ASSOCIATION OF
METROPOLITAN
WATER AGENCIES

LEADERS IN WATER

1620 I Street NW, Suite 500
Washington, DC 20006

P 202.505.1565
amwa.net

February 6, 2024

The Honorable Andrew Garbarino
Chairman
Subcommittee on Cybersecurity and
Infrastructure Protection
U.S. House of Representatives
Washington, DC 20515

The Honorable Eric Swalwell
Ranking Member
Subcommittee on Cybersecurity and
Infrastructure Protection
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Garbarino and Ranking Member Swalwell:

The Association of Metropolitan Water Agencies (AMWA) appreciates the opportunity to submit this statement for the record of today's hearing on "Securing Operational Technology: A Deep Dive into the Water Sector." AMWA's members provide quality drinking water to more than 160 million Americans from coast to coast, and the threat of cyber intrusions and malicious attacks is a growing concern to these water systems as well as other critical infrastructure owners and operators. We commend the subcommittee for looking into this important issue.

As we recently testified before the House Subcommittee on Environment, Manufacturing, and Critical Materials[1], drinking water systems represent an attractive target for cyber attackers, and a successful attack could not only threaten water quality and public health, but also undermine Americans' confidence in their drinking water nationwide. The recent breach of an industrial control system device at Pennsylvania's Municipal Water Authority of Aliquippa[2], along with those at several other water systems, was just the latest example of why utilities of all sizes must remain on guard against cyber intrusions.

Given the complexity of the issue, it is essential that stakeholders and the federal government maintain open lines of communication and pursue cooperative approaches to closing cyber gaps. While drinking water systems will primarily work through EPA in its capacity as the Sector Risk Management Agency for the Water and Wastewater Systems Sector, our members also value the guidance and tools offered by Cybersecurity and Infrastructure Security Agency (CISA) to help water systems remain cyber-secure.

[1] https://www.amwa.net/testimonycomments/amwa-testimony-house-subcommittee-hearing-cybersecurity

[2] https://industrialcyber.co/industrial-cyber-attacks/iranian-hacker-group-cyberav3ngers-allegedly-breach-municipal-water-authority-of-aliquippa/

As members of this subcommittee, along with their colleagues in Congress, explore ways to help water systems improve their cyber posture, AMWA believes it would be especially valuable to focus efforts on expanding participation in existing resources like WaterISAC, and leveraging sector-based expertise to expose water systems to appropriate cyber best practices.

Promote Participation in Existing Resources Like WaterISAC

The Water Information Sharing and Analysis Center, or WaterISAC, was established in 2002 with seed money from the federal government and subsequent congressional appropriations. One of two dozen ISACs operating across the nation's critical infrastructure sectors, WaterISAC annually issues hundreds of advisories, maintains a portal for water utility 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. AMWA has a management agreement through which it operates WaterISAC on behalf of the water sector.

WaterISAC's membership is comprised of water and wastewater utilities that serve about 60% of the U.S. population. The center is funded exclusively through member dues, and although these dues are structured on a sliding scale based on system size – with the smallest water and wastewater systems able to join for little more than $100 annually – WaterISAC faces challenges in connecting with the thousands of water and wastewater systems across the country. At present, only about 400 of the nation's nearly 50,000 community water systems and 16,000 wastewater systems are WaterISAC members that enjoy full access to the complete library of threat and vulnerability alerts, subject matter expertise, and other information. Lacking access to these essential resources could prove detrimental to a water system in a time of crisis.

In recent years Congress has recognized the value of expanding access to ISACs serving other critical infrastructure sectors. For example, the Infrastructure Investment and Jobs Act of 2021 authorized a new Energy Department program to expand bulk power systems' access to the ISAC serving the Electric Sector.[3] AMWA has endorsed legislation that would direct EPA to similarly support water systems' access to WaterISAC,[4] but we would be eager to explore if there could be a role for the Department of Homeland Security to help raise awareness of, and offer support for, participation of the ISACs serving water and other critical infrastructure sectors.

Leverage Sector-Based Expertise to Expose Water Systems to Appropriate Cyber Best Practices

Currently there is a wealth of information available to water systems aiming to improve their cyber defenses. For example, WaterISAC's free *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* is a menu 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* recommend straightforward but sometimes overlooked tasks like enforcing user

[3] P.L. 117-58, Section 40125(c)

[4] https://www.amwa.net/letter/letter-support-water-system-threat-preparedness-and-resilience-act

access controls and performing asset inventories. Other recommendations in the guide address vulnerability management and creating a cybersecurity culture.[5]

Another key resource available to the sector is CISA's vulnerability scanning tool, a free service that allows utilities and other industrial control system operators to scan their networks for known vulnerabilities, weak configurations, and suboptimal security practices.[6] The National Institute of Standards and Technology (NIST) offers a cybersecurity framework featuring an inventory of existing standards, guidelines, and practices for water systems and other network-connected organizations to manage and reduce cybersecurity risk.[7]

Last month EPA, CISA, the FBI and other federal partners collaborated with water sector stakeholders to release the *Incident Response Guide for the Water and Wastewater Systems (WWS) Sector.*[8] The document provides information about federal support available to water and wastewater systems throughout the incident response process and features a range of measures that drinking water and wastewater systems may choose to adopt to improve their cyber posture.

Through these and other resources, water system owners and operators have a range of opportunities to identify cybersecurity strategies that can strengthen the defenses of their information technology and operational control systems. Unfortunately, too many of the nation's 50,000 community water systems lack the appropriate personnel to make sense of these tools or the funding to put them into action.

In AMWA's testimony last month before the Environment, Manufacturing, and Critical Materials Subcommittee the association offered to work with Congress to explore ways to encourage all the nation's community water systems to adopt appropriate cybersecurity best practices through a tiered, risk-based program led by water sector experts, and overseen by EPA in its capacity as the Water

[5] 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

[6] https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning

[7] https://www.nist.gov/cyberframework

[8] https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide-0

and Wastewater Sector’s Sector Risk Management Agency. We also urged the panel to avoid prescriptive, one-size-fits-all federal mandates that may not lead to workable outcomes for many of the nation’s thousands of community water systems.

As these discussions continue, we would welcome the opportunity to work with you to explore how CISA may be able to support these efforts to connect water sector stakeholders with appropriate cyber resources.

Conclusion

Thank you for the opportunity to submit this statement for the record of today’s hearing, and we look forward to working with you to increase the cyber preparedness and resilience of the nation’s water systems.

Sincerely,

Tom Dobbins
Chief Executive Officer