American Water Works Association

Dedicated to the World's Most Important Resource®

Government Affairs Office
1300 Eye Street NW
Suite 701W
Washington, DC 20005-3314
T 202.628.8303
F 202.628.2846

U.S. House Committee on Energy and Commerce
Subcommittee on Environment, Manufacturing, and Critical Materials
Hearing on Ensuring the Cybersecurity of America's Drinking Water Systems

Testimony

Kevin M. Morley, PhD
Manager, Federal Relations
American Water Works Association

January 31, 2024

Good afternoon, Chairman Carter, Ranking Member Tonko, and members of the Subcommittee. My name is Kevin Morley, and I am Federal Relations Manager for the American Water Works Association (AWWA), on whose behalf I am speaking today. Established in 1881, AWWA is the largest nonprofit, scientific and educational association dedicated to managing and treating water, the world's most vital resource. We represent water systems large and small, municipal and investor-owned, urban and rural. With approximately 50,000 members, AWWA provides solutions to improve public health, protect the environment, strengthen the economy and enhance our quality of life. In the modern era of water utility operations, that mission also includes managing cybersecurity risks that could threaten the essential lifeline function water professionals provide 24/7/365.

Enhanced Oversight and Accountability.

Drinking water and wastewater systems sustain our way of life and support public health, safety and economic vitality. These systems are robust and resilient but, like all critical infrastructure entities, are not immune to cyber threats.

Strong cybersecurity measures are essential to ensuring a cyber incident does not threaten public health. Water systems need resources and regulatory oversight designed to mitigate the potential risks from cyberattacks around the clock, every day of the year. This means we need to act now.

That is why AWWA has recommended congressional action to support a new cybersecurity governance framework in the water sector. This collaborative approach leverages the technical knowledge of utilities, cybersecurity experts and regulators to implement a comprehensive cybersecurity risk management strategy.

This collaborative approach builds on a similar model that has already been successfully applied in the electric sector. This model, authorized by federal legislation, would create an independent, non-federal entity to lead the development of cybersecurity requirements using in part subject matter experts from the water sector. Federal oversight and approval of requirements would be provided by the U.S. Environmental Protection Agency, which already regulates drinking water and wastewater utility operations.

This governance model follows a proven tiered, risk- and performance-based approach that accommodates the differences in operational complexity and maturity in the sector. This recommendation aligns with calls for public-private collaboration included in the National Cyber Strategy. It recognizes that cybersecurity is a shared responsibility that benefits from direct engagement and operational knowledge of owner/operators and the accountability that comes with federal oversight.

The diverse nature of water utilities requires a tiered framework that recognizes the technical challenges facing the sector and sets reasonable cybersecurity requirements that focus on practical, protective, and implementable solutions.

Strong oversight of cybersecurity in the water sector remains critical. There have been and will continue to be serious attempts to attack water systems. AWWA, CISA, EPA and others have developed resources to help utilities assess vulnerabilities and implement cybersecurity best practices.

We believe it is timely and prudent for Congress to authorize this proposed collaborative model to ensure utilities are directly engaged in developing appropriate cybersecurity requirements -- with oversight from EPA – to create a robust cybersecurity risk management paradigm in the water sector.

In addition to establishing a sound oversight model, it is critical to recognize the challenges and opportunities for enhancing cybersecurity in the water sector. Functionally, we see the following areas of collaboration as being the most essential:

- Overcoming the Digital Divide
- Threat Information Sharing
- Vulnerability Mitigation and Technical Assistance

Overcoming the Digital Divide

Water utility owners and operators are stewards of public health and the environment. This is a calling that the profession takes seriously. However, that dedication cannot overcome the fiscal realities that often constrain utility operations. Water systems of all types and sizes require a combination of physical assets and people to fulfill their mission. We are at an inflection point where the operational efficiencies and cost savings enabled by increasing automation are resulting in a smaller workforce. One effect of the move to automation is a growing footprint of digital dependency that presents a critical cybersecurity risk. One key dimension is the community of water utilities are stuck in a digital canyon, meaning the operational technology that runs the pumps and motors has been unable to keep pace with advances in the enterprise systems that upgrade to new editions at a much faster pace.

