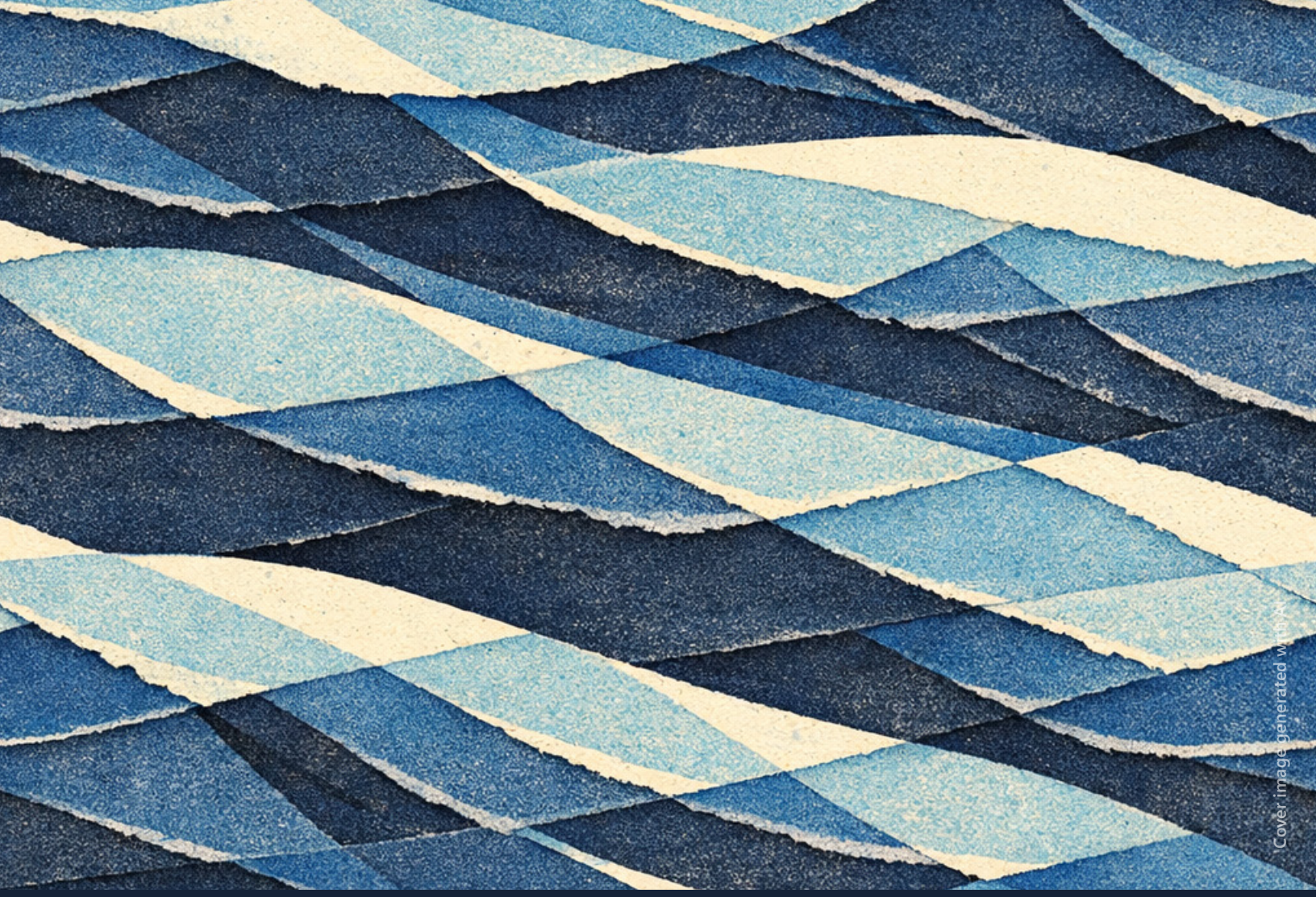


Cover image generated with AI

Water Utilities Need Cyber Support:

Lessons from the Cyber Readiness Institute's Pilot Project

Microsoft

CYBER READINESS INSTITUTE

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Executive summary

Cyberattacks on the nation's water and wastewater utilities are becoming more frequent and more dangerous. This critical infrastructure is an easy target for foreign adversaries because far too many have outdated software and poor password practices, and their control systems are exposed to the open internet, the Office of the Director of National Intelligence has warned.[1] In October 2024, American Water — the largest publicly-regulated U.S. water utility, serving more than 14 million customers — disclosed that a cybersecurity incident forced the company to disconnect customer billing and online portals.[2] Other utilities have found malicious activity in their networks, and hackers accessed or manipulated control systems.[3] Many utilities have been forced to revert to manual operations to continue delivering safe and clean water to customers during attacks.

