Testimony of Scott Dewhirst
Superintendent
Tacoma Water

On Behalf of the
Association of Metropolitan Water Agencies

Subcommittee on Environment, Manufacturing, and Critical Minerals

U.S. House of Representatives

"Ensuring the Cybersecurity of America's Drinking Water Systems"

January 31, 2024

Chairman Carter, Ranking Member Tonko, and members of the Subcommittee: I appreciate the opportunity to appear on behalf of the Association of Metropolitan Water Agencies (AMWA) at today's hearing on "Ensuring the Cybersecurity of America's Drinking Water Systems."

I am Scott Dewhirst, and since 2017 I have served as the Superintendent of Tacoma Water. As a division of Tacoma Public Utilities (TPU) alongside Tacoma Power, Tacoma Water provides direct water service to more than 350,000 people throughout Pierce and King counties in Washington State.

I currently serve on the Board of Directors of AMWA, which represents the nation's largest publicly owned drinking water systems and whose members are committed to providing safe, reliable, and high-quality drinking water to more than 160 million Americans from coast to coast. I am also a member of the Board of Managers of WaterISAC, the Water Information Sharing and Analysis Center, which is the water sector's dedicated information sharing entity on cyber, physical, and natural threats.

Drinking water systems represent an attractive target for cyber adversaries, and a successful attack would not only threaten water quality and public health, but also undermine the confidence that Americans have in their drinking water nationwide. The recent breach of an industrial control system device at Pennsylvania's Municipal Water Authority of Aliquippa,[1]

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

along with breaches at several other water systems, are just the latest example of why utilities of all sizes must remain on guard against cyber intrusions.

As a large municipal utility provider, TPU prioritizes maintaining cybersecurity best practices to minimize vulnerabilities to our electric and water systems. We take part in periodic threat exercises, we have partnered with the Washington National Guard on a cybersecurity assessment of our industrial control systems, and we are implementing a key cybersecurity roadmap to stay at the forefront of cyber best practices. To manage this work, we employ a dedicated cybersecurity staff and leverage resources offered by federal and sector partners like the Environmental Protection Agency, the Cybersecurity and Infrastructure Security Agency (CISA), and the Information Sharing and Analysis Centers for the water and electric sectors.

Because Tacoma Power is subject to industry-developed cybersecurity standards for the electric sector, TPU has the unique ability to leverage necessary investments made in enterprise grade cyber tools to benefit both our power and water utilities. Our staff utilize several tools and practices to monitor our systems with a key focus on tracking all communications with external sources. The majority of the external communications occur due to the interconnectivity of the electrical sector participants and are more limited for water system operations due to the localized nature of the majority of water systems. We have standing and rehearsed incident response plans that can be activated should an intrusion be identified so that it can be contained, removed, and recovery (if any) be performed.

While this level of investment in cyber preparedness may be typical for a large, well-resourced public utility like TPU, we know that abilities and resources vary greatly across the nation's 50,000 community water systems. A 2021 *Cybersecurity State of the Sector* survey conducted by the Water Sector Coordinating Council found that while 55 percent of utility respondents identified cybersecurity as a high priority, only about 25 percent participate in cyber-focused tabletop exercises and about 40 percent conduct cyber risk assessments on at least an annual basis.[2] We have an opportunity to make progress across the sector.

AMWA commends the subcommittee for convening this hearing to collect viewpoints on the best path forward. First and foremost, the association believes it is essential that stakeholders and the federal government, primarily through EPA in its capacity as the Sector Risk Management Agency for the Water and Wastewater Systems Sector, maintain open lines of communication and pursue cooperative approaches to closing cyber gaps. AMWA was disappointed in EPA's March 2023 interpretive memorandum that would have folded cybersecurity reviews into periodic public water system sanitary surveys.[3] The association appreciated EPA's efforts to address cyber risks, but believed EPA's proposal was the wrong approach due to a variety of concerns. For example, this approach would have potentially allowed sensitive security information to be made public and entrusted state officials with little cybersecurity expertise to conduct these critically important assessments. AMWA supported EPA's decision last fall to withdraw the memorandum and the association remains committed to working with the agency, Congress, and other stakeholders on policy solutions that will truly enhance cybersecurity for all water systems across the country.

[2] https://www.waterisac.org/2021survey

[3] https://www.epa.gov/system/files/documents/2023-10/addressing-pws-cybersecurity-in-sanitary-surveys-memo_march-2023.pdf

As members of this subcommittee survey the current landscape and explore ways to help water systems improve their cyber posture, AMWA has three broad suggestions to help guide the conversation:

- Promote participation in existing sector-based resources like WaterISAC;
- Fund the EPA cyber resilience program authorized in the Infrastructure Investment and Jobs Act of 2021 and revisit expired technical assistance programs; and
- Leverage existing resources and incentivize the adoption of cyber best practices.

While AMWA remains eager to work with the subcommittee on additional strategies for improving the cybersecurity of the nation's water infrastructure, the association believes these core principles should guide any comprehensive cybersecurity policy for the water sector.

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,[4] WaterISAC annually issues hundreds of advisories, maintains a portal for water utility members, and hosts webinars and threat briefings. For example, since last year's cyberattack targeting the Aliquippa water system, WaterISAC has issued multiple reports, updates, and advisories referencing the incident and recommending specific actions for water systems to take to close similar vulnerabilities that their utilities may face.[5] Additionally, WaterISAC provides regular incident reports and conducts threat analyses that are made available 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 members include drinking water and wastewater utilities that serve about 60 percent of the U.S. population. The center is funded exclusively through member dues. 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. However, WaterISAC still has 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.