The “fix” for this digital division is complex since it requires more than simply upgrading older enterprise platforms to the latest edition. The operational technology in many cases will not work on newer enterprise platforms and therefore requires total overhaul, rip and replace, of various OT elements to upgrade. This often requires a lengthy and costly capital project since utility services must continue working 24/7 until the transition is complete. As an example, a larger water system that recently embarked on this type of capital project indicated that it would take five years and is estimated to cost $80 million. Smaller systems in our sector have significantly constrained budgets and must take into consideration new obligations to comply with multiple regulations, including the revised lead and copper rule and pending PFAS standards. These new regulatory obligations are not included in the $1.2 trillion AWWA estimated needed over 20 years for the repair and replacement of distribution and transmission lines across all drinking water systems.

Unlike other critical infrastructure sectors, to date, there has been no dedicated funding to expedite technology upgrades at water systems. Cybersecurity is one of many eligible activities within the State Revolving Fund (SRF) program, but constraints on that program may not allow utilities to acquire the optimal cybersecurity support they need. If the water sector is truly a national security priority, then we will need support to expedite these technology upgrades, address this digital chasm in a manner that is not punitive, and fulfill our shared commitment to the communities we serve. Congress has allocated resources to the State and Local Cybersecurity Grant Program (SLCGP) which could potentially address challenges facing water utilities, but it appears too early to assess how the funds are being allocated at the local level. We also encourage full appropriations for the grant programs authorized in America’s Water Infrastructure Act (AWIA) of 2018 to support water utility resilience with an emphasis on cybersecurity projects,

Threat Information Sharing

We recognize the complexity and sensitivity of the intelligence efforts developed by our federal partners. When packaged correctly, that information can provide meaningful opportunities to mitigate the potential consequences of harmful threats that exploit vulnerabilities in an expanding digital footprint across all sectors.

To enhance the effectiveness of information sharing, we recommend that CISA and EPA, as the Sector Risk Management Agency (SRMA), work with partners like the WaterISAC and the Water Sector Coordinating Council to properly contextualize threat information prior to its release. In many cases, advisories and alerts are quite technical, and often assume a certain level cybersecurity expertise in order to take action on the information provided. While there is often tension in getting information moved below a certain classification level, the reality is most entities simply want to know what the vulnerability is and how it can be mitigated. The variables that drive classification such as attribution and tactics, techniques, and procedures (TTPs) are rarely of direct interest to the end user of the technology or system that may have been compromised.

Establishing a standard operating procedure for the inclusion of subject matter experts from the affected community into the review and development of threat alerts and advisories will help to ensure that the information transmitted to the sector is concise, actionable, and properly contextualized.

Vulnerability Mitigation and Technical Assistance

AWWA has developed multiple resources to facilitate the assessment of cybersecurity vulnerabilities and inform the implementation of best practices. This effort is centered on the controls provided in the NIST Cybersecurity Framework (CSF) which also serves as the source of the Cybersecurity Performance Goals (CPGs) developed by CISA. AWWA's sector-specific cybersecurity guidance and assessment tool[1] provides any water utility with a tailored application of the NIST CSF that is based on their application of certain technologies. Using the tool allows utility assessment of cybersecurity controls and practices to be right-sized to that utility's operations. In this manner, the tool emphasizes actions that address the highest priority controls expected to quickly provide the greatest risk reduction value. Collaboration with our federal partners provided a strong foundation for creating a consistent and repeatable course of action to reduce vulnerabilities to cyberattacks as recommended in Executive Order 13636 and several ANSI/AWWA standards.[2,3,4] The guidance and assessment tool were first released in 2014 and regularly updated to help water systems create a sound cyber risk management program. This includes addressing the cybersecurity provisions in section 2013 of AWIA (PL 115-270). In AWIA, Congress placed greater emphasis on assessing and taking action to mitigate cybersecurity threats that could impact drinking water utility operations and/or business enterprise systems.

AWWA's resources are designed to assist water systems in assessing potential vulnerabilities with various technology applications. We encourage our federal partners to recognize the value of these resources in supporting this shared mission, which requires a combination of government and non-governmental resources. Our efforts are made stronger through collaboration, including in the following instances:

- AWWA worked with CISA and the Idaho National Lab to integrate output from AWWA's Assessment Tool into the Cyber Security Evaluation Tool (CSET®). This new functionality allows a water system that has used AWWA's tool to seamlessly transition their information into CSET®, a resource that provides advanced features and analysis of system architecture and controls.