If large, well-resourced utilities remain vulnerable, the risk is far more acute for the smaller systems that make up most of the sector. More than 97 percent of the nation's 156,000 public water systems serve fewer than 10,000 customers,[4] and many of these utilities have aging systems and operate with minimal IT or cybersecurity personnel. Their capacity to respond to a cyber incident is limited.

To help address the sector's cybersecurity gap, the Cyber Readiness Institute (CRI), in partnership with the Center on Cyber and Technology Innovation (CCTI) at the Foundation for Defense of Democracies and with sponsorship from Microsoft, launched a pilot to test whether accessible, behavior-focused cybersecurity training could measurably improve cyber readiness among water and wastewater utilities. The pilot sought to engage up to 200 small and medium-sized utilities over the course of two years.

The pilot leveraged CRI's existing, free Cyber Readiness Program, a self-paced program that presents fundamental cybersecurity concepts and focuses on the human behavior aspect of security. The Program aims to provide information at a level that can be understood by individuals with or without a cybersecurity background.

To support water utilities as they completed the Program, CRI also provided free Certified Cyber Coaches. The coaches met regularly with the utility's designated "Cyber Leader," the individual within an organization accountable for its cybersecurity decisions and for promoting cybersecurity awareness among an organization's employees. The Program is designed to help the Cyber Leader develop and implement cyber readiness policies and incident response procedures by providing one-on-one support.

To recruit participants, CRI and CCTI briefed water sector organizations, federal and state government partners, and state and local government associations. CRI and CCTI experts spoke at conferences and webinars. CRI made phone calls to more than 1,000 utilities. Enthusiasm and interest were high among audiences. Several utilities participating in the pilot cited growing concerns about ransomware and other disruptive cyber threats as motivation for enrolling, even if they had not previously experienced an incident.

Ultimately, the pilot confirmed the need for cybersecurity training and the recognition among water utilities of the importance of improving their resilience against cyber threats. The discrepancy between the high level of interested and the lower completion rates, however, raises concerns about the capacity of the sector – particularly of the small and medium-size members – to address cybersecurity gaps without more significant financial and technical support. Policymakers, sector associations, and private organizations should use the following recommendations when implementing future programs to strengthen cybersecurity readiness:

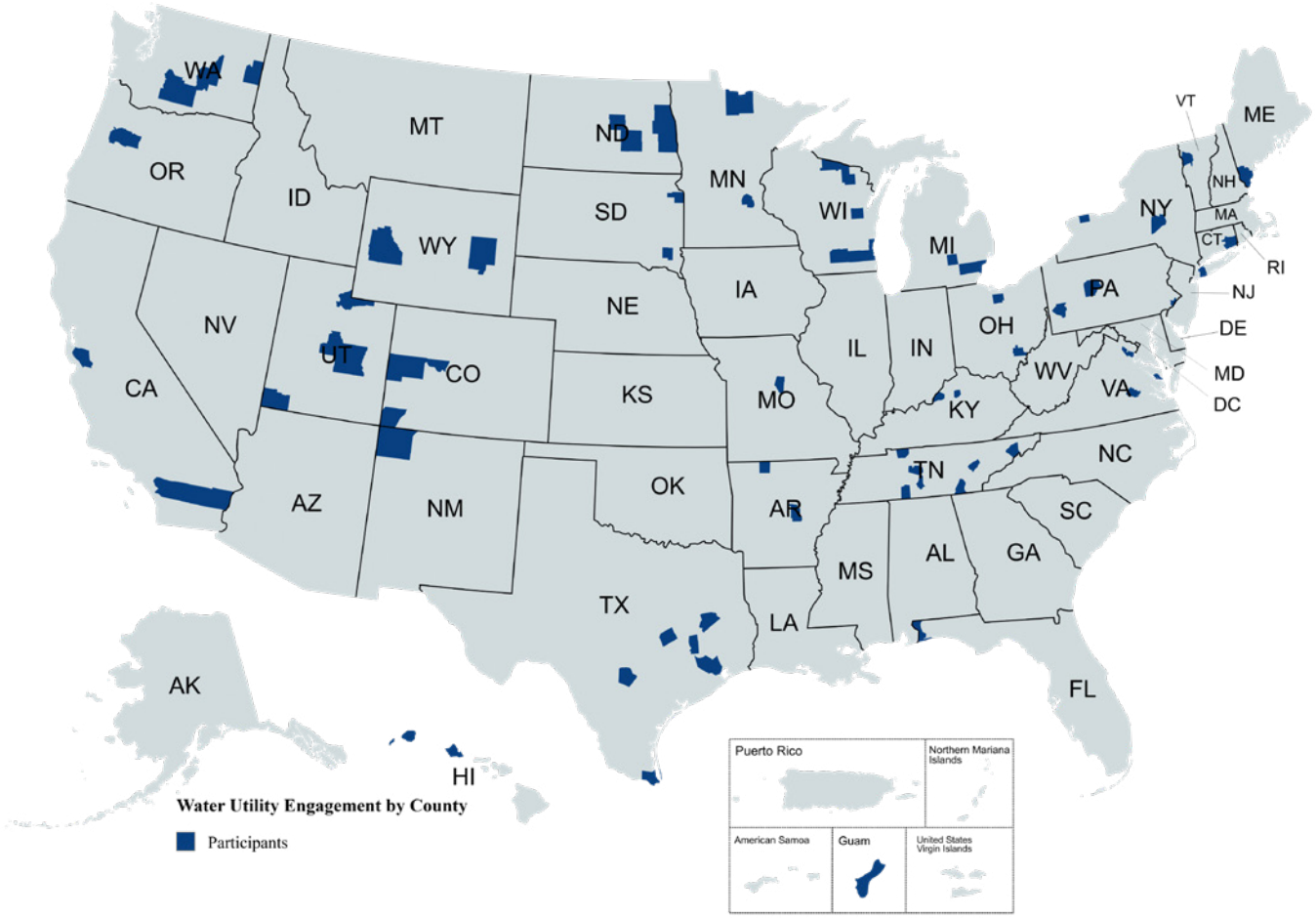
1. **Recognize that "Free" Is Not Enough**
2. **Include Hands-On Technical Assistance to Support Implementation**
3. **Add Cybersecurity Training to Operator Licensing and Continuing Education Requirements**
4. **Leverage Water Sector Associations to Drive Cybersecurity Improvements**

Pilot results

The Cyber Readiness Program's modules educate the Cyber Leader on the "Core Four," that is, strong passwords and multifactor authentication, software update management, phishing awareness, and secure file storage and sharing. The Program also explains how to develop a business continuity plan. The "Cyber Readiness Playbook," a set of cybersecurity and incident response policies that the Cyber Leader completes as part of the Program, contains worksheets on asset management, cybersecurity policy and incident response templates, and additional employee training resources.

To receive verification of completion from CRI, participants must complete the training modules, submit their Cyber Readiness Playbook for CRI's review, including an Incident Response Plan, policies, asset management worksheets, and provide an attestation that they provided cyber readiness training to their employees. Because of this last requirement, CRI's water pilot succeeded in training 551 employees and contractors across 27 states and territories, including Hawaii and Guam.

MAP OF PARTICIPANTS



While the pilot was initially conceived as targeting small (501-3,300 customers) and medium-sized (3,001-10,000 customers) utilities,[5] the Program ended up engaging roughly an equal number of small, medium, and large systems (serving more than 10,000 customers). Most utilities in the pilot were drinking water providers or combined water and wastewater systems, with only a small minority operating wastewater-only services.

