Public Health and Health Planning Council

Codes, Regulations and Legislation Committee Meeting Agenda

September 18, 2025
9:30 a.m.

90 Church Street, 4th Floor, Conference Rooms 4 A/B, NYC, 10007

I. WELCOME AND INTRODUCTION

Thomas Holt, Chair, Commitee on Codes, Regulations and Legislation

II. REGULATIONS

For Adoption

24-22 Amendment of Section 405.4 of Title 10 NYCRR (12-Week Rule for Foreign Medical School Graduates and Limited Permit Allowances)

22-06 Amendment of Section 23.5 of Title 10 NYCRR (Expedited Partner Therapy for Sexually Transmitted Infections)

For Information

25-09 Addition of Appendix 5-E to Subpart 5-1 of Title 10 NYCRR (Cybersecurity Requirements for Public Water Systems)

III. ADJOURNMENT

Pursuant to the authority vested in the Public Health and Health Planning Council and the Commissioner of Health by section 2803 of the Public Health Law, section 405.4 of Title 10 of the Official Compilation of Codes, Rules and Regulations of the State of New York (NYCRR) is hereby amended, to be effective upon publication of a Notice of Adoption in the New York State Register, to read as follows:

Subparagraph (ii) of paragraph (1) of subdivision (f) of section 405.4 is amended to read as follows:

(ii) [except for individuals eligible for licensure under section 6528 of the State Education Law,] a graduate of a foreign medical school who enrolled in such medical school after October 1, 1983 shall have completed the clinical component of a program of medical education which:

(*a*) included no more than 12 weeks of clinical clerkships in a country other than the country in which the medical school is located; or

(*b*) included clinical clerkships of greater than 12 weeks in a country other than the country in which the medical school is located [if], provided:

(*1*) the clinical clerkships were offered by a medical school approved by the State Education Department for the purposes of clinical clerkships; or

(*2*) the individual subsequently completed a post-graduate training program approved by the Accreditation Council for Graduate Medical Education or the American Osteopathic Association, and the individual is eligible to complete additional training in a postgraduate fellowship program.

Paragraph (2) of subdivision (g) of Section 405.4 is amended to read as follows:

(2) (i) physicians who possess limited permits to practice medicine issued by the New York State Education Department pursuant to section 6525 of the State Education Law if such physicians are under the supervision of a physician licensed and currently registered to practice medicine in the State of New York, and if the physicians possessing limited permits are:

[(i)] *(a)* graduates of a medical school [offering a medical program accredited by the Liaison Committee on Medical Education or the American Osteopathic Association, or] registered with the State Education Department or accredited by an accrediting organization acceptable to the State Education Department, and have satisfactorily completed one year of graduate medical education in a postgraduate training program accredited by the Accreditation Council for Graduate Medical Education or the American Osteopathic Association, or their predecessors or successors [or an equivalent accrediting agency acceptable to the State Education Department]; or

[(ii)] *(b)* graduates of a foreign medical school, defined as those schools which are not accredited or registered by the State Education Department pursuant to clause (*a*) of this subparagraph, and have satisfactorily completed three years of graduate medical education in a postgraduate training program accredited by the Accreditation Council for Graduate Medical Education [or], the American Osteopathic Association, or the Committee on Accreditation of Canadian Medical Schools, or their predecessors or successors [or an equivalent accrediting agency acceptable to the State Education Department; or];

[(iii) graduates of a foreign medical school who have satisfactorily completed three years in a postgraduate training program and who are receiving advanced training as part of an official

exchange visitor program approved by the United States Information Agency and the Educational Commission for Foreign Medical Graduates (ECFMG);]

(ii) if the physician possessing the limited permit has not completed a postgraduate training program of a satisfactory length or accreditation, as set forth in subparagraph (i) of this paragraph, but such physician will be a member of the workforce of a public hospital licensed under article 28 of the Public Health Law, such physician shall be permitted to provide patient care services within such hospital. Provided, however, that such limited permit holder must be directly supervised by a physician licensed and currently registered to practice medicine in the State of New York, who is credentialed by the hospital in the field in which the limited permit holder is practicing, and who is responsible for monitoring and supervising the limited permit holder in the same manner as required for supervision and monitoring of postgraduate trainees pursuant to paragraph (3) of subdivision (f) of this section. For the purposes of this subdivision, a public hospital shall mean a general hospital operated by a county, municipality, or public benefit corporation;

REGULATORY IMPACT STATEMENT

Statutory Authority:

Public Health Law (PHL) section 2803 authorizes the Public Health and Health Planning Council (PHHPC) to adopt and amend rules and regulations, subject to the approval of the Commissioner of Health (Commissioner), to implement the purposes and provisions of PHL Article 28 and to establish minimum standards governing the operation of health care facilities.

