



*Testimony of the*

New York State Conference of Mayors – Barbara Van Epps, Executive Director

*and the*

New York Association of Towns – Christopher A. Koetzle, Executive Director

*Submitted to the*

New York State Senate

Standing Committee on Local Government

Hon. Monica Martinez, Chair

New York State Senate

Standing Committee on Cities 1

Hon. Erik Bottcher, Chair

New York State Senate

Standing Committee on Cities 2

Hon. Chris Ryan, Chair

***Hearing to Examine the Implementation, Fiscal Impact, and Technical Sufficiency of  
Mandatory State Water Security and Wastewater Security Regulations***

Thursday, October 1, 2026

New York, New York

On behalf of the New York State Conference of Mayors and Municipal Officials (NYCOM) and the New York Association of Towns (NYAOT), we appreciate the opportunity to express our views related to the implementation, fiscal impact, and technical sufficiency of water and wastewater security requirements.

Founded in 1910, NYCOM is a nonpartisan, voluntary membership organization consisting of 576 of the State's 594 cities and villages. NYAOT is likewise a voluntary membership whose membership consists of 908 of New York State's 933 towns. Together, our associations encompass the vast majority of New York's cities, villages, and towns and the residents they serve. We provide training, education, and advocacy on matters affecting our respective municipal members and their local officials and our testimony is grounded in the collective experience, perspectives, and operational needs of the communities we represent.

Municipalities share the State's goal of protecting public health, water quality, and critical infrastructure from both natural and human-made threats. Local governments also recognize that drinking water and wastewater systems are increasingly targeted by cybersecurity threats and that preparedness planning is essential to ensuring safe and reliable systems for all residents of the State. The cyber-attacks on water systems in August 2026 confirmed how important it is for local governments to be prepared. To that end, we support efforts to strengthen cybersecurity protections for these critical systems and recognize the importance of establishing consistent security requirements. At the same time, the effectiveness of these requirements depends in significant part on whether the municipalities have the resources, technical and staffing capacity, and practical ability to implement them. Our goal is to ensure that these requirements achieve their intended security objectives while providing municipalities with a workable framework for compliance.

Local governments own and operate the majority of these facilities in New York State, making them essential partners in protecting this critical infrastructure. Their day-to-day experience managing water and wastewater systems provides an important perspective on how security requirements function in practice. Our testimony therefore reflects both the priorities and concerns of our members and the practical realities of implementation at the local level. We look forward to working with the Legislature to ensure that statewide obligations strengthen cybersecurity, while remaining technically appropriate, fiscally responsible, and achievable for local governments to implement.

We wish to highlight several considerations:

- 1. Resource and Capacity Constraints**

Municipalities vary widely in size, staffing, technical expertise, and budgets. While larger water and wastewater systems may have greater resources to implement comprehensive

cybersecurity programs, many smaller and rural systems operate with limited personnel and information technology (IT) capacity. Requirements for maintaining cyber asset inventories and management programs, conducting vulnerability assessments, implementing multi-factor authentication and network monitoring, development cybersecurity policies and incident response plans, and integrating those plans into emergency response actions can present significant challenges for smaller systems.

These requirements also create both initial and ongoing costs for local governments, including investments in hardware, software, consultants, monitoring services, training, and compliance. For municipalities already operating with limited IT budget and competing technology priorities, these costs will have a disproportional impact on their ability to implement new requirements. While the value of protecting critical water and wastewater infrastructure from cyber threats is clear, requiring cities, towns, and villages to absorb these costs without additional support creates a significant unfunded mandate.

We appreciate the State's establishment of the Strengthening Essential Cybersecurity for Utilities and Resiliency Enhancements (SECURE) grant program, administered by the Environmental Facilities Corporation, to support cybersecurity assessments and implementation measures for drinking-water and wastewater systems. The program's inaugural round initially made \$2.5 million available, and the State subsequently announced awards totaling more than \$9 million for 153 local-government projects statewide. These investments, together with EFC's no-cost technical assistance, are meaningful steps toward assisting local governments with the State's new minimum cybersecurity standards for water and wastewater systems.

Nevertheless, sustained and expanded assistance remains necessary to meet the comprehensive security needs of water and wastewater systems statewide. Local systems must assess and mitigate operational and information-technology risks, implement appropriate access controls, develop cybersecurity policies and incident-response capabilities, train personnel, and maintain these protections over time. A competitive, capped grant program, even one that has supported many communities, may not provide sufficient or predictable resources for every municipality, particularly those with smaller systems with limited staff, technical capacity, and fewer ratepayers.

