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

Mobilizing Our Cyber Defenses:
Securing Critical Infrastructure Against Russian Cyber Threats

Testimony

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

Before the House Committee on Homeland Security

March 30, 2022

Good morning, Chairman Thompson, Ranking Member Katko, and members of the committee. My name is Kevin Morley, and I am the Federal Relations Manager for the American Water Works Association, or AWWA, on whose behalf I am speaking today. I appreciate this opportunity to offer AWWA's perspectives on how cybersecurity threats are being addressed in the water sector (drinking water and wastewater systems). AWWA's 50,000 members span the full spectrum of the water profession. Our utility members represent water systems large and small, municipal and investor-owned, urban and rural. We work to protect public health and the environment, support the economy, and enhance our quality of life. In the modern era of water utility operations, our mission also includes managing cybersecurity risks that threaten the essential lifeline function water professionals provide 24/7/365.

AWWA strongly values collaboration and information sharing with our federal partners to address the dynamic nature of the cyber threats facing our critical infrastructure systems. Recent federal recommendations on how to mitigate Russian cyber threats have been invaluable. The water sector has actively participated in multiple briefings provided by the Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Environmental Protection Agency (EPA) that illuminate the evolving threat environment and help professional organizations, such as AWWA, build awareness among members. Working with sector partners, EPA reached out to 58,000 water systems collectively serving about 300 million Americans regarding cyber threat concerns at the end of December 2021. This led to several sector level briefings hosted by EPA to share information on Russian cyber threat activity. The associated advisories have been shared across multiple communication platforms to ensure the widest possible distribution to water utility owners and operators.

The current situation illustrates both the necessity and strength of continuous two-way engagement to jointly manage the cyber threats facing critical infrastructure systems, including drinking water and wastewater systems. Functionally, we see the following areas of collaboration as most essential:

- Actionable Threat Intelligence
- Vulnerability Mitigation and Technical Assistance
- Partnership and a Path Forward

Actionable Threat Intelligence

We recognize the complexity and sensitivity of the intelligence efforts developed by our federal partners. CISA, and its predecessors, have generated copious amounts of information, alerts, and advisories on a multitude of cyber vulnerabilities that have enabled many entities to address otherwise unknown security gaps. The new Shields Up campaign deployed by CISA has been very well received and represents a welcome reorganization of the information disseminated to assist and guide critical infrastructure sectors. There are multiple federal partners that assess threats and develop valuable mitigation recommendations that are valuable but often difficult for a single water system to track and monitor absent a centralized hub for dissemination. Shields Up has provided a unified platform to share this information in a format that allows sector organizations, such as AWWA, to effectively amplify the recommendations developed by CISA and our federal partners for cybersecurity risk management.

To enhance the effectiveness of the information being shared, we recommend that CISA work with Sector Risk Management Agencies (SRMA) – EPA in the water sector's case - and partners like AWWA, WaterISAC and the Water Sector Coordinating Council to properly contextualize threat information. In many cases, advisories and alerts are quite technical, and they may be difficult to implement by entities without in-house cyber security experts. It should be recognized that many systems are divisions of municipal government and certain systems are not directly managed by the water utility. Integrating sector subject matter experts into the review and development of threat alerts and advisories will help ensure that the information transmitted to the sector is concise, actionable, and properly contextualized.

Expedient declassification of threat intelligence is essential to ensure that system owners and operators can effectively deploy mitigations. 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 often 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.

Vulnerability Mitigation and Technical Assistance

AWWA, in alignment with our mission, has been directly engaged in developing resources to facilitate the assessment of cybersecurity vulnerabilities. This effort is centered on the controls provided in the NIST Cybersecurity Framework. AWWA's sector-specific guidance and assessment tool[1] provides a water utility with a tailored application of the NIST CSF that is based on its application of certain technologies. Using the tool allows utility assessment of cybersecurity controls and practices to be right-sized in a manner that emphasizes actions that address the highest priority controls expected to quickly provide the greatest risk reduction value. Coordination with NIST, EPA and CISA was essential in developing this resource. 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], two of which hold SAFETY Act designations from CISA. The guidance and assessment tool were first released in 2014 and are regularly updated to help community water systems comply with the cybersecurity provisions included in section 2013 of America's Water Infrastructure Act (AWIA) of 2018 (PL 115-270). In AWIA, Congress placed an emphasis on assessing and taking action to mitigate cybersecurity threats that could impact drinking water utility operations and/or business enterprise systems.

Cybersecurity vulnerabilities are a critical concern in the entire water sector. AWWA's resources are designed to assist all water systems in assessing potential vulnerabilities with various technology applications. Once a vulnerability is identified, many of the CISA resources can help mitigate risks. One valuable resource is the Cyber Hygiene Service that assesses the "health" of an entity's publicly accessible web applications by checking for known vulnerabilities and weak configurations. This service is likely to provide the most immediate risk reduction benefit to users based on the actionable mitigation recommendations included in the reports provided to subscribers by CISA. We recommend that EPA, CISA and sector organizations coordinate a unified outreach campaign to increase deployment of this resource among water systems, especially smaller and medium-sized utilities.