Utilities participating in the pilot repeatedly emphasized the value of the Cyber Readiness Program, particularly having a structured plan to rely on in the event of a cyber incident, such as a ransomware attack. Initially, CRI, FDD, and Microsoft held discussions about whether the Program would fully reflect the complexity of real-world utility operations, but ultimately underscored that its strength is delivering practical, repeatable foundational steps. Participants repeatedly noted that the Program was relevant to their operations. A participant from one large utility noted that they clearly see the value of the Program and its resources for smaller utilities, drawing on prior experience working at a small utility. While none of the surveyed utilities reported experiencing a ransomware attack during the pilot, participants noted the value of the playbook to prepare for scenarios they viewed as increasingly likely.

Among the 57 respondents that completed the feedback survey, more than 90 percent agreed that they better understood cybersecurity basics, and a similar proportion reported they were likely to take action to improve their utilities' cybersecurity posture based on the training. Participants highlighted the value of the "Core Four," the password guidance, and the Playbook's worksheets and incident response plan in particular, as helpful for understanding how to prepare for and respond to ransomware and other disruptive cyber incidents. Several noted that the Program helped them identify gaps in their cybersecurity posture they had not documented, including missing business continuity plans, outdated password policies, or inconsistent staff awareness training.

A case study on the East Rio Hondo Water Supply Corporation, a mid-sized rural utility serving approximately 9,300 customers in southern Texas, confirmed the transformative nature of the Cyber Readiness Program.[6] Through the Program, the utility's Cyber Leader – who did not have previous cybersecurity knowledge or training – successfully used CRI materials and Cyber Coach support to train employees on basic cybersecurity practices. After training, staff demonstrated improved ability to identify and handle phishing emails with employees telling their Cyber Leader, "They hadn't realized how exposed they were. They learned not only how to protect the company but also how to protect themselves at home." This case reinforces a broader finding of the pilot: structured materials paired with coaching can translate cybersecurity awareness into operational readiness.

> This program has made employees more cyber ready and better able to prevent incidents.

Interest is high, capacity is low

While interest among audiences hearing about CRI's Program was high, it was difficult to translate interest into Program completion. While 113 utilities submitted initial interest forms, only 72 began the Program, and only 43 completed it.

Of those that began the Program, 12 opted to move forward without a CRI Certified Cyber Coach. The lack of a Cyber Coach significantly decreased the likelihood of successful completion of the Program. While 76.7 percent of Cyber Coach supported utilities completed the Program, only 23.3 percent of self-paced participants did. Completion rates were consistent across system sizes, indicating that capacity constraints affected utilities regardless of size.

CRI sought feedback from water associations on behalf of the members. In response, the Water Information Sharing Analysis Center's Director of Infrastructure Cyber Defense, Jennifer Lyn Walker, noted, "Despite lower completion rates, participation in the Resiliency for Water Utilities Pilot is encouraging, demonstrating that when effective assistance is provided, utilities were ready, willing, and able to make the necessary time and effort to work toward securing their utilities. Likewise, the Resiliency for Water Utilities Pilot proved the path to cyber resiliency doesn't have to be overwhelming, and even small intentional actions forward go a long way."

While those who dropped out of the Program did not reveal why, survey responses by those who completed the Program reveal that the cause is likely limited staff time and capacity. Several utilities reported having minimal staff — in some cases being "the only employee" — or relying entirely on third-party IT vendors. When asked why they might not act based on the Program's training and recommendations, respondents most frequently cited lack of security personnel (26 responses), lack of funding (24 responses), and lack of guidance to implement security (13 responses). Additionally, although the Cyber Readiness Program is intended to take approximately six weeks, most participants needed significantly more time to complete the Program because of staffing shortages and scheduling.

While awareness and willingness to improve cybersecurity are high, without additional support, utilities will continue to face structural constraints that impede their ability to implement more robust cybersecurity practices.

> This course is an approachable starting point for small organizations who don't know where to start.

Recommendations

The pilot revealed a consistent pattern: water utilities understand the importance of cybersecurity but lack the capacity to implement improvements. Improving cybersecurity in the water sector therefore requires targeted support that addresses operational constraints, not just awareness or training. The following recommendations are based on insights from the pilot into what federal and state policymakers, sector associations, and private organizations can do to strengthen cybersecurity readiness nationwide.

