SUMMARY OF EXPRESS TERMS

In Governor Hochul's 2025 State of the State, she directed the Department of Health (Department) to establish enforceable cybersecurity requirements to protect public water systems that serve the people of New York. The Department developed this regulatory proposal based on the authorities granted in Public Health Law §§ 225 and 1125 to establish risk-based regulations for community water systems that serve more than 3,300 people. This regulatory proposal establishes a new Appendix 5-E to Subpart 5-1 of Title 10 of the New York Codes Rules and Regulations (NYCRR).

Section 5-E.1 establishes that the cybersecurity requirements apply to community water systems that serve more than 3,300 people and for some requirements, only to systems that serve more than 50,000 people.

Section 5-E.2 establishes risk-based exclusions to the regulatory requirements.

Section 5-E.3 establishes definitions for specific technical requirements for this appendix.

Section 5-E.4 establishes that covered water systems that serve more than 50,000 people shall identify an individual who is deemed qualified by the covered water system's owner to be responsible for the covered water system's cybersecurity program.

Section 5-E.5 establishes requirements for cybersecurity vulnerability analysis. This section requires that covered water systems assess the vulnerability to cybersecurity incidents of all operational technology and nonpublic information that impacts or limits a covered water system's ability to comply with the requirements of this Subpart or that may pose a risk to public health.

Section 5-E.6 establishes baseline requirements for a cybersecurity program. The cybersecurity program must be designed to fulfill statutory and regulatory reporting obligations;

provide authentication and access management; maintain a cyber asset inventory; implement defensive architecture to protect operational technology and nonpublic information from unauthorized disclosure, alteration, or destruction; identify and assess risk for operational technology and nonpublic information handling; monitor and log network activity for covered water systems that serve more than 50,000 people; implement response protocols for breach incidents; and recover from cybersecurity incidents.

Section 5-E.7 establishes that all water operators regulated under Subpart 5-4 shall take a minimum of one hour of cybersecurity training every 3 years.

Section 5-E.8 requires covered water systems to incorporate a cybersecurity incident response plan into its water system emergency plan.

Section 5-E.9 requires covered water systems to report cybersecurity incidents to the Department within 24 hours which have created, or may create, a public health hazard.

Sections 5-E.10 and 5-E.11 address confidentiality and severability, respectively.

Pursuant to the authority vested in the Public Health and Health Planning Council and the Commissioner of Health by sections 225 and 1125 of the Public Health Law, a new Appendix 5-E is added to section 5-1 of Title 10 of the Official Compilation of Codes, Rules and Regulations of the State of New York (NYCRR), to be effective upon publication of a Notice of Adoption in the New York State Register, to read as follows:

Appendix 5-E: Cybersecurity Requirements for Public Water Systems

Section 5-E.1 Applicability.

(a) Applicability. This Appendix, except for section 5-E.4 and paragraph 5.E-6(c)(6), shall apply to all community water systems which serve populations greater than 3,300 people, as defined by subdivisions 5-1.1(bj) and (az) of this Subpart referred to throughout this Appendix as "covered water system." Section 5-E.4 and paragraph 5.E-6(c)(6) shall only apply to covered water systems that serve a combined wholesale and retail population of greater than 50,000. Section 5-E.7 shall apply to all drinking water operators certified in accordance with Subpart 5-4 of this Part and is not subject to the exclusions identified in Section 5-E.2.

(b) Covered water systems shall have until January 1, 2027, to comply with the requirements of this Appendix, provided that sections 5-E.7 and 5-E.9 of this Appendix shall be effective immediately upon adoption.

(c) All covered water systems shall:

(1) Prepare and submit a cybersecurity vulnerability analysis (CVA) in accordance with subdivision 5-1.33(c) of this subpart that incorporates the requirements of section 5-E.5 of this Appendix. The cybersecurity vulnerability analysis must be reviewed and updated annually.

(2) Report all vulnerabilities identified in the CVA that may impact a covered water system's ability to comply with the requirements of this Subpart or any situation that may pose a risk to public health to the department within 48 hours of identification in accordance with section 5-1.77 of this Subpart.

(d) Non-compliance with any requirement of subdivision (c) shall be considered a significant deficiency as defined in subdivision 5-1.1(cn) of this Subpart. Significant deficiencies shall be corrected within 120 days in accordance with subdivisions 5-1.71(c) and 5-1.71(d) of this Subpart.

Section 5-E.2 Exclusions.

(a) A covered water system is not required to meet the provisions of this Appendix, except for section 5-E.8 and section 5-E.9, if it has neither physical nor logical connections between operational technology and information technology or external networks.

(b) Billing systems operated and managed by a municipal corporation defined in section 2 of the General Municipal Law that do not affect a covered water system's ability to comply with the requirements of this Subpart are exempt from the requirements of this Appendix.

