

Testimony of
Alexander J. Smith, PhD
Deputy Commissioner for Water Resources
New York State Department of Environmental Conservation

SENATE STANDING COMMITTEE ON LOCAL GOVERNMENT, SENATE STANDING
COMMITTEE ON CITIES 1, and SENATE STANDING COMMITTEE ON CITIES 2 hearing on:
*Examining the Implementation, Fiscal Impact, and Technical Sufficiency of Mandatory State Water
Security and Wastewater Security Regulations*

October 1, 2026

Introduction

The water and wastewater sector is a **lifeline critical infrastructure** sector that, according to the federal Cybersecurity and Infrastructure Security Agency (CISA) is “so vital that [its] incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof.”¹ As providers of essential public services that may sometimes lack rigorous cybersecurity resources and protections, water and wastewater systems are highly attractive targets for malicious cyber actors seeking to disrupt operations and spread fear.² These threat actors include nation-state-affiliated groups seeking to target U.S. critical infrastructure, especially during periods of increased geopolitical tension.³

Over the last several years, there have been numerous documented cybersecurity incidents at water and wastewater systems across the country, including high-profile attacks on programmable logic controllers and other operational control systems in multiple states.⁴ More recently, this summer, CISA confirmed that over one-hundred internet-exposed operational control systems in the U.S. water and wastewater sector were targeted by cyber threat actors; some of these attacks led to operational disruptions.⁵ The threat actors behind those attacks are targeting water entities of all sizes, meaning the problem is not limited to large or high-profile systems.⁶

Fortunately, New York State has already taken action to address these risks. At Governor Hochul’s direction, in June 2024, the New York State Chief Cyber Officer convened experts from nine State

¹ The term “critical infrastructure” is defined in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)). CISA commonly refers to the four lifeline critical infrastructure sectors as (1) Communications; (2) Energy; (3) Transportation; and (4) Water and Wastewater (see <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems>).

² See [epa-apnsa-letter-to-governors_03182024.pdf](#) and [EPA, FBI, CISA, NSA Issue Joint Cybersecurity Advisory to Water System Regarding Iranian-Affiliated Cyber Attacks | US EPA](#).

³ Federal agencies frequently identify China, Russia, Iran, and North Korea among the nation-state threats targeting U.S. critical infrastructure. See [Nation-State Threats | Cybersecurity and Infrastructure Security Agency CISA](#).

⁴ See [GAO-24-106744, Accessible Version, CRITICAL INFRASTRUCTURE PROTECTION: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems](#).

⁵ To DEC’s knowledge, none of the summer 2026 attacks took place in New York. News reports varied in the number of states identified as affected by the incidents. Although the FBI initially reported at least seven (7) states impacted, later news reports indicated that the number may have eventually climbed to at least a dozen states, See: [Internet Exposure Reduction Guidance | CISA](#) and [At least 12 states face cyberattacks on their water systems, sources say - ABC News](#). Since the new mandated cybersecurity incident reporting requirement went into effect on March 11, 2026, no cybersecurity incidents have been reported to DEC.

⁶ See <https://www.cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs>.

agencies⁷ to examine and recommend actions to build the water and wastewater sector’s cybersecurity resilience and reliability. This multi-agency working group came together to discuss risks and solutions for protecting New York’s critical water and wastewater infrastructure. Ultimately, the working group’s efforts helped inform a multi-pronged, whole-of-state approach to strengthening the cybersecurity of New York’s water infrastructure. In January of 2025, Governor Hochul announced a State of the State Initiative to [Safeguard New York’s Water Infrastructure](#) through the establishment of a new grant program and the development of new minimum cybersecurity standards for water and wastewater utilities.

The Department of Environmental Conservation (DEC) promptly began drafting cybersecurity regulations for wastewater utilities, while the Department of Public Service (DPS) and the Department of Health (DOH) began drafting regulations for drinking water utilities. Throughout the regulatory development process, DEC worked closely with state partners at the Division of Homeland Security and Emergency Services (DHSES), Department of Health (DOH), DPS, the Environmental Facilities Corporation (EFC), the New York State Police (NYSP), and the office of the Chief Cyber Officer of the New York State Executive Chamber. More specifically, DEC, DOH, and DPS collaborated throughout the rule development process to harmonize the wording of each agency’s regulatory express terms to the extent that it was reasonably feasible given different legal and regulatory frameworks and given different risks and concerns of the regulated entities. Ultimately, after a public comment period, on March 11, 2026, DEC and DOH adopted [nation-leading minimum standards](#) for wastewater and drinking water systems, respectively, that are threat-informed, risk-centric, and cost-balanced.