1 - Recognize that "Free" is not enough

Federal agencies – including the Environmental Protection Agency (EPA) and Cybersecurity and Infrastructure Security Agency (CISA) – offer advisories, threat alerts, and technical assistance.

In October 2025, the EPA released yet another water sector cybersecurity procurement checklist.[7] However, many utilities report difficulty navigating dispersed guidance, connecting resources to day-to-day operations, or carving out staff time for cybersecurity training.

The survey responses highlight a structural mismatch between what free cybersecurity programs offer and what water utilities need to improve their security posture. Despite broad agreement that the Cyber Readiness Program strengthened basic understanding, utilities consistently reported barriers that free materials alone cannot overcome. The two most cited obstacles — lack of security personnel and funding — both directly limit a utility's ability to engage with and apply no-cost resources. Several respondents also indicated they outsourced most IT responsibilities or lacked the internal bandwidth to complete policies or processes even when templates were provided.

Federal and state cybersecurity programs therefore must move beyond the assumption that no-cost tools, checklists, and voluntary offerings are sufficient for improving sector-wide cybersecurity. CISA's recent decision to rely even more heavily on its own free services and cut funding to organizations like Multi-State Information Sharing Analysis Center and other associations that provide hands-on assistance will only exacerbate the practical constraints highlighted by the survey.

2 - Expand hands-on technical assistance to support implementation

Policymakers should fund programs that provide capacity building, not just content. Embedding cybersecurity coaches, regional support teams, and technical experts who can assist with configuration will improve implementation of cybersecurity best practices. Free offerings should be paired with personalized support that helps utilities apply guidance, complete policies, and adopt foundational controls. Without this shift, the utilities most willing to improve will remain the least able to act, and the sector's cybersecurity posture will continue to lag despite widespread availability of no-cost resources.

Federal and state policymakers should invest in hands-on technical assistance models that help small and medium-sized utilities implement basic cybersecurity practices. Respondents described being "the only employee," relying heavily on third-party IT vendors, or needing clearer examples to complete policies. Many reported that while the program provided a useful "starting point," "great material," or "a plan to implement," they still lacked the staff, time, or direction to carry out the recommendations. Meanwhile, others already understood the concepts but needed help turning best practices into fully developed policies or security processes.

This support should go beyond training materials and include direct assistance with configuring systems, drafting policies, and operationalizing incident response playbooks. The American Water Works Association's Federal Relations Manager, Dr. Kevin Morley, testified before the House Homeland Security Committee that the sector needs "funding that prioritizes and expedites technology upgrades."[8] In addition to cybersecurity grants, federal and state agencies could fund dedicated implementation teams or regional cybersecurity coaches who pair with utilities to adapt materials to their specific operational environment. Incorporating cybersecurity assistance into the National Rural Water Association's (NRWA) existing Circuit Rider Program likely would provide the scale and existing local relationships necessary to get hands-on cybersecurity assistance to utilities quickly.[9]

3 - Include cybersecurity training in operator licensing and continuing education requirements

One of the clearest findings from the pilot is that incentives matter. Regulators often require operators to earn periodic continuing education credits or units to maintain state licenses. Credits are typically earned through approved courses, programs, and industry conferences on treatment processes, quality, and safety that meet state-specific guidelines.

In August, the Water Sector Cybersecurity Task Force co-led by EPA released a series of recommendations for government, associations, and utilities. The task force noted the need to "embed cybersecurity in utility culture," recommending integrating "cybersecurity into operator certification and continuing education."[10]

During the Resiliency for Water Utilities Pilot, the New York Department of Environmental Conservation approved the Cyber Readiness Program for wastewater operator renewal credits, providing a model that other states could replicate. The approval process began after a single operator submitted their CRI certificate of completion for credit hours, demonstrating both operator demand and the Program's alignment with state training standards. The State of New York granted four hours of credit to reflect the learning experience, and the Program is now listed alongside other pre-approved courses for wastewater operator recertification.

Because operators are already required to complete continuing education hours, aligning cybersecurity training with existing workforce requirements offers a powerful, low-burden, nonregulatory incentive. This approach allows states to strengthen sector cybersecurity without imposing new mandates but instead leveraging existing professional development pathways.