[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 (SAFETY Act Designated)

[3] ANSI/AWWA J100: Risk and Resilience Management of Water and Wastewater Systems (SAFETY ACT Designated)

[4] ANSI/AWWA G440: Emergency Preparedness Practices

As water system cyber capabilities mature, other CISA-based resources provide support for long-term, sustainable cyber risk management strategies. The Cyber Security Evaluation Tool (CSET®) provides more advanced capabilities to users. AWWA worked with CISA and Idaho National Lab to integrate AWWA's Assessment Tool output with 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. This is an excellent demonstration of partnership between the sector and federal government to advance our shared objective of improving the cybersecurity capabilities of water utilities.

The diversity in the water sector is unique among U.S. utility sectors in both the size and complexity of water systems that provide drinking water and wastewater services across the country as either a public agency or a privately owned utility. Consequently, education and training are an ongoing activity and need within the sector. A partnership with the United States Department of Agriculture facilitated the development of materials and important training on cybersecurity for small systems. Through an EPA small systems capacity development grant, AWWA and the Rural Community Assistance Partnership (RCAP) also were able to provide guidance and training on AWIA compliance, including directed outreach and training on cybersecurity. The training drew on a scaled-down version of the AWWA guidance, targeted to the needs of small systems. AWWA produced facilitated training, eLearning resources, and a guidance document for small utilities titled Water Sector Cybersecurity Risk Management Guidance for Small Systems.[5] This "getting started guide" is intended to help small, rural utilities improve their cybersecurity practices. The intended users serve populations of fewer than 10,000 people, and particularly, utilities that serve fewer than 3,300 people. This resource was prepared to reflect the reality that many of the controls in the NIST CSF do not apply to the environment of many small utilities.

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

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, given that cybersecurity is a threat to critical infrastructure systems of all sizes and types.

The water sector is actively engaged with CISA and EPA through the Water Sector Coordinating Council on the Industrial Control Systems (ICS) Cybersecurity Initiative. This 100-day action plan will review the scalability of ICS monitoring technology deployment, such as CISA's CyberSentry, including the development of criteria for the adoption of such technology by water systems. In addition, the action plan will seek to establish the necessary information sharing protocols with federal partners leveraging the actions already taken by the electric and gas sectors. The direct involvement of subject matter experts from the water sector is essential for ensuring that this type of action properly accounts for the operational needs and constraints of a water utility.

Partnership and a Path Forward

Under Presidential Policy Directive 21, each sector has an established Sector Coordinating Council (SCC). The intent of this framework is partnership between CISA and SRMAs on critical homeland security matters facing the nation. While SCCs have provided invaluable support in fulfilling the mission of CISA and SMRAs, there is always opportunity for improvement and continued growth. Given the scale of the water sector, the function of the Water SCC and WaterISAC can be more consistently leveraged to provide real-time assessment and calibration of critical information-sharing products that may be developed by federal partners. Federal water sector-specific resources should not be developed and released independent of review and coordination by relevant subject matter experts, such as the members that constitute the Water SCC and supporting associations. Our shared mission to facilitate the secure operations of critical infrastructure is stronger when we work collaboratively and leverage the assets and resources each can bring to bear on the challenges imposed by cyber threats. Consistent messaging and clarity on how our respective resources and guidance documents complement each other is in the best interest of the public we serve together.

AWWA recognizes the cybersecurity challenge and is committed to establishing a new paradigm for cybersecurity governance in the water sector. We believe a new approach[6] is necessary, one that recognizes the technical and financial challenges facing the sector and sets minimum cybersecurity standards for all types of water systems. A tiered risk- and performance-based requirements model similar to the approach used in the electric sector under the auspices of North American Electric Reliability Corporation (NERC) would underpin this approach in the water sector. An entity similar to NERC would be created in the water sector to lead the development of the requirements using subject matter experts from the field. It would also perform periodic third-party conformity assessments. Federal oversight and approval of requirements would be provided by the EPA, given existing statutory authority for water and wastewater utility operations. A recent report by Foundation for the Defense of Democracies (FDD)[7] recognized the merits of such an oversight body in providing ongoing industry-led cyber threat mitigation efforts. AWWA welcomes the opportunity to work with our federal partners to implement a strategy that provides sustainable cybersecurity protection that recognizes the variability in the maturity and complexity of water systems.

[6] Paul Stockton, *Strengthening the Cybersecurity of America's Water Systems: Industry-Led Regulatory Options* (Washington, DC: American Water Works Association, August 2021),

[7] Foundation for the Defense of Democracies*, Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure*

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

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 practice for water sector risk and resilience management, including cybersecurity guidance. 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 is a member of the President's National Infrastructure Advisory Council and a past Disaster Resilience Fellow for the National Institute of Standards and Technology. Dr. Morley received a PhD from George Mason University for research on water sector resilience and created 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.

###