Stakeholder Engagement

During the regulatory development process and in advance of issuing its Notice of Proposed Rule Making (NPR), DEC conducted stakeholder outreach. From March-May of 2025, DEC met with representatives of various wastewater systems, municipalities, and wastewater professional associations. In these meetings, DEC provided background on the proposed regulations and a general overview of the anticipated rules and solicited feedback. Most of the feedback on the proposed rules was focused on three concerns: (1) the ability for publicly owned treatment works (POTWs) to tailor their approaches to security controls to their specific facility; (2) the ability for wastewater system employees to understand the new rules and requirements; and (3) how the rules will fare in a rapidly changing cybersecurity landscape.

DEC considered this feedback during rule development and incorporated it into the draft documents issued during the NPR. DEC addressed items (1) and (3) by incorporating cybersecurity documents into the proposed rules by reference.⁸ This allows POTWs to select from a variety of approaches discussed in the documents, allowing them to tailor their cybersecurity systems to their specific facility, but still meeting the overall regulatory goals. In addition, incorporating documents by reference allows DEC to remain flexible; as guidance and recommendations change, DEC can update the referenced documents more efficiently without completely rewriting the text and structure of the rules.

⁷ The New York State Water and Wastewater Reliability and Resilience Working Group (“WWRR group”) originally consisted of Department of Environmental Conservation, Department of Health, Department of Labor, Department of Public Service, Division of Homeland Security and Emergency Services, Environmental Facilities Corporation, New York Power Authority, New York State Police, and State University of New York.

⁸ These documents, incorporated by reference at 6 NYCRR 750-1.25(j) through (o) and 750-2.9(e)(4) include: *EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems*, EPA 817-B-23-001 (August 2024); *Wastewater Utility Emergency Response Plan: Template and Instructions*, EPA 817-B-21 003 (July 2021); *Incident Action Checklist – Cybersecurity*, EPA 810-B-17-004 (February 2021); *Guide to Operational Technology (OT) Security*, NIST SP 800-82r3 (September 2023); *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800 (o) 53 (December 10, 2020); and *Drinking Water and Wastewater Systems Cybersecurity Incident Response Plan Template Instructions* (April 2025).

Finally, to address item (2), DEC chose to require wastewater operators to obtain cybersecurity training pursuant to Part 650 amendments, and DEC maintains a list of clear, actionable, and free cybersecurity documents, resources, and training opportunities on its website. Cybersecurity trainings and resources assist wastewater system employees in understanding the new rules and requirements. To date, DEC has provided fourteen direct trainings for operators and other stakeholders to explain the new cybersecurity regulations. Additionally, future training opportunities will be communicated through *DEC Delivers* and posted on the Wastewater Cybersecurity Resources webpage. (See “[Implementation: Education, Outreach, and Training](#)” section).

The official public comment period⁹ for the cybersecurity and related regulations was open from June 25, 2025, to September 26, 2025. Two public hearings were held on the proposed rulemaking on August 26, 2025 via webinar. No comments were received at the public hearings. Sixty-six written comments for the rule making were received from fifteen entities, primarily representing wastewater and municipal professional associations and municipalities.

DEC published an [Assessment of Public Comments](#) to address each comment on March 11, 2026.

New DEC Regulations—Overview

On March 11, 2026, DEC adopted regulations which amend 6 NYCRR Parts 616, 650, and 750 to safeguard New York’s critical wastewater infrastructure from cyber-attack so New Yorkers will continue to have access to safe and reliable wastewater services.

- Part 616 was amended to add a provision allowing DEC to consider whether a record contains sensitive cybersecurity information when determining whether it can be exempt from disclosure under the Freedom of Information Law (FOIL).
- Part 650 was amended to mandate cybersecurity training for certified wastewater operators.
- Part 750 was amended to require the following: mandatory cybersecurity incident reporting for all SPDES permittees; an Emergency Response Plan (ERP) that includes a cybersecurity Incident Response Plan (IRP) for all POTWs; baseline cybersecurity controls for POTWs; new cybersecurity-related definitions; incorporation by reference of documents containing cybersecurity guidance and recommendations; and annual certifications of compliance.

