Testimony of the New York Section American Water Works Association

Before the New York State Senate Standing Committees on Local Government, Cities 1, and Cities 2

Joint Public Hearing on the Implementation, Fiscal Impact, and Technical Sufficiency of Mandatory State Water and Wastewater Security Regulations

Senate Hearing Room, 250 Broadway, 19th Floor, New York, NY

October 1, 2026

Chair Martinez, Chair Bottcher, Chair Ryan, and members of the Committees, thank you for the opportunity to testify on the implementation, fiscal impact, and technical sufficiency of New York's water and wastewater cybersecurity regulations.

My name is Daniel DuBois and I am a member of the Water Utility Council and testifying today on behalf of the New York Section American Water Works Association. NYSAWWA is the statewide voice of water professionals who safeguard public health and sustain New York's essential water infrastructure. Our members include operators, engineers, utility leaders, scientists, regulators, manufacturers, service providers, and other experts who bring firsthand knowledge of the operational, technical, and financial realities facing water systems of every size.

NYSAWWA supports New York's efforts to strengthen the cybersecurity and operational resilience of its water and wastewater systems. As the State moves from adopting these regulations to implementing them, the focus must be on ensuring that the requirements achieve meaningful risk reduction within the complex operating environments of public utilities.

Every affected utility will be responsible for meeting these requirements, but utilities do not all have the same staffing, financial resources, infrastructure, or access to specialized expertise. Successful implementation will require sustained funding, professionals who understand both cybersecurity and operational technology, clear guidance from each State agency, and reasonable implementation timelines. With the right support, these regulations can strengthen security and resilience while allowing utilities to continue providing safe and reliable service.

Operational and Technical Considerations

Water and wastewater systems operate continuously and cannot simply be shut down for extensive technology upgrades. Many utilities rely on a combination of modern information technology, specialized operational technology, supervisory control and

data acquisition systems, and legacy equipment designed to remain in service continuously . Alterations to these systems and networks must be carefully planned, tested, and integrated without interrupting treatment or distribution.

Cybersecurity in this environment requires specialized knowledge. Utilities need professionals who understand not only conventional information technology, but also operational technology, industrial control systems, treatment processes, and the public-health consequences of service disruptions. That expertise is limited and can be especially difficult for smaller and resource-constrained utilities to obtain.

Technical sufficiency therefore cannot be measured only by whether a utility has completed a required document or installed a particular product. The requirements must produce measurable risk reduction without disrupting treatment operations. Implementation guidance should recognize the differences between information technology and operational technology, allow appropriate compensating controls for legacy equipment, and remain adaptable as threats and technologies evolve. It should also be developed with continuing input from utility operators, engineers, and cybersecurity professionals.

The Department of Health and Department of Environmental Conservation regulations adopted in 2026 appropriately address operator training, incident reporting, emergency and incident-response planning, asset inventories, access controls, vulnerability management, network security, monitoring, documentation, and recurring certification. These are reasonable security objectives. Implementing them correctly, however, requires sustained attention and ongoing investment.

The two agencies regulate different systems and impose different requirements. The Department of Health requirements apply to community water systems serving more than 3,300 people, with additional provisions for systems serving more than 50,000 people. The Department of Environmental Conservation requirements include reporting requirements for State Pollutant Discharge Elimination System permittees, as well as additional controls for publicly owned treatment works and monitoring and logging requirements for larger facilities.

Utilities must understand which provisions apply, identify qualified assistance, complete assessments, develop or revise plans, procure technology and services, train personnel, and document compliance. Major implementation deadlines beginning in January and March 2027 leave a limited window for this work. Each agency should provide clear, practical guidance so utilities can determine which requirements apply and avoid repeating work already completed.

Many water utilities also operate within larger municipal IT environments. Changes such as network segmentation or dedicated systems may require coordination with municipal staff, specialized integration, and additional funding. Implementation guidance should account for these shared systems and the time needed to make changes safely.

Fiscal Impact

NYSAWWA recently conducted a preliminary survey of its utility members to better understand the financial impact of the new regulations. Because the sample is preliminary, the results should not be treated as a statewide average. They nevertheless show the magnitude and variability of the costs utilities are confronting.

