ASSOCIATION OF
METROPOLITAN
WATER AGENCIES

Testimony of

Scott Dewhirst
Deputy General Manager
Engineering and Technology
Fairfax Water

On behalf of the Association of Metropolitan Water Agencies

U.S. Senate
Committee on Environment and Public Works

Hearing on

"Identifying and Addressing Cybersecurity Challenges to Protect America's Water Infrastructure"

February 4, 2026

Chairman Capito, Ranking Member Whitehouse, and Members of the Committee, thank you for the opportunity to testify before you today. My name is Scott Dewhirst and I am the Deputy General Manager of Engineering and Technology at Fairfax Water. 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.

I am here today on behalf of the Association of Metropolitan Water Agencies (AMWA), of which Fairfax Water is a member. AMWA is an organization that represents the nation's largest publicly owned drinking water systems. AMWA members collectively provide over 160 million people across the country with clean drinking water. Members of AMWA are the general managers and CEOs of these large water systems. AMWA represents the perspectives and priorities of its members by working with Congress and federal agencies to ensure drinking water systems have input into the federal laws and regulations that affect them and their customers.

I'm here today to discuss cybersecurity in the water sector, a topic that is becoming more urgent by the day. Drinking water systems represent an attractive target for cyber adversaries. A successful attack could not only threaten water quality and public health but would also undermine public confidence in the safety and reliability of drinking water. Cyber attacks also have the potential to harm the economy if water systems are taken offline. Estimates show that a single day of downtime in U.S. water service could result in $122 billion in lost economic activity and a $69 billion decline in GDP. [1]

Background

It is important to distinguish between two categories of cyber attacks that could target water systems. The first targets utilities' information technology, or business and enterprise systems, such as email platforms, websites, and billing databases. In recent years, water systems have reported a variety of such attacks, which include ransomware incidents, email scams, and social engineering and phishing attempts. While such attacks, if successful, can disrupt day-to-day business and compromise sensitive data, they do not by themselves affect the treatment or distribution of drinking water or wastewater. A second and more serious category of cyber attack targets a utility's industrial control systems. These systems, which are managed online by most utilities, control treatment processes, sensors, valves, pumps, and other utility infrastructure. If these systems were to be compromised in a cyber attack, a worst-case scenario could lead to negative effects on water quality and public health.

[1] https://static1.squarespace.com/static/67dd711d1a117219a03e4f7a/t/6917b2fbc2843b7310c7ace1/1763160827739/FINAL+VOW+Economic+Report.pdf

The Cyber Threat Landscape

Cyber threats to water systems have grown in recent years. According to WaterISAC, from April 2024 through March 2025, roughly 14 percent of water utilities responding to its quarterly incident survey reported experiencing at least one cybersecurity incident. This is an increase from about 11.5 percent of responding water systems during the same period the year before.[2] At the same time, cyber threats are becoming more frequent, more sophisticated, and more damaging, requiring ongoing and sustained investment by water utilities to manage risk.

As more water systems use internet-connected operational technology—such as industrial control systems—to remotely monitor and control pumps, valves, and chemical dosing, new cybersecurity challenges are introduced. While these technologies improve efficiency, they also turn operations that were once handled directly by humans into complex, interconnected cyber-physical systems. That shift introduces new vulnerabilities if systems are not properly secured, as is the case too often. In 2024, researchers identified more than 18,000 industrial control systems in the United States that were accessible from the internet. More than half of the devices linked to water and wastewater systems could be manipulated online without any authentication at all.[3]

Pro-Russia hacktivist groups have taken advantage of this widespread lack of basic security, targeting water and other critical infrastructure systems using simple, widely available tools. For example, in January 2024, an attack by a Russian hacktivist group claimed responsibility for manipulating human-machine interfaces, resulting in water storage tank overflow and minor, temporary disruption of operations in a small Texas town.[4] Just last month, a hacktivist group known as Infrastructure Destruction Squad claimed in a Telegram post that it had gained unauthorized access and compromised a Texas water treatment system.[5]

Nation-state threats also pose a serious risk. In recent years, a Chinese-affiliated cyber group known as Volt Typhoon has been linked to long-term, stealthy intrusions into U.S. critical infrastructure networks. In one case, a combined electric and water utility discovered that the group had maintained access to its systems for approximately ten months before being detected.[6] These types of intrusions are especially concerning because they may be intended to enable future disruptive or destructive attacks.

