local governments increase cybersecurity of their infrastructure, Congress should continue to ensure state and local control regarding public works projects. Local officials know their communities best.
- APWA opposes unfunded mandates that would overly burden state and local governments as they construct, maintain, and operate critical infrastructure.
- APWA recommends investment in physical and cybersecurity programs to ensure secure water resources and protect public safety. Operators of flood control infrastructure utilize automation and connected technologies which can be vulnerable to cyberattacks, and federal resources should be directed at enhanced cybersecurity of this infrastructure.
- The federal government's Environmental Protection Agency (EPA) or Department of Homeland Security (DHS) may be the proper departments to lead an effort to standardize and utilize important tools to secure communications protocols to protect these critical assets, including SCADA or ICS systems.
- APWA additionally recommends that financing mechanisms for investment in water infrastructure at the local level be preserved and enhanced to ensure that local governments have the resources to invest in the cybersecurity of their flood control infrastructure. This can be accomplished by preserving the tax-exempt status of municipal bonds, lifting the cap on Private Activity Bonds for water infrastructure, and restoring advance refunding of tax-exempt municipal bonds.
- I would urge Congress to consider acting through legislation or working with federal partners on regulatory steps. The federal government should likewise include public works in consultations pertaining to any proposed telecommunication modifications that may impact right-of-way, thereby allowing an additional

expert voice for consultation at the state and local government level to help map out where communication may be located as it may need to be accessed during an emergency.

- APWA believes the Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA) are two key components within DHS. We recommend DHS evaluate implementing practices to award grants based on estimates. Implementing these estimate-based grants would allow states to disburse funds to applicants up front (where state laws allow for such payments), rather than through the later reimbursement of actual costs. Congress enabled various pilot programs as part of the Post-Katrina Management Reform Act, Public Law 109-205, however those programs have expired. APWA supports enacting many of these pilot programs as permanent additions to the Stafford Act.

Thank you to the Committee for holding this important hearing and allowing me to provide testimony. APWA stands ready to work with you towards finding effective methods to support and safeguard our infrastructure and the American public. I sit before you today because this sector is scrambling to catch up and all agencies are not on top of this – I look forward to answering any questions you may have.

Attachment: APWA's public policy priorities for the 117th Congress--*Surface Transportation Reauthorization, Water Resiliency,* and *Emergency Management.*

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 licensures?

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. OK.

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 cyber attack 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 o'clock 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 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 cybersecurity?

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 cybersecurity 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 cybersecurity. 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 e-mail, 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 cybersecurity.

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 cybersecurity?

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 backward 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 e-mail, despite the training we had, and it takes constant training. That is the biggest problem for the large utilities. Cybersecurity, the element of people watching out all the time. Everyone assumes that e-mail comes in, it looks good, let's open this attachment.

Senator WHITEHOUSE. You click the attachment, and suddenly 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?

[Laughter.}

Senator WHITEHOUSE [continuing]. 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 it 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 APWA 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. OK.

Mr. Sullivan.

Mr. SULLIVAN. I heard them, and I would like to add that there needs to be funding for the smaller 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. All right, 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 thought 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 cybersecurity, 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 cybersecurity 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 work force 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 that; 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 thoughts?

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 cyber attacks 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 any 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 e-mails 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 e-mails from the IT department, and we test to see who hits them. Invariably, somebody opens up an e-mail, 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 I want to make sure to, in my limited time, 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 cybersecurity 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 OK; 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, the 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 cybersecurity. Committees like EPW are showing the importance of cybersecurity 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, as always.

Mr. Sullivan, in your testimony, you stated that larger utilities with more resources have fewer challenges to implement cybersecurity 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 OK, 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 carrots.

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, No. 1, you have got 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, you 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 the 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 pipes, 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.

Senator Markey, I don't know if you know John 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, 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 cyber attacks?

Mr. SULLIVAN. Well, Senator, there is money needed. However, the larger cities are able to, because of their work force 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 just up what you are willing to pay in order to protect against the sinister side of cyber space, 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 begin 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 with 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, OK, 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. That was, now, 11 years ago. Otherwise, we would have already had a mandate out there that utilities would 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, OK?

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's 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 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 work

force. 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 work force 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 work force 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, sort of like 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 and 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 on 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 got 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 then 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 start up, to do electronic sensing and controls.

So I would say my first 5 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 2 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 a top priority because we make up the majority of the water systems across the country.