[1] American Water Works Association, Water Sector Cybersecurity Risk Management Guidance and Assessment Tool, https://www.awwa.org/cybersecurity

[2] ANSI/AWWA G430: Security Practices for Operations and Management

[3] ANSI/AWWA J100: Risk and Resilience Management of Water and Wastewater Systems

[4] ANSI/AWWA G440: Emergency Preparedness Practices

- CISA worked with the Water Sector Coordinating Council to develop an outreach campaign to increase deployment of the Vulnerability Scanning service to water systems, especially smaller and medium-sized utilities.

- The Indiana Finance Authority partnered with the Indiana Section of AWWA to train over 150 utilities to use AWWA's cybersecurity guidance and assessment tool, through a combination of in-person and virtual sessions.

- AWWA and the Rural Community Assistance Partnership (RCAP) provided guidance and training on AWIA compliance, including directed outreach and training on cybersecurity, supported by an EPA small systems capacity development grant.

- AWWA partnered with the United States Department of Agriculture to facilitate training, produce eLearning resources, and provide a guidance document for small utilities, *Water Sector Cybersecurity Risk Management Guidance for Small Systems*.[5] This "getting started guide" helps small, rural utilities assess and implement cybersecurity best practices.

These types of capacity development efforts are essential when considering there are more than 45,000 community water systems that serve fewer than 3,300 people. AWWA encourages continued support for this type of engagement, which has proven time and again to be the most effective for advancing the implementation of new practices. This is also why we support the initiative recommended by the National Rural Water Association to deploy cybersecurity specialists to help rural water systems that often lack the resources and in-house expertise to implement cybersecurity best practices.

Finally, research to identify and detect vulnerabilities in technology commonly deployed in the water sector is essential. This includes providing mitigation solutions to the utility community and building partnerships with the service providers. The Water Security Test Bed (WSTB), developed by Idaho National Laboratory (INL) and the EPA Office of Research and

[5] AWWA, Water Sector Cybersecurity Risk Management Guidance for Small Systems

Development’s (ORD), can help support research into water sector-specific vulnerabilities and coordinate information sharing. The WSTB is a large-scale, adaptable testing environment that can be disrupted or destructively tested by government and industry partners. Funding for this program would provide an objective platform to evaluate cyber intrusion scenarios, demonstrate physical impacts, deliver scalable mitigations useful for water utilities of various sizes and budgets, and provide realistic utility operator training.

#################

Kevin M. Morley, PhD

Kevin M. Morley, PhD is Manager, Federal Relations for the American Water Works Association (AWWA). Over the past 20 years he has worked closely with multiple organizations to advance security and preparedness in the water sector. This includes establishing the Water/Wastewater Agency Response Network (WARN) and guiding the development of several ANSI/AWWA standards that represent minimum best practices for water sector risk and resilience management, including cybersecurity. He is a leading expert on §2013 of America’s Water Infrastructure Act (AWIA) of 2018 and multiple resources that enable water systems to implement an all-hazards approach to security and preparedness. Dr. Morley has supported the national discourse on risk and resilience as a Disaster Resilience Fellow for the National Institute of Standards and Technology, a member of the President’s National Infrastructure Advisory Council and the Water Sector Coordinating Council. Dr. Morley received a PhD from George Mason University for research developing the Utility Resilience Index (URI). He holds a MS from the State University of New York College of Environmental Science and Forestry and a BA from Syracuse University.

################

What is the American Water Works Association?

The American Water Works Association (AWWA) is an international, nonprofit, scientific and educational society dedicated to providing total water solutions to protect public health and assure the effective management of water. Founded in 1881, the association is the largest organization of water professionals in the world.

Our membership includes more than 4,500 utilities that supply roughly 80 percent of the nation's drinking water and treat almost half of the nation's wastewater. Our 50,000 members represent the full spectrum of the water community: public water and wastewater systems, environmental advocates, scientists, academicians, and others who hold a genuine interest in water, our most important resource.

AWWA is accredited by ANSI (American National Standards Institute) as a standards development organization and publishes over 170 Standards that provide valuable information on design, installation, disinfection, performance, and manufacturing of products including pipe, chemicals, storage tanks, valves, meters and other appurtenances; industry-recognized consensus prerequisites; and best practices for water utility management and operations. AWWA unites the diverse water community to advance public health, safety, the economy, and the environment.

###