Legislative Objectives:

The legislative objectives of PHL Article 28 include the protection of the health of the residents of the State by promoting the efficient provision and proper utilization of high quality health services at a reasonable cost.

Needs and Benefits:

Needs and Benefits of Proposed Amendments to Section 405.4(f):

Under 10 NYCRR section 405.4(f), a post-graduate trainee (intern or resident) may practice medicine in a hospital under licensing exemptions set forth in Education Law section 6526. 10 NYCRR section 405.4(f)(1)(ii)(b) contains special requirements for graduates of foreign medical schools to engage in such a post-graduate training program, including setting forth the "12-week rule." Specifically, under this provision, if the graduate of the foreign medical school had a clinical clerkship of greater than 12 weeks in a country other than the country where their medical school was located, then the clinical clerkship must have been in a "a medical school approved by the State Education Department for the purposes of clinical clerkships."

There are currently only 17 international medical schools approved by the State Education Department (SED) "for the purposes of clinical clerkships." If a medical school is not one of these 17 schools approved by SED for the purposes of clinical clerkships, and a graduate of that medical school received more than 12 weeks of clerkship education in another country to complete the requirements for the applicant's medical education degree, that graduate is barred from enrolling in any post-graduate training program that includes providing patient care services in a New York teaching hospital.

The proposed amendment to section 405.4(f)(1)(ii)(b) would allow individuals who subsequently completed a post-graduate training program approved by the Accreditation Council for Graduate Medical Education or the American Osteopathic Association, and who is eligible to complete additional training in a postgraduate fellowship program, to meet the "12-week" exception to graduate medical education that occurs outside of the US. Considering severe physician staffing shortages throughout the State, this proposed revision is necessary to expand the number of sufficiently educated and trained physicians who can practice in post-graduate training programs in New York State hospitals.

Needs and Benefits of Proposed Amendments to Section 405.4(g):

10 NYCRR section 405.4(g)(2) allows an unlicensed physician to provide medical services in a general hospital under a limited permit to practice medicine, issued by SED pursuant to Education Law section 6525 if SED determines that the applicant meets criteria for issuance of a limited permit and appropriate levels of supervision and oversight are in place.

Section 405.4(g)(2) requires additional years of post-graduate training, beyond what is required for a limited permit under Education Law section 6525, in order for a holder of an SED-issued "limited permit" to provide care in a "general hospital," with the number of years of post-

graduate training dependent on whether the limited permit holder graduated from a foreign or domestic medical school. Public Health Law section 2801(10) defines "general hospital" as a facility that provides medical and surgical services primarily to in-patients under 24-hour supervision of a physician. The term "general hospital" does not include a "residential health care facility, public health center, diagnostic center, treatment center, out-patient lodge, dispensary and laboratory or central service facility serving more than one institution."

Currently, section 405.4(g)(2) imposes additional years of training for limited permit holders, specifically one year for domestic medical graduates and three years for international (foreign) medical graduates, as a condition of working in a New York State hospital. This requirement was originally intended to ensure that international students' educations were equivalent to those of physicians educated in the United States. As a result, hospitals hiring doctors to meet patient needs often must turn away otherwise qualified applicants to maintain compliance with the regulation. These candidates, if unable to work in New York State hospitals, may seek employment in other states or in other types of health care settings where the extra years of experience are not required.

SED already considers training and experience before approving and issuing limited permits; however, SED does not screen candidates for their eligibility to work in hospitals. In addition, limited permit holders working in other settings in New York State, such as nursing homes and psychiatric hospitals, are not required to have these additional years of training. As such, there is inconsistency in the standards required of limited permit holders with equivalent background and training, making limited permit holders less likely to be to be utilized in hospitals.

The proposed regulation, through the addition of new subparagraph (ii), would eliminate the additional years of post-graduate training required for limited permittees if the limited permit holder would be a member of the workforce of a public hospital—defined in the regulation as a general hospital operated by a county, municipality, or public benefit corporation—and provided that the limited permit holder would be subject to the same supervision required of a medical resident. Given the shortage of licensed physicians to cover vital hospital services, this proposed amendment will eliminate a barrier to limited permit holders practicing in public hospitals, which serve a critical portion of New York's patient population.

