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 Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

Hearing on Securing Operational Technology: A Deep Dive into the Water Sector

Testimony

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

February 6, 2024

Good morning, Chairman Garbarino, Ranking Member Swalwell, and members of the Subcommittee. My name is Kevin Morley, and I am the 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.

Drinking water and wastewater utility operations have been evolving and adapting to new technologies since the turn of the last century. A paper presented during AWWA's 1965 Annual Conference includes a statement that is just as relevant today as it was then:

> *The complex expansion of water systems has resulted in substantial adoption of instrumentation by the water industry. Modern instrument systems have made possible the surveillance and remote control of wells, treatment facilities, pumping stations, storage tanks, and transmission main valving, while rising labor costs have prompted water utility management to follow other industries in establishing some degree of automation and centralized control.*[1]

The difference today as it relates to cybersecurity is the convergence of technology systems that had traditionally operated independently. Information technology (IT) are the business enterprise systems like laptops and software systems used to manage email, payroll, customer billing, and service contracts. The operational technology (OT) are the systems used to manage and control various physical operations for the treatment and distribution of drinking water or the collection and treatment of wastewater. The integration of IT and OT systems has improved operational efficiency to optimize various unit processes and allowed greater visibility into those systems.

The challenge is that many current IT systems were designed to be connected to the internet, while OT systems were not but have since been plugged in. This integration began before the prospect of cybersecurity threats targeting today's critical infrastructure systems were envisioned. The cost savings realized were long ago absorbed into capital projects and

[1] Crow, W.B. & Eidsness, F.A (1965) Savings Through Instrumentation and Control In Two Water Systems. *Journal AWWA*, 57:12:1509.

reconfigurations of the workforce. Those OT systems were capital intensive and often had an expected service life of 20-25 years. This is very different than IT systems which have cycled through new versions at a pace that has outpaced the support for OT systems. As a result, older legacy OT systems are dependent on IT systems that are no longer supported and are unable to communicate with the new versions.

The “fix” for this digital divide is complex since utility services must continue working 24/7 until the transition is complete. While implementation of certain controls can help to manage cyber risk, ultimately IT upgrades may require total overhaul, rip and replace, of various OT elements. These capital projects are often lengthy and cost intensive. As an example, a large water system recently embarked on a 5-year, $80 million capital project to complete these upgrades. The financial cost associated with this type of transformation is amplified by the reality that 90% of water systems serve less than 3,300 people and have severely constrained budgets.

Drinking water utilities are already facing significant costs to comply with multiple regulations, including the revised lead and copper rule and pending PFAS standards. The treatment processes necessary to comply with these rules will require greater automation and digital dependency. The compliance costs for new regulatory obligations come on top of the $1.2 trillion that AWWA estimates is needed over 20 years for the repair and replacement of aging distribution and transmission lines nationally.[2] Escalating supply chain costs on essential treatment chemicals, piping materials and equipment have also imposed considerable pressure on operating budgets, which are not expected to moderate in the near term.[3]

Unlike other critical infrastructure sectors, to date, there has been no dedicated funding appropriated to expedite technology upgrades at water systems with legacy OT systems. While cybersecurity is one of many eligible activities within the State Revolving Fund (SRF) program,

[2] AWWA (2012) Buried No Longer: Confronting America’s Water Infrastructure Challenge.

[3] Morley, KM. (2023) Supply Chain Threats Persist. *Journal AWWA* 115(2):6. https://doi.org/10.1002/awwa.2048

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 it will need support to expedite technology transformations to address the digital divide in a manner that is not punitive and fulfills our shared commitment to the communities we serve.

Prioritizing Cybersecurity in the Water Sector

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. In recognition of this threat, AWWA has actively engaged our members, and the sector at large, in building cybersecurity awareness and providing resources to support the implementation of best practices. As evidence of growth in awareness, utility leaders have consistently rated cybersecurity as a very high priority in AWWA's annual State of the Water Industry report for several years. This trend runs parallel to AWWA's collaboration with water utility subject matter experts and federal partners to provide a water sector-specific approach for implementing the NIST Cybersecurity Framework (CSF), as called for in Executive Order 13636.

AWWA's Water Sector Cybersecurity Risk Management Guidance and Assessment Tool, first issued in 2014, helps a utility examine which cybersecurity controls and practices are most applicable based on the technology applications they have implemented. The resource emphasizes actions that address the highest priority controls expected to quickly provide the greatest risk reduction value. AWWA also partnered with the United States Department of Agriculture to develop the Water Sector Cybersecurity Risk Management Guidance for Small Systems, a "getting started guide" that helps small, rural utilities serving fewer than 10,000 people assess and implement cybersecurity best practices.