Utilities serving between 10,000 and 49,999 people estimated initial costs of approximately $15,000 to $300,000 and continuing annual costs of approximately $15,000 to $90,000. Utilities serving between 50,000 and 99,999 people estimated approximately $15,000 to $350,000 in initial costs and $40,000 to $500,000 in annual costs. Among responding utilities serving 100,000 people or more, estimated initial costs ranged from approximately $20,000 to more than $350,000, while annual costs ranged from approximately $50,000 to more than $700,000.

These estimates include vulnerability assessments, third-party monitoring and scanning, software and licensing, consulting, cybersecurity insurance, penetration testing, equipment, training, documentation, and staff time. The survey confirms that compliance creates both substantial initial expenses and significant recurring obligations. In many cases, the annual cost of continuous monitoring, scanning, licensing, testing, and expert support may exceed the initial implementation cost.

Utilities also identified broader implementation challenges, including uncertainty about regulatory expectations, limited staff capacity, compressed timelines, legacy equipment, and difficulty obtaining qualified cybersecurity and operational-technology expertise. These issues are interconnected. A utility may understand what must be done but still lack the personnel, procurement flexibility, or financial capacity to complete it on schedule.

For a smaller utility with only a few licensed operators, the same employees responsible for treatment and daily operations may also have to manage assessments, procurement, training, and cybersecurity documentation. Time away for training or implementation requires staff coverage, while specialized monitoring and support contracts are spread across a limited customer base. This is why recurring funding and access to shared technical expertise matter as much as help with the initial upgrade.

Traditional municipal procurement processes can present another obstacle. Cybersecurity and SCADA projects often require specialized qualifications, careful integration, and rapid response to evolving risks. Lowest-price bidding alone may not identify the provider best qualified to protect an operational system. The Legislature should evaluate whether municipalities need expanded access to qualifications-based selection, design-build authority, cooperative purchasing, and updated bidding and bonding thresholds for specialized cybersecurity and SCADA projects.

NYSAWWA appreciates the State's early support, including the more than $9 million awarded in August 2026 through the SECURE grant program for 153 cybersecurity projects. This was an important step. However, one-time grants cannot by themselves support continuing monitoring, licensing, testing, training, maintenance, and specialized assistance. Sustainable compliance will require recurring support.

Legislative Recommendations

NYSAWWA respectfully recommends that the Legislature take the following actions:

1. **Provide recurring funding for both implementation and operations.** Funding should cover eligible capital improvements as well as ongoing monitoring, software and licensing, testing, training, maintenance, documentation, and specialized professional services. Programs should use streamlined applications, reasonable local-match requirements, and predictable funding cycles.
2. **Prioritize systems with limited financial and technical capacity.** State support should account for a utility's customer base, staffing, existing infrastructure, fiscal capacity, and level of risk—not simply the size of an individual project. Compliance should not force utilities to choose between cybersecurity and other essential public-health investments.
3. **Expand accessible technical assistance.** Shared or regional access to professionals who understand both cybersecurity and water-sector operational technology could expand access to specialized expertise, reduce duplication, and help more utilities use limited public funding effectively. Assistance should include assessments, procurement support, implementation planning, incident-response exercises, and workforce training.
4. **Use existing processes to identify implementation needs.** Direct DOH and DEC to draw on regulatory oversight, State grant programs, and confidential utility input to brief the Legislature on common costs and barriers. Report findings in aggregate so future funding reflects demonstrated need without exposing sensitive system information.
5. **Protect sensitive information and maintain utility involvement.** Cybersecurity plans, network details, vulnerability assessments, and incident information must be protected from unnecessary public disclosure. Utilities should remain directly

involved as guidance and programs are refined, working with the State and trusted partners such as CISA, EPA, and the American Water Works Association.

New York's water and wastewater utilities understand the seriousness of the cyber threat and their responsibility to protect the communities they serve. They are prepared to do this work, but durable security depends on more than a compliance deadline. It requires sustained investment, specialized expertise, practical guidance, and a long-term partnership between the State and its utilities.

We ask the Legislature to support recurring funding, accessible technical assistance, appropriate procurement tools, protection of sensitive information, and aggregate reporting on implementation costs. With continuing utility input, these actions can turn regulatory requirements into measurable risk reduction and lasting operational resilience.

Thank you for the opportunity to testify. NYSAWWA looks forward to working with the Legislature, State agencies, and our utility partners on effective implementation.