(c) Information technology that does not affect a covered water system's ability to comply with the requirements of this Subpart is exempt from the requirements of this Appendix.

Section 5-E.3 Definitions.

For the purposes of this Appendix the following terms shall have the indicated meaning:

(a) "Control" means any mechanism, safeguard, policy or security measure that is put in place pursuant to an implementation specification to satisfy the requirement for a security measure.

(b) “Compensating control” means any alternative measure that is put in place to satisfy the requirement for a security measure.

(c) “Cyber asset inventory” means an inventory of:

(1) operational technology assets that are reachable or accessible by a management, control, or communications protocol; and

(2) information technology assets that are physically or logically connected to operational technology.

(d) “Cybersecurity event” means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse a covered water system’s operational technology.

(e) “Cybersecurity incident” means a cybersecurity event or attack that, directly or indirectly:

(1) has an adverse impact on any operations of the covered water system that affect the ability of the covered water system to comply with the requirements of this Subpart; or

(2) has a reasonable likelihood of compromising any operations of the covered water system or any of its components; or

(3) actually or imminently jeopardizes the confidentiality, integrity, or availability of nonpublic information related to the covered water system, or results in loss or damage to the covered water system’s normal operations.

(f) “Cybersecurity vulnerability analysis” or “CVA” means the analysis of vulnerability to cyber attack that each covered water system shall conduct in accordance with Public Health Law section 1125(2)(k) and subdivision 5-1.33(c) of this Subpart.

(g) “Department” means the New York State Department of Health.

(h) “Information technology” means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of

electronic information, provided that information technology does not include operational technology.

(i) “Multi-factor authentication” means user identity authentication that requires a user to provide at least two of the following distinct factors for successful authentication:

(1) something the user knows; or

(2) something the user has; or

(3) something the user is.

(j) “Nonpublic information” means all electronic information that is not publicly available information and is:

(1) a covered water system’s business-related information, where compromise to its confidentiality, integrity, or availability would impact that system’s ability to comply with the requirements of this Subpart; or

(2) information determined by the covered water system to pose a security risk to the operation of the water system in accordance with subdivision 5-1.33(h) of this Subpart.

(k) “Operational technology” means hardware, software, and firmware that detect or cause changes in physical processes through the direct control and monitoring of industrial equipment, assets, processes, and events in the covered water system.

(l) “Principle of least privilege” means a security principle that restricts the access privileges of users, or processes acting on behalf of users, to the minimum necessary to accomplish assigned tasks.

(m) “User” means any employee, contractor, agent or other person that operates a covered water system and is authorized to access and use any operational technology and data of such covered water system.

Section 5-E.4 Cybersecurity personnel

(a) Each covered water system serving a combined wholesale and retail population of greater than 50,000 shall designate an individual who is deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management who shall be the individual responsible for the covered water system's cybersecurity program.

(1) The name and contact information for the individual responsible for the covered water system's cybersecurity program identified in subdivision (a) of this section shall be included in the water supply emergency plan of the covered water system, in accordance with paragraph 5-1.33(b)(6) of this Subpart.

(2) The individual responsible for the covered water system's cybersecurity program shall make a confidential report in writing at least annually to the system's governing body on the system's cybersecurity program and material cybersecurity risks. For the purposes of this Appendix, a covered water system's governing body may be the board of supervisors, board of trustees or council of a municipality as defined in General Municipal Law; a board of directors of an investor-owned utility regulated under the Public Service Law; or a governing body of a utility authorized under Article 5 of Public Authorities Law.

Section 5-E.5 Cybersecurity vulnerability analysis.

(a) All covered water systems shall conduct a CVA to meet the requirements for an analysis of vulnerability to cyber attack in accordance with subdivision 5-1.33(c) of this Subpart. The covered water system shall incorporate the findings of the CVA into the water system emergency plan submitted to the State in accordance with subdivision 5-1.33(e) of this Subpart.

(b) The CVA shall be approved by an authorized representative of the covered water system. For covered water systems serving a combined wholesale and retail population of greater than 50,000, the CVA shall be approved by the individual responsible for the covered water system's cybersecurity program.

(c) The CVA shall assess risks of known cybersecurity vulnerabilities to cybersecurity incidents of all information technology, operational technology, and nonpublic information that may impact a covered water system's ability to comply with the requirements of this Subpart. The assessment shall be based on the likelihood that the vulnerability will be exploited and the consequences to the covered water system's normal operations that may occur if the vulnerability is exploited.

(d) The CVA shall evaluate the effectiveness of all controls associated with the source or sources of supply, water treatment plants, disinfection stations, pipes and valves, storage tanks, and system operations management to ensure the covered water system can comply with the requirements of this Subpart during a water supply emergency caused by a cybersecurity incident.