⁹ The Notice of Proposed Rule Making announcing the public comment period was published in the Environmental Notice Bulletin on June 25, 2025. See [Statewide - Notice of Proposed Rule Making - 6 NYCRR Parts 616, 650, and 750 Wastewater Cybersecurity and Related Regulations - NYSDEC](#). In addition, on June 25, 2025, DEC sent courtesy notices to the following organizations to inform them of the Notice of Public Rule Making and the public comment period: the New York Conference of Mayors (NYCOM), the New York State Association of Counties (NYSAC), and the New York Association of Towns (NYAOT), the New York Section of the American Water Works Association (NY AWWA), the New York Water Environment Association (NYWEA), and the New York Rural Water Association (NYRWA). On July 1, 2025, DEC also published an electronic bulletin to *DEC Delivers* to inform subscribers to the Wastewater Cybersecurity topic about the Notice of Public Rule Making and the public comment period.

The following chart lists the applicability and effective dates for the requirements in Part 750.

Summary of Applicability and Effective Dates Requirement	Applicability	Effective Date
Mandatory Cybersecurity Incident Reporting	All SPDES Permittees (publicly owned and privately owned)	March 26, 2026
Cybersecurity Training	NYS-certified Wastewater Operators	All certificates that expire on or after January 1, 2027
ERP with Cybersecurity IRP incorporated	All POTWs	March 11, 2027
Written rules and/or procedures for access control and authentication	All POTWs	March 11, 2027
Written cybersecurity vulnerability management process (including cyber asset inventory)	All POTWs	March 11, 2027
Written documentation of secure network structure	All POTWs	March 11, 2027
Network Monitoring and Logging	POTWs with a design flow of greater than or equal to 10 million gallons per day (MGD)	March 11, 2027
Two Annual Certifications (one for ERP and one for all cyber controls)	Principal executive officer or ranking elected official of any municipality that is the LPR for a POTW, or an executive level municipal official that is a duly authorized representative.	March 28, 2027

New DEC Regulations—Detail

6 NYCRR Part 616 – Access to Records

6 NYCRR 616.7(c)(2)(i) through (vii) previously contained seven factors that DEC may consider in making a determination to grant or continue an exception from disclosure under the Public Officers Law (POL). The amendment under 6 NYCRR 616.7(c)(2)(viii) adds an eighth factor, related to cybersecurity information or information related to technology network vulnerabilities and data privacy risks, that DEC may consider in making a determination to grant or continue an exception from disclosure under the POL. This allows DEC to protect sensitive information related to a cybersecurity incident at a critical infrastructure facility from public disclosure. This change became effective as of March 26, 2026.

6 NYCRR Part 650 – Qualifications of Operators of Wastewater Treatment Plants

6 NYCRR 650.8 and 650.12 require that wastewater treatment plant operators, certified in accordance with Part 650, complete a minimum number of training hours on the topic of cybersecurity to renew their

certification every five years. This change does not add to the overall required hours, but instead requires operators to complete cybersecurity training within their existing required hours. Grades 1/1A and 2/2A operators are required to complete 2 hours, while Grades 3/3A and 4/4A operators are required to complete 4 hours of cybersecurity training every five years. This new requirement is effective for all wastewater operator certifications that expire on or after January 1, 2027.

6 NYCRR Part 750 – State Pollutant Discharge Elimination System (SPDES) Permits

Part 750 contains new cybersecurity control requirements. The following requirements, which are all effective as of March 11, 2027, were added to Part 750:

- 1) **750-2.7(h): All SPDES permittees**, including both publicly and privately owned facilities, must report cybersecurity incidents to DEC within 24 hours of becoming aware of the incident. (There is a publicly available online incident reporting portal where permittees can report to DEC, DOH, and DHSES simultaneously to streamline required reporting; the agencies collaborated to create this combined reporting portal as a direct result of public comments. After submitting an online report within 24 hours, permittees then call DEC dispatch, which is available 24x7, to confirm they submitted an online report; this avoids a single point of failure in the reporting structure and satisfies the oral reporting component of the regulation. 750-2.7(h) also requires that permittees provide a 30-day follow-up report, which is also submitted using the online portal.
- 2) **750-2.9(d): All POTWs** must establish, maintain, and implement a written ERP. A United States Environmental Protection Agency (EPA) ERP template was incorporated into the regulation by reference. POTWs are allowed to use any plans that exist prior to March 11, 2027, as long as they meet certain minimum requirements.¹⁰
- 3) **750-2.9(e)(3): All POTWs** must establish, maintain, and implement a written cybersecurity IRP. An EPA IRP checklist and template were incorporated into the regulation by reference. POTWs must incorporate the cybersecurity IRP into the overall ERP.
- 4) **750-2.9(e)(1)(i): All POTWs** must establish, maintain, and implement written rules and/or procedures for access control and authentication for access to operational technology (OT), SPDES program data, information technology (IT) that may indirectly or directly allow access to OT, and the ERP. These written rules and/or procedures must be consistent with the principle of least privilege; address password security, complexity, and management; require multi-factor authentication for remote access to OT; and disallow use of preset or default credentials. In addition, the POTW must review the written rules and/or procedures annually by March 28th and must update the rules and/or procedures within 90 days after a cybersecurity incident, cybersecurity assessment or audit.
- 5) **750-2.9(e)(1)(ii): All POTWs** must establish, maintain, and implement a written vulnerability management process. The written process must include a cyber asset inventory and must identify which assets can be accessed remotely. The POTW must identify known cybersecurity vulnerabilities for assets included within the cyber asset inventory and must undertake a risk assessment, based on the likelihood that the vulnerability will be exploited and the consequences to the POTW's normal operations that could occur if the vulnerability were exploited. Next, the POTW must prioritize the cybersecurity vulnerabilities according to the risks identified and mitigate and/or remediate these vulnerabilities according to their priority. The POTW must review the written vulnerability management process annually by March 28th and must update the process when assets are added or decommissioned or when a new vulnerability is identified.
- 6) **750-2.9(e)(1)(iii): All POTWs** must establish, maintain, and implement a written description of network structure that protects OT by physically and logically separating it from IT and external networks; or by securing necessary connections by using appropriate cybersecurity controls (i.e., controls that are discussed within the cybersecurity documents incorporated into the regulation by reference).

¹⁰ They must describe the POTW's strategies, resources, plans, and procedures to prepare for, and respond to, a natural or human-made incident, that threatens health, safety, property, or the environment and include up-to-date includes titles and contact information for persons with responsibilities in the ERP.

- 7) **750-2.9(e)(2): All POTWs with a design flow greater than or equal to 10MGD** must implement, manage, and maintain, or cause to be implemented, managed, and maintained, procedures, products, and/or services that monitor and log the POTW's network activity. There are two exceptions to this requirement; one for POTWs that have no connection between OT and IT or external networks and one for POTWs where the only connection between OT and IT or external networks is unidirectional (i.e., the OT can send data but cannot receive data).
- 8) **750-2.9(e)(5): All municipalities that are legally responsible parties (LRPs) for a POTW** must certify annually, by March 28, that the municipality is complying with the cybersecurity controls in section 750-2.9(e)(1) through (3). This certification must be made by the principal executive officer or ranking elected official or, upon written notice to DEC, by a duly authorized representative who is an executive-level municipal official having responsibility for oversight of information technology, operational technology, or cybersecurity functions.

Fiscal Impact on Local Governments

The new rules under Part 750 may impose costs on local governments. Municipalities are often the LRPs for POTWs, so they will ultimately be responsible for ensuring that POTWs comply with the cyber controls set forth in the new rules.

Costs will vary widely depending on the size of the POTW, its network structure, the number of critical OT and physically or logically connected IT assets, the number of employees, users, and devices, the degree to which cybersecurity controls are already in place, and the way the POTW chooses to comply with the requirements. Furthermore, the extent to which municipalities and POTWs share network and IT resources varies significantly, resulting in varying compliance costs. Pages 41-47 of the [Revised Regulatory Impact Statement](#) (RIS) address costs in detail. As the RIS explains, low and no-cost resources are available to meet some of the new requirements.