While WaterISAC is aggressively pursuing strategies to expand access to more water systems, particularly those serving rural areas, there is a role for EPA to play in building awareness of the service. To this end, last year Rep. Jan Schakowsky introduced the Water System Threat Preparedness and Resilience Act (H.R. 1367). The bill, along with its Senate companion, would authorize a targeted EPA program that would encourage eligible entities to participate in WaterISAC, and allow EPA to offset costs incurred by community water systems and treatment

[4] https://www.nationalisacs.org/member-isacs-3

[5] https://www.waterisac.org/resources?search_api_views_fulltext=Aliquippa+

works associated with maintaining or initiating WaterISAC memberships. The proposal would also direct EPA to cooperate with WaterISAC on incident data collection and analysis of threats to the water sector.

H.R. 1367 is based on language in the Infrastructure Investment and Jobs Act of 2021 that authorized a new Energy Department program to expand bulk power systems' access to the E-ISAC, WaterISAC's counterpart in the electricity sector.[6] AMWA urges the subcommittee to explore establishing a similar program as a component of any larger policy that supports water utilities' efforts to improve their cybersecurity standing.

Fund EPA cyber resilience program authorized in the Infrastructure Investment and Jobs Act of 2021 and revisit expired technical assistance programs

AMWA strongly supported a new EPA program established in the Infrastructure Investment and Jobs Act (IIJA) of 2021 that will help drinking water systems build resilience to cyber threats, and the association urges members of the subcommittee to call on appropriators to provide full funding for this important program going forward.

IIJA authorized $250 million over five years for the Midsize and Large Drinking Water System Resilience and Sustainability Program, which will offer grant assistance to public water systems that serve communities of 10,000 or more people to support projects to increase resilience to extreme weather threats or to reduce a water system's vulnerability to a cyber-attack. To date Congress has appropriated $5 million for the program, and EPA is expected to begin soliciting grant applications during the 2024 fiscal year. However, fully funding the program – or at least providing a level of appropriations closer to its annual $50 million authorization – would greatly expand the number of water systems that can tap these resources to improve their cyber defenses. With additional federal funding, a wider range of public water systems would be able to undertake security initiatives such as pursuing new software upgrades, making investments in security personnel, or implementing threat detection and monitoring procedures.

As part of America's Water Infrastructure Act of 2018, Congress established a Drinking Water Infrastructure Risk and Resilience Program through which EPA would offer grants to help community water systems implement measures to increase resilience to specific vulnerabilities identified in mandatory risk and resilience assessments. These measures could include improvements to electronic and computer systems and investments in training programs for personnel; a portion of funds were to be set aside to aid the smallest water systems. However, though Congress authorized $50 million for the program over two years, it was never funded and expired after the 2021 fiscal year. AMWA encourages the subcommittee to consider reauthorizing this program to offer another potential path for EPA to deliver needed cyber assistance to the nation's water systems.

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

Leverage existing resources and incentivize the adoption of appropriate cyber best practices

Tacoma Water takes advantage of 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 access controls and performing asset inventories. Other recommendations in the guide address vulnerability management and creating a cybersecurity culture.[7]

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.[8] And 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.[9]

New products continue to be developed as well. Earlier this 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.*[10] 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.

---

[7] 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

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

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

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

This is why AMWA believes that in addition to federal funding assistance and technical support for utilities that need it, there must be a level of rigor and accountability to encourage the adoption of tiered best practices appropriate for a given water system's size and risk profile.

One potential model for the water sector can be found in the electric sector, where the North American Electric Reliability Corporation (NERC) oversees a suite of ANSI-accredited Reliability Standards that aim to ensure that bulk power systems meet a baseline level of preparedness.[11] NERC's Reliability Standards are developed by electric sector leaders, with oversight from the Department of Energy, and the body has the ability to enforce compliance by individual systems. While there are many key differences between the bulk power and water sectors – such as the interconnected nature of electric systems offering greater opportunities for the spread of malicious code and cascading industrial control system failures – it is worth exploring whether this sector-led approach to the development of appropriate cyber best practices could be replicated in the water utility community.

As the subcommittee contemplates the best approach for the water sector, it is critical to include stakeholders at the table. Any path forward should reflect a tiered, risk-based approach, guided by water sector experts, and focused on clear objectives rather than prescriptive, one-size-fits-all mandates. Aspects of appropriate standards or guidelines in place for the electric and other critical infrastructure sectors should be considered as models for similarly situated water systems. AMWA would welcome the opportunity to participate in any discussions with the subcommittee to pursue these or other strategies to build water systems' resilience to cyber threats.

Conclusion

On behalf of AMWA, I thank the subcommittee for the invitation to testify today, and to share the on-the-ground insights of Tacoma Water. AMWA and its members across the country remain committed to taking all appropriate measures to strengthen our cyber defenses, and we look forward to continuing to collaborate with our federal partners to close the remaining gaps and secure needed funding and technical assistance.

Thank you again, and I am happy to answer your questions.

[11] https://www.nerc.com/pa/Stand/Pages/default.aspx