(e) Vulnerabilities identified in the CVA that may impact a covered water system's ability to comply with the requirements of this Subpart, or any situation that may pose a risk to public health, shall be reported to the department within 48 hours of identification in accordance with section 5-1.77 of this Subpart.

(f) The CVA shall be reviewed and updated at least annually to respond to technological developments and evolving threats; such a review shall be performed within 30 days after major water facility infrastructure changes are made operational.

(g) The CVA shall identify the actions needed to mitigate or remediate identified vulnerabilities.

(h) The CVA shall follow a form approved by the department.

Section 5-E.6 Cybersecurity program requirements.

(a) Each covered water system shall establish a cybersecurity program based on the findings of the covered water system's CVA.

(b) For covered water systems that serve a combined wholesale and retail population of greater than 50,000, the individual responsible for the covered water system's cybersecurity program, designated in accordance with section 5-E.4(a) of this Appendix, shall submit, as part of the water system emergency plan submission to the department required by 5-1.33(e) of this Subpart, a certification that the covered water system's cybersecurity program complies with the requirements of subdivision (c) of this section. The certification shall follow a form approved by the department.

(c) The cybersecurity program shall be designed to perform the following functions:

(1) Fulfill applicable statutory and regulatory reporting obligations.

(2) Address identity and access management protocols:

(i) Multi-factor authentication shall be required for any individual accessing the covered water system's operational technology from an external network, unless the covered water system's authorized representative, or the individual responsible for the covered water system's cybersecurity program designated in accordance with section 5-E.4 of this Appendix, has approved in writing the use of compensating controls.

(ii) Each covered water system shall limit user access privileges for operational technology and nonpublic information to those necessary to perform each user's assigned tasks.

(iii) Each covered water system shall separate user accounts authorized to access operational technology from user accounts authorized to access information technology.

(iv) Each authorized user shall have unique credentials for accessing operational technology covered by this Appendix whenever unique user credentials can be supported by the operational technology. Operational technology that cannot support unique user credentials shall have compensating controls implemented. For covered water systems that serve a combined wholesale and retail population greater than 50,000, such compensating controls shall be documented in writing by the individual responsible for the covered water system's cybersecurity program designated in accordance with section 5-E.4(a) of this Appendix.

(v) Each covered water system shall at least annually review all user access privileges and remove or disable accounts and access that are no longer necessary to perform the user's job. Each covered water system shall immediately terminate access to user accounts following the user's departure from the covered water system or following a change in the user's role at the covered water system such that access is no longer required to perform the user's job. Where group-based or shared credentials have been implemented instead of unique credentials for each user, the group-based or shared credentials shall immediately be changed, or compensating controls shall be implemented to prevent unauthorized access to operational technology.

(vi) Each covered water system shall disable all remote access to operational technology that is not necessary to monitor or operate the system.

(vii) Each covered water system shall limit the functionality of all remote access to operational technology to only those functions necessary to monitor or operate the system.

(viii) Each covered water system shall securely configure all protocols that permit remote access to operational technology or nonpublic information.

(ix) Each covered water system shall disallow default passwords in all operational technology. Operational technology with default passwords that are technologically incapable of being changed shall have compensating controls implemented.

(3) Maintain a cyber asset inventory.

(4) Use defensive architecture, controls, compensating controls, and policies and procedures to protect operational technology and nonpublic information from unauthorized disclosure, alteration, or destruction.

(5) Identify and assess operational technology and nonpublic information for internal and external cybersecurity risks that may threaten the covered water system's ability to comply with the requirements of this Subpart.

(6) Each covered water system that serves a combined wholesale and retail population of greater than 50,000 shall monitor and log the covered water system's network activity, and be prepared to produce such logs in the event of a cyber incident for investigative purposes. The requirements of this paragraph shall not apply if the covered water system, for the purpose of alarms, notifications, or communications, utilizes devices that only allow, and are only capable of allowing, data to travel unidirectionally from operational technology to either information technology or external networks.

(7) Respond to cybersecurity incidents to mitigate the impacts on the normal operations of the covered water system. The response shall also address any impacts that could affect the ability of the covered water system to comply with the requirements of this Subpart. Additionally, the response shall aim to limit any physical or structural damage to the covered water system or any of its components.

(8) Recover from cybersecurity incidents and restore normal operations and services.

Section 5-E.7 Training

All drinking water treatment operators certified in accordance with Subpart 5-4 of this Part shall complete a minimum of one hour of cybersecurity training every three years. Cybersecurity training curriculum shall be approved by the department.

Section 5-E.8 Emergency response plan.