4 - Leverage Water Sector Associations to Drive Cybersecurity Improvements

The pilot demonstrated that outreach partners played a critical role in generating participation. Utilities that heard about the Program and joined because of recruitment by industry and state associations showed high completion rates. Direct outreach from CRI to utilities yielded little engagement. Calling more than 1,100 utilities produced only 161 interest forms and only a handful of utilities starting the Program. In contrast, association-driven outreach accounted for the majority of utilities that not only enrolled but also completed the Program. Over half of association recruited entities completed the Program whereas a third of those recruited through other means completed the Program.

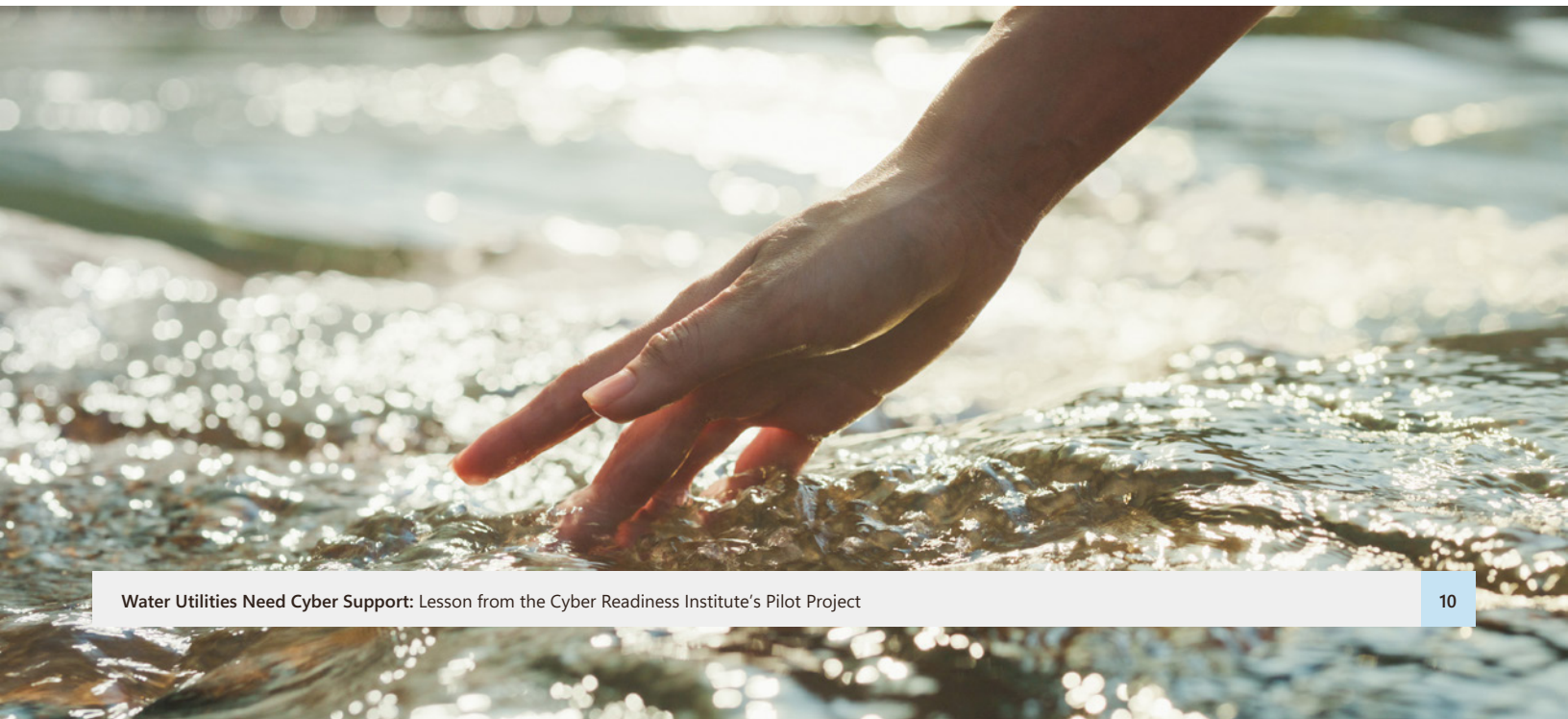
Feedback survey responses reinforce this dynamic: utilities that already had some policies, vendor support, or training in place still chose to participate when they heard about the Program through a trusted association, indicating that utilities depend on sector intermediaries to filter, validate, and prioritize which cybersecurity efforts are worth their limited time. To increase participation in existing programs and to improve the cybersecurity particularly of smaller utilities, federal and state agencies must partner with sector associations that are already viewed as trusted sources of information. These associations in turn can integrate cybersecurity into routine association trainings, conferences, and certifications. This will likely be the most effective channel for scaling voluntary cybersecurity programs.

