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.