Each covered water system shall establish a written cybersecurity incident response plan in accordance with paragraph 5-1.33(b)(6) of this Subpart. This plan shall describe tasks to be performed during or following a cybersecurity incident to maintain or restore the covered water system's compliance with the requirements of this Subpart.

Section 5-E.9 Department Reporting.

The covered water system shall, in a manner prescribed by the department in accordance with section 5-1.77(a) of this Subpart, notify the department as soon as possible, but no later than 24 hours after determining a cybersecurity incident, as defined in 5-E.3(e) of this Appendix, has occurred which has created or may create a public health hazard. Notification to the department under this section does not replace any other notifications required under State or Federal laws or regulations.

Section 5-E.10 Confidentiality.

Information provided by a water system pursuant to this Part shall be subject to the applicable provisions of the Public Health Law, Education Law, and the Public Officers Law or any other applicable State or Federal law or regulations related to disclosure of such information.

Section 5-E.11 Severability.

If any provision of this section or the application thereof to any person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this section or the application thereof to other persons or circumstances.

REGULATORY IMPACT STATEMENT

Statutory Authority:

Public Health Law §1125 authorizes the adoption of regulations regarding water system emergency plans that include a vulnerability analysis to terrorist attack and cybersecurity incident or attack; and Public Health Law §225 authorizes the Public Health and Health Planning Council (PHHPC) to establish the sanitary code.

Legislative Objectives:

The objective of Public Health Law §1125 is to ensure water systems can provide water to their customers during an emergency by analyzing vulnerabilities and preparing emergency response plans beforehand. The emergency conditions water systems are required to consider has expanded over the years to include terrorist attack and cybersecurity incident, in addition to natural hazards. Public Health Law §225 authorizes the PHHPC to establish the sanitary code.

Needs and Benefits:

The United States (U.S.) water sector is critical infrastructure which is an attractive target for cybersecurity incidents and attacks. The water sector is vital to national security, economic security, public safety, and health. According to the U.S. Environmental Protection Agency, the overall cybersecurity maturity of the sector is low. This finding is consistent with the Office of the New York State Comptroller's audits of select municipalities in the last five years. As community water systems increase usage of computer-enabled and internet-connected systems, their potential vulnerability to attack increases, as does the attendant risk of public water supply

contamination. Without effective cybersecurity controls implemented, community water systems may unintentionally increase their risks to disruptive cybersecurity attacks.

As geopolitical conflicts escalate, the threat landscape for the water sector becomes more volatile. U.S. adversaries are outpacing the U.S. water sector's current cybersecurity defenses. Publicly reported cybersecurity incidents in the water sector as well as the U.S. intelligence community illustrate that adversaries are well-resourced to carry out disruptive cybersecurity attacks against the water and wastewater systems across the U.S.

This proposed regulation addresses sector-specific cybersecurity concerns by establishing risk-based baseline cybersecurity requirements. Specifically, community water systems that serve more than 3,300 people will be required to: conduct a cybersecurity vulnerability analysis (CVA) which must be reviewed and updated at least annually, and within 30 days of major infrastructure changes; establish compliance of a cybersecurity program informed by the CVA; create a cybersecurity incident response plan; report cybersecurity incidents which have created, or may create, a public health hazard to the Department of Health (Department) within 24 hours ; and report vulnerabilities that may impact or limit a covered water system's ability to comply with the requirements of 10 NYCRR Part 5 Subpart 5-1, or that may pose a risk to public health, to the Department within 48 hours of identification. Additionally, certified operators will be required to complete cybersecurity training approved by the Department for new certifications and renewal certifications.

Water systems serving a combined wholesale and retail population of greater than 50,000 will be subject to the same requirements, with additional requirements to designate an individual who is deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management who

shall be the individual to be responsible for the covered water system's cybersecurity program and monitor and log network activities in order to detect cybersecurity incidents.

The program leverages the existing cyber security vulnerability assessment program authorized under Public Health Law § 1125. While the existing program identifies baseline cybersecurity vulnerabilities and addresses all-hazards emergency response, the proposed regulation requires water systems to implement baseline cybersecurity controls to prevent the exploitation of potential vulnerabilities.

Costs

Costs for the Implementation of, and Continuing Compliance with the Regulation to the Regulated Entity, Including Costs to State and Local Governments:

The costs to regulated entities will vary due to the diversity of technology environments, as well as the presence and varying maturity of existing cybersecurity programs. Specifically, an entity's total costs will depend on its size; its network structure; the number of its critical assets, devices, employees, and users; and the way the entity chooses to comply with the requirements set forth in the proposed rule. The Department estimates that cybersecurity will cost $0-$150,000 per year for those systems that serve populations from 3,301 to 50,000 people; and $0-$5,000,000 per year for systems that serve more than 50,000 people, which includes the largest covered water supplies.

