Public Hearing on Water Security and Preparedness

Comments submitted by the
New York State Association of Counties
to the New York State Senate Standing Committees on
Local Government, Cities 1, and Cities 2

September 25, 2026

Chair Martinez, Chair Bottcher, Chair Ryan, and distinguished members of the Committees:

On behalf of the New York State Association of Counties (NYSAC), thank you for the opportunity to submit testimony on the cybersecurity threats facing New York's water and wastewater infrastructure and the resources and coordination counties need to meet them. NYSAC is a bipartisan association representing New York's 62 counties, including the City of New York.

Counties are central to this issue in three ways. First, counties operate and maintain many of the publicly owned treatment works (POTWs) and drinking water systems across New York. Second, county health departments carry statutory responsibilities for public water system oversight and are increasingly asked to assist water suppliers with cybersecurity planning. Third, county governments are themselves among the most frequent targets of cyberattacks in the state, operating interconnected information technology and operational technology environments in which a water system is one node among many. Whatever the ownership structure of a given system, the fiscal and public-health consequences of a successful attack land on county governments and the residents they serve.

The Cyber Threat to Water Infrastructure Is Real and Immediate

These are not hypothetical risks. In September 2022, Suffolk County's systems were compromised in a ransomware attack that forced the county to shut down much of its digital infrastructure while working to maintain continuity of services. In October 2020, days before early voting, Chenango County discovered its data had been encrypted and

held for ransom, and its IT staff worked for roughly three months to rebuild the network. More recently, the Federal Bureau of Investigation reported in July 2026 that cyberattacks had affected water systems in at least seven states, with operational technology disrupted at several facilities. New York's water and wastewater systems face the same threat environment.

Counties understand what is at stake because of their operational and oversight roles. A disruption to a water or wastewater system is not only an information-technology problem; it is a public-health and environmental emergency that county emergency management, health, and public works staff must manage in real time.

Counties Support New York's Nation-Leading Standards—and Ask the State to Make Them Achievable

NYSAC supported the State's decision to establish first-in-the-nation cybersecurity standards for drinking water and wastewater systems, and we appreciate the coordinated, whole-of-government approach the Department of Environmental Conservation (DEC), Department of Health (DOH), Environmental Facilities Corporation (EFC), and Division of Homeland Security and Emergency Services (DHSES) have taken to align those standards and reduce duplication. We also appreciate the State's investment in the Strengthening Essential Cybersecurity for Utilities and Resiliency Enhancements (SECURE) grant program and the no-cost technical assistance available through EFC's Community Assistance Teams.

As these standards move into implementation, our members have identified five priorities that will determine whether they succeed in practice.

1. Sustained, dedicated funding—not one-time grants. The SECURE program is a meaningful start. Its initial $2.5 million appropriation, followed by roughly $9 million awarded in 2026 to more than 150 local government projects, has begun to move resources to the communities that need them. But the scale of the need is far larger: New York has more than 7,000 public water systems, and SECURE is a competitive program built primarily for one-time assessments and upgrades. It does not address the recurring costs these standards create—annual monitoring, maintenance, attestations, and staff time—that counties must absorb year after year.

These pressures fall hardest on smaller and rural systems, which compete for the same limited grant dollars while operating under the property tax cap and constrained local revenues. New compliance costs on public water suppliers are ultimately passed on to ratepayers, straining affordability for residents already facing rising costs. We respectfully urge the Legislature to pair these requirements with sustained, dedicated funding: a recurring appropriation rather than a single-year program, expanded and renewed SECURE funding, and need-based direct assistance weighted toward small and rural systems.

2. Coordination and alignment across state agencies. Counties are already subject to overlapping cybersecurity obligations from multiple state entities, including DHSES, and county water and wastewater systems now face additional requirements from DEC and DOH. Municipalities that operate both water and wastewater systems can face stacked and sometimes inconsistent requirements from three or more agencies. As one concrete example, DOH's cybersecurity regulations for drinking water systems require one hour of cybersecurity training every three years; even if that training is intended to be water-specific and to supplement—rather than replace—the annual cybersecurity training already required of municipal employees under recently enacted law, it still leaves operators managing two different training standards for the same workforce. We ask the Legislature to direct the relevant agencies to align training, reporting, and attestation requirements and to move toward a single, coordinated reporting pathway, so that limited local resources go to actual security improvements rather than duplicative paperwork.

Similarly, incident-notification requirements should be coordinated so that water and wastewater operators, local government IT and cybersecurity personnel, emergency management, public health officials, and appropriate State agencies and security operations resources understand when and how potentially consequential cyber incidents are to be reported and coordinated.

3. Workforce and technical expertise. Cybersecurity is a specialized field, and most small systems have no in-house IT or cybersecurity staff. We appreciate that the State has recognized this capacity gap: in its adopted cybersecurity regulations for drinking water systems, DOH provided that statewide oversight, implementation of the new requirements, and technical assistance will be handled by the Department's Albany office, reducing the burden on local health departments that likewise lack in-house cybersecurity expertise. That centralized, state-provided model is the right approach, and it should be fully resourced, sustained, and—where possible—extended across the water and wastewater sectors, including through EFC's Community Assistance Teams, DHSES, and the Office of Information Technology Services. Small systems also need model policies, template plans, and regional or shared-services options so that they are not left to build these capabilities on their own.