Overall, the Department of Health believes that amending both of these regulations is the most effective means to ease physician staffing shortages in hospitals, with guardrails to ensure that physicians educated outside of the US still meet an appropriate education and oversight bar. SED has reviewed and approved the proposed amendment, and they have support from key industry stakeholders. Finally, since all limited permit holders are subject to supervision and oversight by a licensed physician, their practice within the hospital will be monitored to help ensure the highest standards of patient care are met.

COSTS:

Costs to Private Regulated Parties:

This proposal will not result in increased costs to regulated parties.

Costs to Local Government:

This regulation amendment will not impact local governments unless they operate a general hospital. In any event, this proposal will not increase costs for local governments. They

are expected to help hospitals, including those operated by a local government, by alleviating physician staffing shortages.

Costs to the Department of Health:

The proposed regulatory changes will not result in any additional operational costs to the Department of Health.

Costs to Other State Agencies:

The proposed regulatory changes will not result in any additional costs to other State agencies.

Local Government Mandate:

The proposed regulatory changes will not impose any new programs, services, duties or responsibilities upon any county, city, town, village, school district, fire district or other special district.

Paperwork:

The proposed regulatory changes will not create any additional paperwork.

Duplication:

There are no relevant State regulations which duplicate, overlap or conflict with the proposed regulatory changes.

Alternatives:

The alternative would be to take no action and have hospitals continue to screen limited permit holders for additional years of training as a condition of employment. This is not a viable option, however, as taking no action would only exacerbate the current physician staffing shortage.

Federal Standards:

The proposed regulatory changes do not duplicate or conflict with any federal regulations.

Compliance Schedule:

The regulations will be effective upon publication of a Notice of Adoption in the New York State Register.

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

STATEMENT IN LIEU OF REGULATORY FLEXIBILITY ANALYSIS

No Regulatory Flexibility Analysis is required pursuant to section 202-(b)(3)(a) of the State Administrative Procedure Act. The proposed amendment does not impose an adverse economic impact on small businesses or local governments, and it does not impose reporting, record keeping or other compliance requirements on small businesses or local governments.

STATEMENT IN LIEU OF
RURAL AREA FLEXIBILITY ANALYSIS

A Rural Area Flexibility Analysis for these amendments is not being submitted because amendments will not impose any adverse impact or significant reporting, record keeping or other compliance requirements on public or private entities in rural areas. There are no professional services, capital, or other compliance costs imposed on public or private entities in rural areas as a result of the proposed amendments.

STATEMENT IN LIEU OF JOB IMPACT STATEMENT

No Job Impact Statement is required pursuant to section 201-a(2)(a) of the State Administrative Procedure Act. No adverse impact on jobs and employment opportunities is expected as a result of these proposed regulations.

Pursuant to the authority vested in the Public Health and Health Planning Council and the Commissioner of Health by sections 225(4) and 2312 of the Public Health Law, section 23.5 of Title 10 (Health) of the Official Compilation of Codes, Rules and Regulations of the State of New York is amended, to be effective upon publication of a Notice of Adoption in the New York State Register, to read as follows:

23.5 Expedited [p]Partner [t]Therapy for [chlamydia trachomatis infection] sexually transmitted infections.

(a) Definitions. As used in this section:

(1) "Expedited Partner Therapy" or "EPT" means a practice whereby a health care practitioner chooses to provide a patient with either antibiotics intended for the patient's sexual partner or partners or a written prescription for antibiotics for the sexual partner or partners to be delivered by the patient to the sexual partner or partners for treatment of exposure to [Chlamydia trachomatis] sexually transmitted infections (STIs).

(2) "Health care practitioner" means a physician, midwife, nurse practitioner, physician assistant, or other person who is authorized under Title 8 of the Education Law to diagnose and prescribe drugs for [Chlamydia trachomatis] STIs, acting within [his or her] their lawful scope of practice.

(b) Liability. A health care practitioner who reasonably and in good faith renders expedited partner therapy in accordance with section 2312 of the Public Health Law and this section, and a pharmacist who reasonably and in good faith dispenses drugs pursuant to a prescription written in accordance with section 2312 of the Public Health Law and this section, shall not be subject to civil or criminal liability or be deemed to have engaged in unprofessional conduct.