Covered water supplies will also be required to conduct a cyber asset inventory as part of the required cybersecurity program. A cyber asset inventory will range in costs depending on the size of the water system and the volume of assets needing evaluation. Asset inventory costs may include discovery tools and their associated licensing fees, consulting fees, and ongoing expenses

for updating and maintaining the asset inventory. Covered water supplies with less than 100 assets may see an annual cost of $0-$24,500, while systems with approximately 500-1000 assets could see annual costs from $0-$135,000.

Covered water supplies serving a combined retail and wholesale population of greater than 50,000 will also be required to designate an individual who is deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management to be responsible for the covered water system's cybersecurity program. It is anticipated that most public water systems of this size already have a qualified professional on staff that can serve in this role and a robust cybersecurity program. Additionally, these water systems will be required to monitor and log network activities in order to detect cybersecurity incidents, which the Department estimates will cost between $0-$54,000 per year.

New York State has funding available for the water and wastewater sectors, including hundreds of millions of dollars in infrastructure grants for addressing public health priorities and a new cybersecurity grant program totaling $2,500,000 that the Environmental Facilities Corporation will implement to support covered entities' compliance with this regulation. No- and low-cost cybersecurity services may be available that covered systems may utilize. However, this funding will likely not cover the full costs of these cybersecurity programs, and the remaining costs of these changes or upgrades, if any, may be borne by ratepayers or taxpayers depending on the size and/or complexity of the covered water system and their existing cybersecurity program.

Because of the wide range of technologies used at community water systems throughout the State, this proposed program uses a flexible regulatory model where covered water suppliers are required to obtain the expertise needed and make changes in accordance with their CVA,

either by hiring employees, contracting with cybersecurity experts, or leveraging no- and low-cost services to improve their baseline cybersecurity controls.

Local health departments will continue to have a role in verifying the completion of the statutorily required CVAs and are not expected to incur any additional costs. Most of the regulatory requirements will affect State and Local Governments. The Department estimates that cybersecurity will cost $0-$150,000 per year for those systems that serve populations from 3,300 to 50,000 people; and $0-$5,000,000 per year for systems that serve more than 50,000 people, which includes the largest covered water supplies.

Costs to the Department:

The Department proposes that oversight continue to be provided by its Bureau of Water Supply Protection in Albany. The tasks that will be completed by the Department include: developing guidance, templates and approved training curriculum for water system use and regulatory implementation; providing information about the water sector threat landscape; working with stakeholders and industry experts to identify cybersecurity best practices; coordinating with federal regulatory agencies and other experts on improving the cybersecurity position of the sector at large; and coordinating with the Division of Homeland Security and Emergency Services as well as the Department of Environmental Conservation to share ideas and expertise.

The Department estimates that 4 full-time equivalents will be required. It is expected that these positions will require approximately $600,969 per year inclusive of salary, fringe, travel, and indirect expenses.

Local Government Mandates:

There are 318 water systems serving more than 3,300 people that are owned and operated by local governments, with 37 of those water systems serving a combined wholesale and retail population of greater than 50,000. The majority of impacts will be on local governments.

This proposed regulation will affect local governments that own or operate water systems by requiring the development and implementation of a cybersecurity program to enhance system security and resilience. Systems serving populations of greater than 50,000 will also be required to designate an individual who is deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management who will be responsible for overseeing system cybersecurity. All affected systems must complete a CVA, consistent with existing requirements in Public Health Law §1125.

Additionally, authorized representatives for covered water systems will be required to report identified cybersecurity vulnerabilities within 48 hours that affect their ability to comply with the requirements of this Subpart, or that may pose a risk to public health, and to report cybersecurity incidents within 24 hours which have created, or may create, a public health hazard, which would increase paperwork.

Because of the wide range of technologies used at community water systems throughout the State, this proposed program uses a flexible regulatory model where covered water suppliers are required to obtain the expertise needed and make changes in accordance with their CVA, either by hiring employees, contracting with cybersecurity experts, or leveraging no- and low-cost services, to improve their baseline cybersecurity controls.

Paperwork:

This proposal builds on the existing cybersecurity vulnerability analysis required by Public Health Law §1125. It would increase paperwork by requiring documentation of cyber vulnerabilities and mandatory reporting of same to the Department.

Duplication:

This proposed regulation is designed to complement existing requirements in 10 NYCRR 5-1.33 and require a cybersecurity program for covered water systems. There are no similar federal requirements. Similar regulations may be promulgated by other State agencies with authority to regulate components of a covered water system's operation, such as the Department of Environmental Conservation or the Public Services Commission.

Alternatives:

Multiple alternatives were explored for this proposal, including maintaining the existing cybersecurity vulnerability assessment program and requiring a uniform cybersecurity program for all public water systems serving more than 3,300 people.

