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

On Behalf of the
Water Information Sharing and Analysis Center

Before the
House Committee on Transportation and Infrastructure

Hearing on
"The Evolving Cybersecurity Landscape:
Industry Perspectives on Securing the Nation's Infrastructure"

November 4, 2021

Chairman DeFazio, Ranking Member Graves, and members of the committee: I appreciate the opportunity to appear at today's hearing on "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's 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 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 am also a member of the board of directors of the Association of Metropolitan Water Agencies and the National Association of Clean Water Agencies, and serve on the Water Utility

[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.

Council of the American Water Works Association.

I testify today on behalf of WaterISAC, 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 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 206 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 and wastewater systems, the sector's response thus far, and what we can do looking forward.

Water and Wastewater Systems' Cyber Risks

Water and wastewater systems are an attractive target for cyber attackers, and the implications of an attack could be significant. This is why water, along with transportation, energy, and communications, are the four "lifeline functions" designated by the Department of Homeland Security. This means that the operations of these sectors are so critical that any disruption or loss will directly affect the security of other critical infrastructure sectors as well.

However, it is important to distinguish between different types of cyber-attacks that could target water and wastewater 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 and wastewater 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 target a utility's industrial control system. Industrial control systems operate treatment processes, valves, pumps, and other utility infrastructure.

Last month EPA published a joint cyber advisory along with the FBI, Cybersecurity and Infrastructure Security Agency, and NSA outlining "Ongoing Cyber Threats to U.S. Water and Wastewater Systems."[2] The advisory featured input from WaterISAC and summarized some common cyber threats to water and wastewater systems, recommended mitigation actions, and resources for systems to access. It also cited several cyber intrusions against U.S. water and wastewater systems since last year, including incidents affecting utilities in California, Maine, Nevada, New Jersey, and Kansas. While none ultimately affected public health or environmental

[2] https://us-cert.cisa.gov/sites/default/files/publications/AA21-287A-Ongoing_Cyber_Threats_to_U.S._Water_and_Wastewater_Systems.pdf

quality, the growing number of incidents makes clear that utilities must be prepared to defend against and respond to these attacks.

One of the most-publicized recent cyber intrusions against a U.S. water utility played out this past February at the drinking water system serving the city of Oldsmar, Florida. In this 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 water service but would have carried severe impacts on the community's environmental, fire protection, and public health.

With wastewater systems, one danger is that an attack can disable the treatment train or the pumps that move treated and untreated sewerage from one point in the process to another. A successful attack could release large amounts of sewerage into rivers and streams, harming the natural ecology of the receiving waters, creating a direct public health risk and also contaminating sources of drinking water.

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 water and wastewater systems. This is likely due to a lack of understanding, among many utilities, of its importance and a lack of expertise and budget to implement it.

WaterISAC was instrumental in helping Boston Water and Sewer recover from this incident. The center referred the utility 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 and wastewater sector could be doing to prepare for cyber-attacks. According to a cybersecurity survey on water and wastewater systems - *2021 State of the Sector*[3] - 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 utility risk management plans, that is not the case for nearly 40% of respondents, which included many 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.

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 portal for members and hosts webinars and threat briefings. The center also receives incident reports and conducts threat analyses to help water and wastewater 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

[3] waterisac.org/2021survey

performing asset inventories. Other recommendations in the guide address vulnerability management and creating a cybersecurity culture.[4]

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 through AWWA and the Department of Agriculture.

In terms of federal oversight of the sector's cybersecurity drinking water and wastewater systems are not subject to the same requirements. On the drinking water side, America's Water Infrastructure Act of 2018 (P.L. 115-270) requires drinking water utilities, under the oversight of EPA, to periodically take an "all-hazards" look at potential threats, including risks to "electronic, computer, or other automated systems." This provides an opportunity to evaluate potential threats and develop response measures. However, there is no statutory requirement for wastewater systems to take similar actions.

A New Approach to Water Sector Cybersecurity

Despite these differences, both water and wastewater 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 and wastewater sector is large and diverse, and we see room for improvement, as demonstrated by the *State of the Sector* report noted above. The current approach could leave utilities vulnerable to cybersecurity attacks that could endanger health and the environment.

[4] 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

One of the most effective ways for Congress to help the nation's wastewater systems withstand cyber threats is to provide more resources to both the systems themselves and to EPA in its capacity as the Sector Risk Management Agency (Sector-Specific Agency) for the water and wastewater sector. These resources could come in the form of technical assistance programs to help medium and small wastewater systems, additional grant funding to help individual wastewater systems implement technology upgrades and secure external services, initiatives to expand the reach of WaterISAC to all wastewater systems nationwide, assessment assistance, and training to help wastewater systems comply with best practices. Indeed, the *State of the Sector* survey cited resources such as these among utilities' top needs.

One promising model could be based on provisions included in Section 40125(c) of the Infrastructure Investment and Jobs Act. This proposal aims to improve the cybersecurity of bulk power systems and would authorize $250 million over five years to support a new Energy Sector Operational Support for Cyberresilience Program at the Department of Energy. Among the objectives of this program would be supporting efforts "to expand industry participation in [Electricity]-ISAC," the Electricity Information Sharing and Analysis Center, WaterISAC's counterpart for the electricity sector. Should the Transportation and Infrastructure Committee develop legislation related to cybersecurity in the wastewater sector, a similar EPA program aimed at increasing participation in WaterISAC should be considered.

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 $100 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 small and medium-sized water and wastewater systems 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 provide a broader array of services to water and wastewater systems nationwide. Specifically, this level of funding would be used to cover the cost of membership for thousands of small and medium systems, expand our threat analysis capabilities, conduct exercises and training, and offer technical support to utilities.

Conclusion

WaterISAC appreciates the opportunity to share our views on the cyber threat landscape facing the nation’s water and wastewater systems, and effective stragegies to help utilities respond to these challenges. I am proud of the work the water and wastewater 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 and wastewater utilities are as prepared as they can be. We stand ready to work with you to make this a reality.