(c) Eligibility criteria for EPT. EPT shall:

(1) [be provided only for the partner or partners of a patient diagnosed with Chlamydia trachomatis infection] be provided for sexual partner(s) of patients diagnosed (either through laboratory confirmation or clinical diagnosis) with an STI for which EPT is recommended by the Federal Centers for Disease Control and Prevention (CDC). The department shall list which STIs are eligible for EPT on the department's website and shall promulgate guidelines that include partner eligibility criteria. If the patient's sexual partner(s) are pregnant or there is a suspicion of possible pregnancy, some EPT medications are not recommended, and the partner(s) should seek medical care as soon as possible; and

(2) not be provided [for any partner or partners, when the patient with Chlamydia trachomatis infection seen by the health care practitioner is found to be concurrently infected with gonorrhea, syphilis or HIV] in cases involving suspected or confirmed child abuse, sexual abuse/assault, or where the diagnosed patient's safety may be impacted.

(d) Educational material requirements for patients provided with EPT. Each patient provided with antibiotics or a prescription in accordance with this section must be given informational materials for the patient to give to [his or her] their sexual partner or partners. Each patient shall be counseled by [his or her] the patient's health care practitioner to inform [his or her] the patient's partner or partners that it is important to read the information contained in the materials prior to the partner or partners taking the medication.

The materials shall:

(1) encourage the partner to consult a health care practitioner for a complete [sexually transmitted infection] sexual health evaluation, including HIV testing, as a preferred alternative to EPT and regardless of whether they take the medication;

(2) disclose the risk of potential adverse drug reactions, including allergic reactions, and the possibility of dangerous interactions between the patient-delivered therapy and other medications that the partner may be taking;

(3) inform the partner that [he or she] they may be affected by other [sexually transmitted infections] STIs that may be left untreated by the delivered medicine;

(4) inform the partner that if symptoms of a more serious infection are present (such as abdominal, pelvic, or testicular pain, fever, nausea or vomiting) [he or she] they should seek medical care as soon as possible;

(5) recommend that a partner who is or could be pregnant should consult a health care practitioner as soon as possible;

(6) instruct the patient and the partner to abstain from sexual activity for at least seven days after treatment of both the patient and the partner in order to [decrease the risk of recurrent infection] reduce the likelihood of reinfection;

[(7) inform a partner who is at high risk of co-morbidity with HIV infection that he or she should consult a health care practitioner for a complete medical evaluation including testing for HIV and other sexually transmitted infections] and

[(8)] (7) inform the patient and the partner how to prevent [repeated chlamydia infection] and reduce the likelihood of reinfection.

(e) Prescription format. Whenever a health care practitioner provides EPT through the use of a prescription:

(1) the designation "EPT" must be written in the body of the prescription form above the name of the medication and dosage for all prescriptions issued;

(2) if the name, address, and date of birth of the sexual partner are available, this should be written in the designated area of the prescription form; and

(3) if the sexual partner's name, address, and date of birth are not available, the written designation "EPT" shall be sufficient for the pharmacist to fill the prescription.

(f) Reporting of cases of [Chlamydia trachomatis] STIs by health care providers.

(1) This section shall not affect the obligation to report individual cases and suspected cases of [Chlamydia trachomatis] STIs imposed by Part 2 of this [Chapter] Title.

(2) Reports of cases of [Chlamydia trachomatis] STIs who are provided with EPT shall include the added designation of "EPT" plus the number of sexual partners for whom a prescription or medication was provided.

REGULATORY IMPACT STATEMENT

Statutory Authority:

Pursuant to sections 225(4) and 2312 of the Public Health Law (PHL), the Commissioner of Health and the Public Health and Health Planning Council have the authority to adopt regulations concerning Expedited Partner Therapy for Chlamydia Trachomatis Infection and Other Sexually Transmitted Infections.

Legislative Objectives:

Laws of 2008, Chapter 577, allowed health care providers with prescriptive privileges to provide Expedited Partner Therapy (EPT) for Chlamydia when the prescriber's judgment is that the partner(s) will not seek a personal medical visit. This law has helped improve treatment rates for partners and decrease re-infection rates for partners. Laws of 2019, Chapter 298, amended PHL section 2312 to expand the use of EPT for other sexually transmitted infections (STIs) that the Centers for Disease Control and Prevention (CDC) recommends for EPT, in addition to Chlamydia.