The Department determined that maintaining the existing program was insufficient in that it did not require mandatory training or incident reporting or critical cybersecurity controls. The Department also determined that the additional requirements placed on systems serving populations of greater than 50,000 were impracticable for "medium water systems" as that term is defined in 10 NYCRR 5-1.1(bj).

Federal Standards:

The United States Environmental Protection Agency requires that all community water systems that serve more than 3,300 people complete a risk and resilience assessment that includes an assessment of cybersecurity. This requirement is authorized through section 2013 of the America's Water Infrastructure Act (AWIA) of 2018, which amended Section 1433 of the Safe Drinking Water Act (SDWA). There are no additional federal standards.

Compliance Schedule:

Covered water systems shall comply with most requirements of this Appendix by January 1, 2027, though training and cybersecurity incident notification requirements are effective upon publication of the Notice of Adoption in the State Register. Operators shall complete the requisite training by the end of the first full registration cycle for an individual operator following the effective date of the regulation.

Contact Person

Katherine Ceroalo
New York State Department of Health
Bureau of Program Counsel, Regulatory Affairs Unit
Corning Tower Building, Rm. 2438
Empire State Plaza
Albany, New York 12237
(518) 473-7488
(518) 473-2019 (FAX)
REGSQNA@health.ny.gov

REGULATORY FLEXIBILITY ANALYSIS FOR SMALL BUSINESS AND LOCAL GOVERNMENTS

Effect of Rule:

This proposed regulation addresses sector-specific cybersecurity concerns by establishing risk-based baseline cybersecurity requirements. Specifically, all community water systems which serve populations greater than 3,300 people will be required to: conduct a cybersecurity vulnerability analysis (CVA), which must be reviewed and updated at least annually and within 30 days of major infrastructure changes; establish compliance of a cybersecurity program informed by the CVA; create a cybersecurity incident response plan; report cybersecurity incidents to the Department of Health (Department) within 24 hours which have created, or may create, a public health hazard; and report vulnerabilities that may impact or limit a covered water system's ability to comply with the requirements of 10 NYCRR Part 5 Subpart 5-1, or that may pose a risk to public health, to the Department within 48 hours of identification. Additionally, certified operators will be required to complete cybersecurity training approved by the Department for new certifications and renewal certifications.

This rule will primarily impact local governments since 318 public water systems that serve more than 3,300 people are owned by local governments, with 37 of those water systems serving a combined wholesale and retail population of greater than 50,000.

Water systems serving a combined wholesale and retail population of greater than 50,000 will be subject to the same requirements, with additional requirements to designate an individual who is deemed qualified by the covered water system's owner with demonstrable knowledge of

cybersecurity principles and practical experience in system protection or risk management who shall be the individual responsible for the system's cybersecurity program.

A covered water system that has neither physical nor logical connections between operational technology and information technology or external networks is exempt from the cybersecurity requirements in this Appendix. All covered water suppliers that are required to meet the requirements of section 5-1.33 of Subpart 5-1 shall continue to do so.

Compliance Requirements:

Covered water systems shall comply with the requirements of this Appendix by January 1, 2027, though training and cybersecurity incident notification requirements are effective upon adoption. Operators shall complete the requisite training by the end of the first full registration cycle for an individual operator following the effective date of the regulation.

Professional Services:

Water systems that serve more than 50,000 must designate an individual who is deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management who shall be the individual responsible for the system's cybersecurity program. Some covered water systems will be required to obtain this expertise via contract and could be delayed by the competitive bidding requirements for professional services. We anticipate the one-year implementation time frame included in the proposed regulation will be sufficient to allow municipalities to undergo the competitive bidding process for services, if needed. However, that is dependent upon

municipalities undertaking the process in a timely manner and then receiving acceptable responses.

Compliance Costs:

The costs to regulated entities will vary due to the diversity of technology environments, as well as the presence and varying maturity of existing cybersecurity programs. Specifically, an entity's total costs will depend on its size; its network structure; the number of its critical assets, devices, employees, and users; and the way the entity chooses to comply with the requirements set forth in the proposed rule. The Department estimates that cybersecurity will cost $0-$150,000 per year for those systems that serve populations from 3,300 to 50,000 people; and $0-$5,000,000 per year for systems that serve more than 50,000 people, which includes the largest covered water supplies.

Covered water supplies will also be required to conduct a cyber asset inventory as part of the required cybersecurity program. A cyber asset inventory will range in costs depending on the size of the water system and the amount of assets discovered. Asset inventory costs may include discovery tools and their associated licensing fees, consulting fees, and ongoing expenses for updating and maintaining the asset inventory. Covered water supplies with less than 100 assets may see an annual cost of $0-$24,500, while systems with approximately 500-1000 assets could see annual costs from $0-$135,000.