Strong cybersecurity measures are essential to ensuring a cyber incident does not threaten public health. Several cyber incidents led AWWA in 2021 to assess a variety of potential options, which resulted in our recommendation to establish a new cybersecurity governance framework in the water sector. Our recommended approach would create an independent, non-federal entity to lead the development of minimum cybersecurity requirements, leveraging subject matter experts from the water sector. Federal oversight and approval of requirements would be provided by the EPA. This framework builds on a similar model that has been applied in the electric sector with congressional approval.

This governance model would follow a 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 the direct engagement and operational knowledge of owner/operators and the accountability that comes with federal oversight.

We believe it is timely and prudent for Congress to authorize this 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 other collaborative opportunities to support cybersecurity in the water sector.

Consistent Public-Private Collaboration

CISA's maturity has evolved significantly since its formation, including predecessor functions. Most notable is the permanent addition of a water sector liaison in the Stakeholder Engagement Division. This has provided continuity in communications and generated productive engagement with the Water Sector Coordinating Council (SCC) and EPA as the Sector Risk Management Agency (SRMA). The most recent output was a stakeholder engagement process facilitated by the Joint Cyber Defense Collaborative (JCDC) which published "Incident Response Guide: Water and Wastewater Systems (WWS) Sector." This effort integrated the insights and recommendations provided by the stakeholder community to ensure that the guidance is best suited address their needs.

Another useful outcome was a collaborative effort to raise the visibility and awareness of CISA's Vulnerability Scanning service, as recommended in prior testimony. Before the fact sheet developed with the WSCC and Association of State Drinking Water Administrators, the value and purpose of this tool was not accessible to the entities that would derive the greatest benefit if enrolled. The fact sheet requires an organized outreach campaign that can provide a unified message on the resources provided by CISA and their relationship with other resources.

In the earlier years of CISA's predecessor, the SCCs would come together with agency staff for strategic planning, a requirements assessment of sorts, to identify the needs of the various critical infrastructure sectors. While not all sector needs became action items for agency workplans, it was a useful exercise to examine unique conditions and identify cross-sector needs. The WSCC, working with state and federal partners, has developed a strategic roadmap that defines top-level priorities for managing risk and building resilience. When federal partners initiate projects to act on those priorities, it is in our collective interest that collaboration occurs early and often to ensure the approach is aligned with the needs of the stakeholders for whom it is presumably designed to support. Miscues lead to missed opportunities, duplication of effort and products that do not fulfill the needs of owner/operators.

As we did following 9/11, collaboration with trusted partners like AWWA is a high value force multiplying capability that should be maximized to address the national security risk cyber threats impose on drinking water and wastewater systems. Other action items to be considered further include the following:

1. **Unified Messaging**. Launch a collaborative campaign to expedite enrollment in CISA's vulnerability scanning service to help utilities address threat exposure. This is a highly valuable service for systems with limited in-house resources to provide timely information on exposures and recommended mitigations.

Work with stakeholders in the water sector to review the myriad resources and prepare a matrix that communicates, in plain English, the function they provide and associated relationship. Currently, the array of “stuff” is overwhelming and as a result undersubscribed or inaccessible to those with the greatest need, absent some order or clearly defined progression of applicability.

2. **Inform and Enable.** Invest in capacity development to empower utility owner/operators to effectively engage cybersecurity issues that are aligned with their needs. We believe AWWA’s small system guidance provides a robust “getting started” guide focused on six key domains from the NIST CSF.

   Training on the application of this guidance delivered by trusted partners like AWWA is a highly effective and proven force multiplier for building awareness and enabling utilities to assess potential vulnerabilities and implement control to mitigate risks. There is a significant opportunity to collaborate to support the cybersecurity needs for 50,000 community drinking water systems and nearly 16,000 wastewater systems.

3. **Technology Transformation**. Funding that prioritizes and expedites technology upgrades to address legacy operational technologies will be necessary to overcome the growing digital divide. These legacy OT systems simply cannot operate on newer enterprise platforms and, in many instances, this requires a rip and replace project that is capital and time intensive.

4. **Improve threat information sharing**. We recommend that CISA and EPA work with partners like the WaterISAC and the Water Sector Coordinating Council to establish a standard operating procedure for the inclusion of SMEs in the development of threat alerts and advisories to ensure that the information transmitted is concise, actionable, and properly contextualized.

   In addition, it is critical to recognize and address the unconscious competence associated with many cybersecurity advisories. Simply state the problem and the recommended mitigation. We would recommend putting the TTPs and MITRE Attack explanation in an appendix, as they are interesting but often a distraction from the action being recommended to mitigate the threat.

5. **Research and Development.** The Water Security Test Bed (WSTB), developed by Idaho National Laboratory (INL) and the EPA Office of Research and 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.

###