EPT helps physicians and other health care providers decrease rates of STIs. While EPT in no way replaces a face-to-face interaction with a health care provider, it can help patients who otherwise would not reach out for treatment.

The CDC has found through randomized controlled tests that EPT has the potential for the same success that it has shown with Chlamydia with other STIs. EPT can be highly effective in decreasing infection rates with other STIs, such as gonorrhea, that can be cured by taking antibiotics by mouth.

Needs and Benefits:

EPT is the clinical practice of providing individuals with medication or a prescription to deliver to their sexual partner(s) as treatment for a presumptive STI, without completing a clinical assessment of those partners.

On January 1, 2020, Chapter 298 of the Laws of 2019 went into effect, expanding PHL section 2312 to permit expedited treatment for STIs for which the CDC recommends the use of expedited therapy. Prior to this change, EPT was allowable in New York State for chlamydia only. In addition to supporting EPT for chlamydia, at this time the CDC also supports or lists EPT as a strategy for partner management for persons diagnosed with either gonorrhea or trichomoniasis.

Chlamydia, gonorrhea, and trichomoniasis are STIs that are transmitted by sexual contact with a penis, vagina, mouth, or anus of an infected sex partner; these STIs can result in adverse health effects if left untreated. According to the 2019 national STI surveillance report released by CDC, both chlamydia and gonorrhea diagnoses have continued to rise, with 19% and 56% increases, respectively since 2015. New York State has mirrored the national increases in both chlamydia and gonorrhea with 20% and 60% increases, respectively, since 2015. Additionally, though trichomoniasis is not a reportable STI both nationally and in New York State, the CDC estimates that nationally there are around 6.9 million (diagnosed or undiagnosed) new infections.

With respect to EPT, three US clinical trials involving heterosexually active males and females with chlamydia or gonorrhea all show that more sexual partners were treated when the patients were offered EPT. Two out of those three trials showed a significant reduction in re-infection of the patients, and the third noted a decreased risk of recurrent infection that was not significant. One trial show that there was a reduction in prevalence as high as 10% in females

when EPT was provided free of charge. Though trials and meta-analyses conducted on EPT differ in findings with respect to the magnitude of the reduction in re-infection, all show a reduction in prevalence in chlamydia and gonorrhea at follow up. Though data on EPT for trichomoniasis is limited, EPT may have a role in partner management, and it should remain an option when treatment of partners cannot otherwise be assured.

The CDC, along with several national professional organizations, recommend EPT as an effective and practical strategy for treating the sex partners of people diagnosed with chlamydia and/or gonorrhea. The New York State Department of Health (NYSDOH) previously released a position statement strongly encouraging providers to utilize EPT as a strategy to treat the sex partner(s) of persons diagnosed with chlamydia. In consideration of the expansion of the law, and of what is a larger shift toward a comprehensive sexual health framework, the position statement was revised to: expand the use of EPT to include gonorrhea and trichomoniasis, remove exclusionary language, and include updated treatment guidelines.

Current New York Codes, Rules, and Regulations (NYCRR) section 23.5, of Title 10 provides definitions, and eligibility specific to EPT for chlamydia only. Given the expansion of PHL section 2312 to include additional STIs beyond chlamydia alone, the regulation needs to be modified as follows: 1) rather than defining EPT as a strategy for treating chlamydia, EPT needs to be defined as a strategy more generically for STIs and be integrated with other sexual health services, 2) rather than stating eligibility is limited to persons diagnosed with chlamydia who are not co-infected with gonorrhea or HIV, the regulation should state persons eligible for EPT are those diagnosed with an STI for which the CDC recommends the use of EPT for partner management, and 3) an addendum to the eligibility section should include language permitting the Commissioner of Health to designate which STIs are eligible in the department's website.

Additional proposed modifications to the current regulation specific to the educational material requirements include: shifting from the use of binary language ("his/her") to gender neutral language ("their") to ensure inclusivity and removing specific language stating persons at high risk of co-morbidity with HIV should seek medical evaluation, as HIV testing for all persons receiving EPT educational materials is already included as a recommendation in a previous section and this additional callout can be deemed stigmatizing.