Covered water supplies serving a combined retail and wholesale population of greater than 50,000 will also be required to designate an individual who is deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management who shall be the individual

responsible for the system's cybersecurity program. It is anticipated that most public water systems of this size already have a qualified professional on staff that can serve in this role and a robust cybersecurity program. Additionally, these water systems will be required to monitor and log network activities in order to detect cybersecurity incidents, which the Department estimates will cost between $0-$54,000 per year.

New York State has funding available for the water and wastewater sector, including hundreds of millions of dollars in infrastructure grants for addressing public health priorities, and a new cybersecurity grant program totaling $2,500,000 that the Environmental Facilities Corporation will implement to support covered entities comply with this regulation. No- and low-cost cybersecurity services may be available to the water sector that the covered entities may utilize. However, this funding will likely not cover the full costs of these cybersecurity programs, and the remaining costs of these changes or upgrades, if any, may be borne by ratepayers or taxpayers depending on the size and complexity of the covered water system and their existing cybersecurity program.

Because of the wide range of technologies used at community water systems throughout the State, this proposed program uses a flexible regulatory model where covered water suppliers are required to obtain the expertise needed and make changes in accordance with their CVA, either by hiring employees, contracting with cybersecurity experts, or leveraging no- and low-cost services to improve their baseline cybersecurity controls.

The benefits of this rule are challenging to quantify, since the risk of cybersecurity incidents, the ability to recover from cybersecurity incidents, and the costs of cybersecurity incidents are specific to the covered water systems' operations, the controls they employ, the nature of the cybersecurity incidents and the ability to operate manually.

Economic and Technology Feasibility:

The regulations are anticipated to be economically and technologically feasible since many covered water systems are already implementing robust cybersecurity programs that meet the requirements of this regulation. The Department has determined that requiring one hour of cybersecurity training per three-year renewal cycle is economically and technologically feasible. In addition, the Department has determined it is both economically and technologically feasible to require covered water systems to report cybersecurity incidents to the Department within 24 hours which have created, or may create, a public health hazard, and vulnerabilities that may impact or limit a covered water system's ability to comply with the requirements of 10 NYCRR Part 5 Subpart 5-1, or that may pose a risk to public health, within 48 hours of identification.

Minimizing Adverse Impact:

The proposed rule incorporates several exemptions for covered water systems at low risk of public health consequences related to a cybersecurity incident. A key exemption excludes covered water systems if they have neither physical nor logical connections between operational technology and information technology or external networks.

Small Business and Local Government Participation:

The Department held engagement sessions with regulated entities on the following dates:

February 26, 2025 – Monroe County Water Authority

March 6, 2025 – NY Rural Water Association, Village of Westfield, Star Lake, David Bunce, independent operator.

March 14, 2025 – American Water Works Association, NYS American Water Works Association, NY Rural Water Association and Suffolk County Water Authority.

March 19, 2025 – Long Island Water Conference

March 26, 2025 – Adirondack Water Works Conference

April 15, 2025 – American Water Works Association, Water Utility Council Meeting

May 20, 2025 –New York Rural Water Association Annual Conference

Most water systems were supportive of the regulatory requirements, and many water systems have already implemented actions to improve their cybersecurity position. However, many were concerned about the cost of the regulation and additional workload required at a time when the water sector was implementing several new regulations. New regulations include the Consumer Confidence Rule, federal rules addressing per- and polyfluoroalkyl substances, and significant amendments to rules that address lead in drinking water. Stakeholders were concerned that there would be insufficient capacity to successfully comply with four new regulatory requirements simultaneously.

RURAL AREA FLEXIBILITY ANALYSIS

Types and Estimated Numbers of Rural Areas:

This rule applies uniformly throughout the State, including rural areas. Rural areas are defined as counties with a population less than 200,000 and counties with a population of 200,000 or greater that have towns with population densities of 150 persons or fewer per square mile. The following 44 counties have a population of less than 200,000 based upon the United States Census estimate of county populations for 2020 (https://www.census.gov/quickfacts/).

Allegany County	Greene County	Schoharie County
Broome County	Hamilton County	Schuyler County
Cattaraugus County	Herkimer County	Seneca County
Cayuga County	Jefferson County	St. Lawrence County
Chautauqua County	Lewis County	Steuben County
Chemung County	Livingston County	Sullivan County
Chenango County	Madison County	Tioga County
Clinton County	Montgomery County	Tompkins County
Columbia County	Ontario County	Ulster County
Cortland County	Orleans County	Warren County
Delaware County	Oswego County	Washington County
Essex County	Otsego County	Wayne County
Franklin County	Putnam County	Wyoming County
Fulton County	Rensselaer County	Yates County
Genesee County	Schenectady County	

The following counties have a population of 200,000 or greater and towns with population densities of 150 persons or fewer per square mile. Data is based upon the United States Census estimated county populations for 2020.