It is also important to note that the benefits may outweigh the costs of implementing cybersecurity controls in the event there is a successful attempt to access wastewater system infrastructure, particularly if that successful attempt includes a demand for ransom. Although the costs of a cybersecurity incident vary and can be very hard to estimate, according to IBM, the cost of a single public sector data breach can be as high as \$2.6M.¹¹ That estimate does not include the cost of potential environmental impacts should a cybersecurity incident lead to an operational disruption.

To support implementation, DEC compiled numerous free resources and templates on the [Wastewater Cybersecurity Resources](#) webpage. DEC has also invested significant resources in education, outreach, and training to support municipalities and POTWs as they work to implement the new requirements. (See "[Implementation: Education, Outreach, and Training](#)" section below). No-cost technical assistance is also available from EFC.

In addition, to support implementation, on March 11, 2026, Governor Hochul launched the new \$2.5 million Strengthening Essential Cybersecurity for Utilities and Resiliency Enhancements (SECURE) grant program, administered by EFC; in July, the Governor announced an additional \$7 million dollars in funding for this grant. Applications opened on March 11, 2026. Funding included:

- Up to \$50,000 for cybersecurity assessments
- Up to \$100,000 to implement cybersecurity upgrades

¹¹ *Cost of a Data Breach Report*, IBM (2024). <https://www.ibm.com/account/reg/us-en/signup?formid=urx-52913>

On August 3, 2026, Governor Hochul announced that more than \$9 million in SECURE grants were awarded to 153 local government projects statewide.

Implementation: Education, Outreach, and Training

DEC's Wastewater Cybersecurity Team ("WCT") has undertaken extensive outreach to inform the regulated community and other stakeholders about the new cybersecurity regulations and the free resources available to support implementation and compliance. Outreach efforts have included:

- A mass paper mailing (mid-March 2026) to the LRPs of all 633 POTWs in New York State. This mailing contained detailed information on the newly adopted cybersecurity regulations and a one-page flyer entitled "*How to Report a Wastewater Cybersecurity Incident to NYS DEC.*" This paper mailing was followed by a mass email notification to over 2,500 POTW email contacts.
- Communication via *DEC Delivers*, DEC's GovDelivery-based electronic communications system, to provide subscribers with timely wastewater cybersecurity information and updates. Since July 2025, DEC has distributed forty-two (42) e-bulletins covering regulatory updates, cybersecurity advisories and emerging threats, DEC-approved cybersecurity training opportunities, and other relevant resources and announcements.
- Development of DEC's [Wastewater Cybersecurity Resources](#) webpage, which serves as a centralized hub for information on the new regulations, incident reporting requirements, free cybersecurity assessments and services, compliance guidance, DEC-approved training opportunities, and other state and federal resources to help wastewater facilities strengthen their cybersecurity and resilience. Throughout the year, the webpage has been updated seventeen (17) times to ensure it continues to provide the most current information, guidance, and available resources.
- Development and maintenance of DEC's [Cybersecurity Incident Reporting](#) webpage and online reporting portal, which provides SPDES permittees with instructions, requirements and access to online forms for streamlined reporting cybersecurity incidents to DEC, DOH, and DHSES.
- Fourteen public presentations and trainings, reaching more than 1,200 stakeholders across the state since rule adoption.
- Continued collaboration with our colleagues at NYS AWWA, NYWEA, and NYRWA to provide outreach, education, and training to wastewater professionals across the state. These important relationships help ensure DEC reaches a wide audience and stays abreast of the latest issues and concerns within the wastewater community.

In addition to DEC-provided outreach and trainings, since January 1, 2026, 460 DEC-certified operators have completed over 648 hours of DEC-approved cybersecurity trainings offered by the EPA.

Finally, DEC added new cybersecurity components to the DEC/EFC Asset Management Program for POTWs, which is in Phase 2 of a multi-year pilot. These new components include a comprehensive cyber asset inventory and a cybersecurity assessment. The experiences shared by the municipalities participating in the latest phase of the pilot program will help inform DEC's guidance going forward.

Collectively, these extensive and sustained outreach efforts have provided the regulated community with multiple opportunities to understand the new cybersecurity requirements, stay informed of important

updates, and access the guidance, training, and free resources available to support successful implementation as the March 2027 compliance deadlines approach.