Conclusion

The pilot demonstrated that no-cost, accessible cybersecurity training can improve awareness and readiness across water and wastewater utilities, but only when paired with the support structures that enable real implementation. As real-world cyber threats targeting water and wastewater systems continue to grow, utilities are increasingly seeking practical and actionable ways to prepare. Small and medium-sized systems showed strong willingness to participate, yet the survey findings underscore that willingness alone cannot overcome chronic staffing, funding, and operational constraints.

Strengthening the cybersecurity of the nation's water sector requires shifting from information distribution to capacity building — embedding hands-on assistance, aligning cybersecurity with existing operator requirements, and leveraging trusted sector associations to scale participation. These approaches will help ensure utilities not only learn foundational cybersecurity practices but are fully equipped to implement and sustain them, translating training into tangible improvements in operational resilience.

> "An excellent program that gives small and large organizations a strong foundation."



Endnotes

1 The Office of the National Director of Intelligence, "Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024," June 2024. (https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf)

2 Raphael Satter, "Water utility American Water disconnects computers following 'cybersecurity incident'," Reuters, October 8, 2024. (https://www.reuters.com/technology/cybersecurity/water-utility-american-water-disconnects-computers-following-cybersecurity-2024-10-08)

3 The Office of the National Director of Intelligence, "Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024," June 2024. (https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf)

4 U.S. Environmental Protection Agency, "Learn about Capacity Development," Last updated on September 9, 2025. (https://www.epa.gov/dwcapacity/learn-about-capacity-development)

5 U.S. Environmental Protection Agency, "Small Drinking Water System Variances," last updated January 23, 2025. (https://www.epa.gov/sdwa/small-drinking-water-system-variances#definition)

6 Cyber Readiness Institute, "Case Study: East Rio Hondo Water Supply Corporation Strengthens Cyber Readiness through CRI Water Utility Program," Accessed on December 15, 2025. (https://cyberreadinessinstitute.org/case-study-east-rio-hondo-water-supply-corporation-strengthens-cyber-readiness-through-cri-water-utility-program)

7 U.S. Environmental Protection Agency, Press Release, "EPA Releases New Resources to Help Protect Water Systems, Strengthen Cyber Resilience," October 23, 2025. (https://www.epa.gov/newsreleases/epa-releases-new-resources-help-protect-water-systems-strengthen-cyber-resilience)

8 Homeland Security Committee Events, "Securing Operational Technology: A Deep Dive into the Water Sector," YouTube, February 6, 2024, 33:30. (https://www.youtube.com/live/LNcX7MCJfnU?si=YKvAReLg6U-cPYPc4&t=2010)

9 Representatives Donald G. Davis (NC-01) introduced H.R. 2109, the Cybersecurity for Rural Water Systems Act, on March 14, 2025. The bill would amend Department of Agriculture's Circuit Rider Program to include cybersecurity technical assistance for rural water systems serving fewer than 10,000 people and was referred to the House Committee on Agriculture. Senator Catherine Cortez Masto (D-NV) introduced the Senate companion, S. 1018 on March 13, 2025. As of publication, no further actions have been taken on either bill. See, (https://www.congress.gov/bill/119th-congress/house-bill/2109/text) and (https://www.congress.gov/bill/119th-congress/senate-bill/1018/all-info)

10 Environmental Protection Agency, "Security the Future of Water: Addressing Cyber Threats Today," August 2025, page 5. (https://www.epa.gov/system/files/documents/2025-08/water-cybersecurity-recommendations_water-sector-cybersecurity-task-force_apr25-072525.pdf)


Microsoft