These support models should also preserve clear lines of responsibility. The regulated entity and system owner should remain accountable for its regulatory and programmatic obligations; the provision of network connectivity, cybersecurity services, technical assistance, or incident-response support by a county or municipal IT department should not, by itself, transfer those obligations to the IT organization.

The county cybersecurity professionals we represent generally support strong, rigorous standards. Some have advocated for more frequent training and more robust requirements, not fewer. The concern our members raise is not the substance of the

standards but the capacity and funding to meet them. Robust standards and adequate support must advance together.

4. Tiered timelines and phased implementation. Reporting and compliance timelines that are workable for large systems with dedicated IT staff and real-time monitoring can be genuinely difficult for small systems that have neither. A tiered approach—phasing advanced requirements in first for larger systems while giving smaller systems additional time and technical support—would allow steady statewide progress without imposing unrealistic burdens on the communities least equipped to absorb them.

5. Resilience beyond the water system. Finally, we encourage the Legislature to view water cybersecurity as one part of a broader local government cyber-resilience picture. Water and wastewater operational technology does not exist in a cybersecurity vacuum. Even where operational technology is appropriately segmented from enterprise IT, these environments may share dependencies involving communications infrastructure, identity and access management, vendors, remote-access pathways, and incident-response resources. Protecting critical water infrastructure, therefore, requires attention both to the security of the operational environment itself and to the systems and services upon which it depends.

Continued state support for the DHSES Cyber Incident Response Team, for shared threat-intelligence resources, and for incident-response planning and exercises benefits water systems and every other essential service a county provides. As federal cybersecurity funding for state and local governments has been time-limited and its future uncertain, a sustained state commitment is increasingly important. State standards and technical assistance should also address third-party and vendor access to operational technology, including secure remote access, authentication, logging, timely termination of access, incident notification, and clear allocation of cybersecurity responsibilities between system owners and their contractors.

Safe Drinking Water Also Depends on Resources for PFAS and Emerging Contaminants

This hearing concerns water security and preparedness. Cybersecurity is the immediate focus, and rightly so—but counties face a second, ongoing challenge to safe drinking water: the presence of PFAS and other emerging contaminants. We raise it here because it impacts the same systems, the same budgets, and the same residents. Counties strongly support health-protective standards for these contaminants, and New York's counties have been active partners in the State's nation-leading work to address them.

Our central concern is the one that runs throughout this testimony: cost. Testing, treatment, and remediation for these contaminants are enormously expensive, and those costs fall largely on counties, municipal water systems, and ratepayers that did not

manufacture or release these chemicals. When a county or a household must pay to remove contamination it did nothing to create, the burden is both substantial and misplaced.

For that reason, counties urge the State to keep advancing source control and producer responsibility. The most durable and cost-effective way to protect drinking water is to keep these chemicals out of the environment in the first place and to ensure that the manufacturers responsible for them—not local taxpayers and ratepayers—bear the primary cost of the contamination they produce.

At the same time, counties appreciate the significant investments the State has already made, including grants and financing through the Environmental Facilities Corporation and the new private-well PFAS testing and mitigation pilot. These are meaningful commitments. As with cybersecurity, however, they are a strong start against a far larger and recurring need. We respectfully urge the Legislature to provide sustained, dedicated funding and continued cost-sharing for contaminant treatment and remediation, weighted toward the small and rural systems least able to absorb these costs on their own.

Counties also need regulatory certainty. Federal drinking water standards for PFAS are in flux: in 2026, the U.S. Environmental Protection Agency proposed to maintain its limits for PFOA and PFOS while extending the compliance deadline to 2031 and to rescind its limits for several other PFAS—proposals that remain pending. New York, meanwhile, maintains its own standards. County systems are being asked to make multi-year, capital-intensive treatment decisions against a shifting federal target layered over state requirements. A stable compliance picture would let counties plan and invest wisely rather than build to a standard that changes midstream.

Finally, the capacity gap described earlier applies here, as well. Small and rural systems often lack the staff and technical expertise to design, finance, and operate advanced treatment. Continued technical assistance and realistic, phased timelines are as important for contaminant compliance as they are for cybersecurity. County health departments, which carry the oversight role for public water systems, will likewise need dedicated funding and technical expertise to keep pace with each new contaminant standard and to help smaller suppliers achieve compliance.

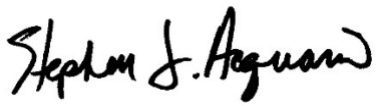
Conclusion

Counties share the State's goal of protecting the water and wastewater systems that millions of New Yorkers depend on—both from cyber threats and from the contaminants that affect the safety of drinking water. We operate these systems, we respond when something goes wrong, and we bring practical, first-hand expertise to this work. Meeting the moment will take partnership: sustained funding, coordinated requirements, investment in workforce and technical assistance, and protection for the

ratepayers and taxpayers who ultimately bear these costs. NYSAC and our members stand ready to work with the Legislature and state agencies to build water systems that are safe, secure, resilient, and affordable for communities of every size.

Thank you for the opportunity to submit testimony.

Respectfully submitted,



Stephen J. Acquario
Executive Director