Utilities also face growing operational risks as disruptions in information technology systems increasingly cascade into operational technology environments, as demonstrated by the July 2024 CrowdStrike outage. Compounding these challenges, AI is reshaping the threat landscape

[2] https://www.waterisac.org/threat-analysis-for-the-water-and-wastewater-sector-october-2025
[3] https://censys.com/blog/research-report-internet-connected-industrial-control-systems-part-one
[4] https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/
[5] https://www.waterisac.org/tlpgreen-russian-aligned-hacktivist-group-claims-texas-water-treatment-system
[6] https://www.waterisac.org/tlpclear-dragos-case-study-volt-typhoons-breach-massachusetts-electric-and-water-utility

and increasing risk by enabling ransomware actors to enhance extortion tactics, making social engineering attacks more convincing and harder to detect, and enabling new modes of attack.

These incidents demonstrate why water utilities of all sizes must remain vigilant against cyber intrusions. Without continued federal investment and support, many water systems will struggle to keep pace with these evolving threats, putting essential public health and safety services at risk.

Tools Available for Cyber Preparedness

As a large public water system, Fairfax Water employs a dedicated cybersecurity staff and leverages resources offered by federal and sector partners, including the Environmental Protection Agency (EPA), the Cybersecurity and Infrastructure Security Agency (CISA), and WaterISAC.

Effective cyber defense depends not only on understanding best practices, but also on continuous and timely awareness of evolving threats. Founded in 2002 as an independent non-profit organization, WaterISAC plays a unique role in the sector's cybersecurity preparedness by actively monitoring cyber threats and vulnerabilities affecting water and wastewater utilities. As one of more than two dozen Information Sharing and Analysis Centers across the nation's critical infrastructure sectors, WaterISAC continuously collects, analyzes, and disseminates threat intelligence specific to the water sector, while also offering guidance on risk mitigation tools, best practices, and response actions that contribute to an all-hazards resiliency posture. The organization issues hundreds of cyber and physical security advisories each year, receives incident reports from utilities, conducts threat analysis, and provides alerts and briefings to help water systems detect and respond to emerging risks. In the past year, WaterISAC also helped provide support to mitigate threats to Arkansas City, Kansas, and the Boston Water and Sewer Commission when they experienced ransomware attacks.

Water systems today have access to a growing body of guidance and tools designed to improve cybersecurity preparedness. For example, WaterISAC's *12 Cybersecurity Fundamentals for Water and Wastewater Utilities*[7]—available at no cost—provides a practical set of best practices for securing both information technology and industrial control systems. CISA also offers a free vulnerability scanning tool, a service that allows utilities and other industrial control system operators to scan their networks for known vulnerabilities, weak configurations, and suboptimal security practices. In addition, the National Institute of Standards and Technology (NIST) offers a cybersecurity framework that compiles existing standards, guidelines, and best practices to help organizations, including water systems, manage and reduce cybersecurity risk.

Multiple organizations are continuing to develop new tools and guidance. For example, AWWA's recent Water Sector Cybersecurity Risk Management Guidance and Assessment Tool

[7] https://www.waterisac.org/fundamentals

focuses on "first-mile" actions a utility can implement to manage cyber risk. It allows utilities to select either a small systems option (recommended for systems serving fewer than 10,000 people) or a full assessment option. Utilities respond to questions regarding technology applications, and the tool generates a customized, prioritized list of controls that are most applicable to mitigate cybersecurity vulnerabilities. In addition, in the past year, the EPA has developed checklists for evaluating cybersecurity practices of vendors during procurement and a template for response plans.

At Fairfax Water, we take a comprehensive multi-layered approach to physical and cybersecurity. Some of the defensive tactics we use include employing a third-party Systems Operations Center to monitor our network activity around the clock, use of multi-factor authentication for network access, fostering an organizational culture of vigilance through training and phishing scheme tests, aggressive patching of software and systems, and segmentation of our business and operational technology networks.

While a large, well-resourced public utility like Fairfax Water can invest in cybersecurity preparedness and take advantage of this collection of tools and resources, capacity across the water sector varies significantly. Unfortunately, far too many of the nation's 50,000 community water systems lack the dedicated personnel to make sense of these tools or the financial resources required to implement recommended measures. This gap is well documented. A 2021 *Cybersecurity State of the Sector* survey conducted by the Water Sector Coordinating Council found that although 55 percent of responding utilities identified cybersecurity as a high priority, only about 25 percent participate in cyber-focused tabletop exercises, and just 40 percent conduct cyber risk assessments on at least an annual basis.[8] Given the burden of complying with the many existing regulations for drinking water services—and addressing the $1.2 trillion of needed water infrastructure investment over the next two decades—many utilities are forced to prioritize their most pressing infrastructure needs, which can result in limited attention to cybersecurity.[9,10]