We therefore urge the State to pair cybersecurity requirements with additional, needs-based financial and technical assistance. This support may include recurring, dedicated, and appropriately scaled cybersecurity funding for local water and wastewater systems, or grant and cost-sharing programs targeted at smaller and rural communities who often lack the staff and resources to submit competitive grant applications compared to their larger counterparts.

## **2. Training and Technical Support**

Training and the development of clear policies and the assignment of responsibilities are essential components of an effective cybersecurity program and are just as important as understanding the technology itself. Cybersecurity protections are most effective when employees understand their roles, municipal officials understand the municipality's response obligations, and everyone involved knows who is responsible for identifying, reporting, and responding to incidents.

Water and wastewater operators already undergo substantial training and certification to maintain compliance with state and federal requirements. Additional cybersecurity training obligations should therefore be accompanied by robust training programs, regional delivery options, online resources and clear technical guidance, all of which is supported by the state. These opportunities would help ensure that operators and other municipal personnel can realistically participate and develop the knowledge necessary to protect critical infrastructure.

The State can further support municipal compliance by developing and distributing model documents and technical resources tailored to municipal water and wastewater systems. Templates for cybersecurity policies, vulnerability management programs, incident response plans, emergency response plan integration, and other required documentation would reduce duplicative efforts and promote consistency across the State. While federal guidance provides a useful foundation, New York-specific resources would be particularly valuable to smaller communities that lack dedicated cybersecurity personnel. State-developed templates and guidance could also help municipalities better understand how the various cybersecurity requirements applicable to their water and wastewater systems fit together.

NYCOM and NYAOT would readily assist the State in these efforts and disseminate information through our publications and direct communications. Our associations are also able to provide opportunities for the State to offer training through at our respective conferences or through webinars.

## **3. Incident Reporting, Compliance Timelines, and Coordination with Existing Requirements**

We appreciate the coordinated efforts of the Department of Homeland Security and Emergency Services (DHSES), the Department of Health (DOH) and the Department of Environmental Conservation (DEC) to address our concerns regarding incident reporting requirements. The clarification and streamlining of reporting obligations is helpful and will make compliance more manageable for local governments throughout the State.

More generally, reporting and compliance timelines should continue to recognize the operational realities and diversity of our systems. Smaller municipalities may rely on outside IT providers or

consultants who are not immediately available when an issue arises. Where appropriate, the State should consider flexible or tiered compliance approaches based on system size and available technical capacity while maintaining appropriate protections for public health and safety.

Local governments are also already subject to statewide cybersecurity obligations through DHSES, and municipalities that operate both water and wastewater systems are subject to overlapping requirements from DOH and DEC. We therefore encourage continued coordination among the agencies to align training, reporting, and compliance mechanisms wherever possible. Improved communication among State agencies and, where feasible, a unified approach to submitting required information would reduce duplication, clarify responsibility, and allow municipal staff to devote more resources to improving actual system security.

#### **4. Phased Implementation**

A phased approach would help balance public health, environmental, and safety objectives with the operational realities facing local governments. Larger systems with greater staffing and technical capacity may be able to implement more advanced requirements sooner, while smaller systems could be provided with additional time and technical support to comply.

Phased implementation would also recognize the significant initial expenses associated with establishing cybersecurity programs and allow municipality to plan for these costs through their normal budgeting and capital planning processes. This approach would avoid placing undue burdens on smaller systems while continuing to advance statewide cybersecurity protections.

#### **Conclusion**

Local governments are essential partners in protecting public health, environmental quality, and critical water and wastewater infrastructure. They own and operate the majority of these systems in New York State and bring critical first-hand experience to the implementation of cybersecurity requirements. Our associations and members share the State's commitment to strengthening cybersecurity and emergency preparedness for critical infrastructure and stand ready to collaborate in building stronger, more resilient systems

Meaningful success, however, will require more than technical requirements alone. Cities, villages, and towns need a practical framework that recognizes differences in size, staffing, technical capacity, and available resources. We appreciate the Legislature's efforts to address concerns related to the implementation and impact of the current cybersecurity requirements for the State's water and wastewater systems and encourage continued collaboration among the Legislature, State agencies, and local governments.

We urge the State to provide adequate funding and technical assistance, support accessible cybersecurity training and guidance, coordinate reporting requirements across agencies, and allow sufficient flexibility and time for implementation. These steps will help ensure that statewide requirements strengthen cybersecurity while remaining technically appropriate, fiscally responsible, and achievable for communities of all sizes.