Albany County	Niagara County	Orange County
Dutchess County	Oneida County	Saratoga County
Erie County	Onondaga County	Suffolk County
Monroe County		

Reporting, Recordkeeping and Other Compliance Requirements; and Professional Services:

Water systems that serve 50,000 or more people must designate an individual deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management who shall be the individual responsible for the system's cybersecurity program. Some covered water systems may choose to obtain this expertise via contract and could be delayed by the competitive bidding requirements for professional services.

Costs:

The costs to regulated entities will vary due to the diversity of technology environments and the presence of existing cybersecurity programs. Each organization's costs depend on the size and complexity of the covered water system and their existing cybersecurity program.

The costs to regulated entities will vary due to the diversity of technology environments, as well as the presence and varying maturity of existing cybersecurity programs. Specifically, an

entity's total costs will depend on its size; its network structure; the number of its critical assets, devices, employees, and users; and the way the entity chooses to comply with the requirements set forth in the proposed rule. The Department estimates that cybersecurity will cost $0-$150,000 per year for those systems that serve populations between 3,300 and 50,000 people; and $0-$5,000,000 per year for systems that serve 50,000 or more, which includes the largest covered water supplies.

Covered water supplies will also be required to conduct a cyber asset inventory as part of the required cybersecurity program. A cyber asset inventory will range in costs depending on the size of the water system and the amount of assets discovered. Asset inventory costs may include discovery tools and their associated licensing fees, consulting fees, as well as ongoing expenses for updating and maintaining the asset inventory. Covered water supplies with less than 100 assets may see an annual cost of $0- $24,500, while systems with approximately 500-1000 assets could see annual costs from $0-$135,000.

Covered water supplies serving a combined retail and wholesale population of 50,000 people or greater will also be required to designate an individual deemed qualified by the covered water system's owner with demonstrable knowledge of cybersecurity principles and practical experience in system protection or risk management who shall be the individual responsible for the system's cybersecurity program. It is anticipated that most public water systems of this size already have a qualified professional on staff that can serve in this role and a robust cybersecurity program. Additionally, these water systems will be required to monitor and log network activities in order to detect cybersecurity incidents, which the Department estimates will cost between $0-$54,000 per year.

New York State has funding available for the water and wastewater sector, including hundreds of millions of dollars in infrastructure grants for addressing public health priorities, and a new cybersecurity grant program totaling $2,500,000 that the Environmental Facilities Corporation will implement to support covered entities comply with this regulation. No- and low-cost cybersecurity services may be available to the water sector that the covered entities may utilize. However, the costs of these changes or upgrades, if any, may be borne by ratepayers or taxpayers depending on the size and/or complexity of the covered water system and their existing cybersecurity program.

Because of the wide range of technologies used at community water systems throughout the State, this proposed program uses a flexible regulatory model where covered water suppliers are required to obtain the expertise needed and make changes in accordance with their cybersecurity vulnerability analysis (CVA), either by hiring employees, contracting with cybersecurity experts, or leveraging no and low cost services to improve their cyber posture and implementing baseline cybersecurity controls.

Minimizing Adverse Impact:

The proposed rule incorporates several exemptions for covered water systems at low risk of public health consequences related to a cyber-attack if they have neither physical nor logical connections between operational technology and information technology or external networks.

Rural Area Participation:

The Department held engagement sessions with regulated entities on the following dates: February 26, 2025 – Monroe County Water Authority

March 6, 2025 – NY Rural Water Association, Village of Westfield, Star Lake, David Bunce, independent operator.

March 14, 2025 – American Water Works Association, NYS American Water Works Association, NY Rural Water Association, Suffolk County Water Authority

March 19, 2025 – Long Island Water Conference

March 26, 2025 – Adirondack Water Works Conference

May 20, 2025 – New York Rural Water Association Annual Conference

Most water systems were supportive of the regulatory requirements, and many water systems have already implemented actions to improve their cybersecurity position. However, many were concerned about the cost of the regulation and additional workload required at a time when the water sector was experiencing several new regulations, including the Consumer Confidence Rule, federal rules addressing per- and polyfluoroalkyl substances, and amended rules addressing lead in drinking water. Stakeholders were concerned that there would be insufficient capacity to successfully comply with four new regulatory requirements simultaneously.

JOB IMPACT STATEMENT

A Job Impact Statement for these amendments is not being submitted because it is apparent from the nature and purposes of the amendments that they will not have a substantial adverse impact on jobs and/or employment opportunities.