Senator CARPER. OK, 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 win 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 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 work force 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. OK, 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 are there to 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 board. 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 toward 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 cybersecurity 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 relating to today's hearing.

Hearing no objection, so ordered.

[The referenced information follows:]

July 21, 2021

The Honorable Thomas R. Carper
Chair
The Honorable Shelley Moore Capito
Ranking Member
Senate Committee on Environment and Public Works
456 Dirksen Senate Office Building
Washington, D.C. 20510

Comments Offered on Hearing,
"Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure"
on July 21, 2021

Dear Chairman Carper and Ranking Member Capito,

The American Water Works Association (AWWA) asks to submit for the hearing record the following comments on cybersecurity issues facing the drinking water community.

AWWA thanks the Senate Committee on Environment and Public Works for addressing the vital issue of cybersecurity threats to our nation's critical infrastructure. Among the most critical of these infrastructure sectors is the water sector. A safe and reliable drinking water supply is necessary to protect public health and safety, and to ensure a community's economic viability. It is easy to forget that the water from a fire hydrant comes from a drinking water utility.

Our organization is very much aware of cyber threats posed by malevolent actors. Therefore, we have developed resources to help water systems of all types assess potential cyber vulnerabilities in both enterprise and operational technology systems. AWWA's Cybersecurity Guidance and Assessment Tool is a sector-based approach for implementing the National Institute of Standards and Technology cybersecurity framework prepared under Executive Order 13636. In addition, this resource facilitates compliance with the cybersecurity provisions in Section 2013 of America's Water Infrastructure Act (AWIA) of 2018.

We also recognize the dynamic and evolving nature of cyber threats, and that all water systems need to be vigilant in managing this risk. AWWA is continuously working to build capacity and educate water professionals on actions that can be taken to manage cyber threats. We believe that a continued and strengthened partnership between the water community, Congress, the U.S. Environmental Protection Agency (EPA), the U.S. Department of Homeland Security (DHS) and others is essential.

In that light, we make the following recommendations:

- Sharing of cyber threat information is essential to helping water sytems mitigate identified threats. However, in many cases the information provided by federal partners lacks the necessary context to facilitate quick action by all systems. Often there is an

assumed level of cyber expertise that is necessary to act on the information provided, which makes it difficult for some entities to take action. Enhanced collaboration with water sector subject matter experts and EPA and DHS would improve the utility of the advisories provided. The Water Information Sharing and Analysis Center (WaterISAC) provides a venue for this type of interaction and would benefit from funding support through EPA's general fund to increase water utility participation and access.

- Federal loan and grant assistance is essential in expediting the implementation of cybersecurity controls to aid water systems in mitigating vulnerabilities that may be identified based on assessments prepared under AWIA. Drinking water utilities are facing significant cost burdens as a result of continuing needs associated with aging infrastructure and new regulatory obligations associated with lead service line removal, and anticipated requirements associated with treatment for per- and polyfluroalkyl substances and other contaminants under regulatory review. The provision in HR 3684 that authorizes $50 million annually to support drinking water resilience is an excellent step forward in supporting this need, but given the spectrum of potential uses for this money, it may not suffiently address the actual need.

- In considering assistance to local governmental bodies in dealing with cyber threats, we encourage Congress to look to H.R. 5823 from the last session of Congress, the State and Local Cybersecurity Act. It would have established a program to provide grants to states that they in turn could use to work with local governments in enhancing their preparedness for cyber attacks. Many water utilities are components of local municipal government and would therefore benefit from such a program.

- Technical assistance and training is a critical component in supporting capacity development in the water sector. AWWA encourages Congress to consider options to continue and expand the the delivery of key resources such as those deployed by AWWA under a grant from the U.S. Department of Agriculture. This outreach has been very effective in supporting small systems in building awareness and supporting the implementation of foundational cybersecurity best practices.

- AWWA welcomes the opportunity to collaborate with federal partners to examine opportunities to enhance cybersecurity protection measures that can be implemented by water systems. Engagement with subject matter experts with operational experience in the water sector is essential in examining any approachs, especially given the diversity in water system size and operational complexity.

Again, we thank the committee for addressing this vital and timely topic, and offer the expertise and experiences of our membership and staff as you investigate solutions to the cyber threats facing the nation's water systems.

Sincerely,

G. Tracy Mehan, III
Executive Director for Government Affairs
American Water Works Association
tmehan@awwa.org

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.

Thank you.

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

○