Legislative Recommendations

There are several legislative proposals pending before Congress that could help drinking water and wastewater systems learn about cyber threats, become educated about appropriate preventative and response actions, and access financial resources to address cyber vulnerabilities. AMWA believes that each of these legislative proposals should remain part of the discussion as Congress explores ways to improve cybersecurity in the water sector. These proposals are discussed further below:

- H.R. 2344/S. 1118, the Water Intelligence, Security, and Cyber Threat Protection Act
- H.R. 5566/S. 3590, Water Infrastructure Resilience and Sustainability Act

[8] https://www.waterisac.org/2021survey
[9] https://www.epa.gov/system/files/documents/2024-05/2022-cwns-report-to-congress.pdf
[10] https://www.epa.gov/system/files/documents/2023-09/Seventh%20DWINSA_September2023_Final.pdf

- S. 3251, State and Local Cybersecurity Grant Program Reauthorization Act
- H.R. 2594, the Water Risk and Resilience Organization Establishment Act

Expand Participation in WaterISAC

Currently, there are few federal grant programs dedicated to bolstering water system cyber capabilities. Expanding existing programs as well as directing additional resources to support private-sector cybersecurity preparedness efforts would improve water systems' awareness of the latest cyber risks. It would also equip them with recommended actions that will help keep their systems and infrastructure secure. WaterISAC is an established water sector program that can help address this need.

ISACs exist for more than two dozen critical infrastructure sectors, such as electricity, aviation, maritime, and oil and natural energy. They are member-driven organizations delivering all-hazards threat and mitigation information to asset owners and operators. Despite its critical role in the water sector, WaterISAC receives no state or federal grant funding and therefore operates as a dues-based subscription service. Although these dues are structured on a sliding scale based on system size—with fees as low as $125 per year for systems serving less than 3,300 people and a partnership with the National Rural Water Association to make access free for their small system members—WaterISAC faces challenges in connecting with the thousands of water and wastewater systems across the country. Currently, only about 680 water and wastewater systems are members of WaterISAC, equating to about one percent of all such systems nationwide. Increasing participation in WaterISAC to include more of the nation's water systems would raise the sector's baseline level of preparedness by providing more utility managers with the tools they need to withstand natural, physical, and cyber threats.

As water utilities continue to experience an increase in cyber attacks, WaterISAC has helped utilities maintain strong cyber and physical security. One example of how WaterISAC does this is through timely reporting on critical vulnerabilities. For example, in January 2025, suspected Chinese threat actors were exploiting four vulnerabilities in Ivanti Cloud Services Appliances, and WaterISAC shared this information with the sector within 24 hours of CISA's and the FBI's advisory. In December 2025, WaterISAC hosted a webinar on safely utilizing the cloud amidst cyber threats. The webinar included information about how leading utilities are assessing risk, securing the cloud, governing across IT and OT, and leveraging AI to build true operational resilience. The webinar helped participants identify and close security gaps across hybrid environments, strengthen governance and compliance for water-sector requirements, use AI-driven tools to train teams and validate readiness, and build continuity and resilience into every layer of operations. WaterISAC is invaluable at facilitating information sharing and peer-to-peer learning opportunities for water utilities, which will only be bolstered by increased participation from more water systems.

Legislation such as H.R. 2344/S. 1118, the Water Intelligence, Security, and Cyber Threat Protection Act, would increase WaterISAC participation by directing EPA to educate water systems about resources offered through WaterISAC and allocating funding to help water systems offset WaterISAC's membership costs. Based on a similar Energy Department program authorized by Congress in 2021 to better connect electric utilities with their sector's ISAC, the legislation recognizes that simply raising awareness of the cyber resources available to water systems is a critical first step to facilitating adoption of cybersecurity best practices. Similarly, the funding assistance provided through the bill would ensure that no water system misses out on having access to these resources because of cost.

Fund EPA Water System Cyber Resilience Programs

In 2021, Congress authorized two EPA grant programs that help drinking water and wastewater systems build resilience to cyber threats. Each of these programs is set to expire following the 2026 fiscal year. AMWA strongly urges Congress to reauthorize and fund these programs to provide water and wastewater systems with a dedicated stream of financial assistance for essential cybersecurity projects, without diverting resources away from public-health focused infrastructure investments.

The Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program (42 USC 300j-19g) and the Clean Water Infrastructure Resiliency and Sustainability Program (33 U.S. Code 1302a) offer grant assistance for drinking water and wastewater utility projects to increase resilience to cyber threats, as well as resilience to extreme weather and natural disasters. Types of cybersecurity enhancements that are eligible for assistance under the program include:

- Conducting cyber risk assessment and implementing priority cybersecurity practices, updating drinking water system operation technology (including Supervisory Control and Data Acquisition (SCADA), Human Machine Interface (HMI), programmable logic controllers (PLCs) or Remote Terminal Unit (RTU) systems);
- Strengthening computer network defenses by implementing or updating cyber locks, multifactor authentication, firewalls, virtual private networks and segmentation;
- Establishing offsite back-ups of critical data, development of an incident response plan, and incident action checklists; and
- Conducting cybersecurity awareness training for water system staff.[11]

While many of these practices are standard operating procedure for large water systems like Fairfax Water, less well-resourced systems may not always prioritize these activities when working to address infrastructure renewal needs and comply with water quality regulations. A major contributing factor to this is the need for water systems to keep water rates affordable for

[11] https://simpler.grants.gov/opportunity/2508c664-7253-4661-a474-8a881d3bc0ae

customers. Having an avenue for EPA to assist water systems with offsetting some of the costs associated with enhancing cyber preparedness would encourage more water systems to give this issue the attention it deserves.

For these reasons, AMWA supports the Water Infrastructure Resilience and Sustainability Act (H.R. 5566/S. 3590), which would reauthorize these programs for another five years, through 2031. Last fall, EPA announced the availability of the first $9.5 million in grant funding for the Midsize program. The agency is expected to announce the first round of grant recipients in Spring 2026.

To date, the programs have received very little appropriations. Fully funding these programs, at their annual authorized levels of $50 million and $25 million, respectively, 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.

State and Local Support

Directly supporting state and local governments with funding has also been an important pillar of improving cybersecurity practices. S. 3251, the State and Local Cybersecurity Grant Program Reauthorization Act, reauthorizes the State and Local Cybersecurity Grant Program (SLCGP) at $300 million for Fiscal Year 2026. SLCGP provides funding to state, local, and territorial governments to address cybersecurity risks and threats to information systems, improving the security of critical infrastructure – including municipal water and wastewater utilities. Again, the availability of these funds will help more water systems maintain awareness of cyber threats and equip them with resources to close identified security gaps.

Federal Cybersecurity Oversight

While the EPA and CISA have guidance documents on best practices, incident response, and scanning tools, it is incumbent on water systems to utilize these resources and abide by these standards. Currently, there are no statutory federal requirements to guide water systems or enforce minimum standards for cybersecurity across the sector. While there is a danger in making federal regulations overly burdensome, complicated, or prescriptive, as cyber threats and technology evolve rapidly, some level of federal guidance to ensure that all water systems are taking appropriate steps to protect against cyber threats would be beneficial. It is important to note that any new federal requirements must be accompanied by the proper level of investment in federal programs and funding to support water systems in adhering to requirements.

Any new requirements must also align with America's Water Infrastructure Act (AWIA) of 2018, which amended section 1433 of the Safe Drinking Water Act to require community water

systems serving over 3,300 people to incorporate considerations of cybersecurity risks into mandated risk and resilience assessments, and strategies to improve cyber resilience into emergency response plans. Today water systems must certify to EPA that they have properly completed these tasks, and because these documents contain sensitive information there is no requirement for them to be shared beyond the utility. AMWA believes this restriction is appropriate and should continue.

One legislative option that AMWA believes should be explored further is H.R. 2594, the Water Risk and Resilience Organization Establishment Act. This proposal would establish a governing body, the WRRO, comprised of cyber experts and drinking water and wastewater system operators to help develop, recommend, and enforce cybersecurity requirements for drinking and wastewater systems. Based on the model of the North American Electric Reliability Corporation in the energy sector, the WRRO would work in partnership with the EPA to ensure that water systems employ minimum best practices to defend against cyber threats, while avoiding one-size-fits-all mandates. The WRRO therefore goes one step beyond simply making water systems aware of cyber best practices and would provide direction on specifically which actions individual water systems should adopt, based upon their size and unique risk profiles.

The WRRO model would leverage the expertise and experience of utility managers and operators when formulating practical requirements that consider utility scale, resources, existing challenges, and the most pressing threats. As Congress explores various options to bolster water systems' cybersecurity posture, AMWA strongly encourages that the WRRO model be part of the discussion.

Conclusion

On behalf of AMWA, I thank the Committee for the invitation to testify today, and to share the on-the-ground insights of Fairfax 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.