Costs:

Costs for the Implementation of, and Continuing Compliance with the Regulation to the Regulated Entity:

An estimated $850 million is spent annually treating chlamydia and gonorrhea in the US. EPT can decrease these costs by reducing the spread of infections and re-infections by reducing the reliance on public services to treat STIs. If left untreated, chlamydia and gonorrhea can progress to pelvic inflammatory disease (PID) in females, resulting in additional treatment costs of $1,167 per case of PID. Both infections are also a common cause of infertility; and because EPT increases STI treatment rates and reduces prevalence of chlamydia and gonorrhea, infertility and PID resulting from such infections will likely decline. Both chlamydia and gonorrhea change the immune system and may increase a person's chances of contracting HIV if exposed to the virus. Data related to costs for screening and treatment of trichomanias are limited. Integrating EPT into a broader sexual health approach can have significant public health benefits, including lowering overall STI rates and reducing healthcare costs associated with untreated infections.

Costs to State and Local Governments:

This regulation imposes no costs on State and local governments. It expands the use of EPT.

Costs to the Department of Health:

The additional costs to the NYSDOH will be related to additional data collection burden and follow up; such costs are expected to be minimal and easily accommodated within existing infrastructure.

Local Government Mandates:

This proposal has no local mandates.

Paperwork:

The existing electronic data collection mechanism was revised when the law was changed such that local health departments could start reporting provision of EPT for the other STIs.

Duplication:

These regulations will not conflict with any State or federal rules.

Alternatives:

The alternative to this regulatory amendment would be to not conform the regulation to PHL section 2312, as amended by Laws of 2019, Chapter 298. This is not a viable alternative as

the Department of Health is obligated to execute the PHL. This regulation is further necessary to expand the availability EPT to reduce the rates of sexually transmitted infections.

Federal Standards:

The Centers for Disease Control and Prevention has recommendations related to expedited partner therapy. This regulation is consistent with federal standards.

Compliance Schedule:

This regulation is effective upon the publication of the Notice of Adoption in the State Register. This regulation permits, but does not require, EPT for STI.

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

STATEMENT IN LIEU OF REGULATORY FLEXIBILITY ANALYSIS

No regulatory flexibility analysis is required pursuant to section 202-b(3)(a) of the State Administrative Procedure Act. The proposed amendment does not impose an adverse economic impact on small businesses or local governments, and it does not impose reporting, record keeping or other compliance requirements on small businesses or local governments.

STATEMENT IN LIEU OF
RURAL AREA FLEXIBILITY ANALYSIS

A Rural Area Flexibility Analysis for these amendments is not being submitted because amendments will not impose any adverse impact or significant reporting, record keeping or other compliance requirements on public or private entities in rural areas. There are no professional services, capital, or other compliance costs imposed on public or private entities in rural areas as a result of the proposed amendments.

STATEMENT IN LIEU OF JOB IMPACT STATEMENT

A Job Impact Statement for these amendments is not being submitted because the New York State Department of Health has determined that these regulatory changes will not have a substantial adverse impact on jobs and employment, based upon its nature and purpose.

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 in some cases only 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 to serve as the qualified executive responsible for the organization'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.

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 access; identify and assess risk for operational technology and nonpublic information handling; monitor and log network activity for water systems serving a population of greater than 50,000; 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.

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

EXPRESS TERMS

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 medium or large water systems, 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.

(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 to the department within 48 hours of identification.

(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 are not under the direct control of the covered water system and 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 the normal operations of the covered water system that affects the ability of the covered water system to comply with the requirements of this Subpart;

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

(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 cybersecurity events 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;

(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 permittee's treatment facility.

(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 qualified through training and experience to serve as the water system's qualified executive responsible for the system's cybersecurity program.

(1) The name and contact information for the qualified executive 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 qualified executive responsible for the cybersecurity program of each covered water system 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 cybersecurity events in 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(a) 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 designated qualified executive responsible for the oversight of 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 shall be reported to the department within 48 hours of identification.

(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 covered water system's qualified executive responsible for the organization'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(a) 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, consistent with the principle of least privilege:

(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 qualified executive responsible for the organization'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 qualified executive responsible for the organization's cybersecurity program designated in accordance with section 5-E.4 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 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 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. Such logs shall be preserved for a period of three years and shall be made available to the department on demand. 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. 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 Objective

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) 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; train certified water operations staff on cybersecurity hygiene; 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 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 a qualified executive to implement a 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 3,300 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 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 a qualified executive to be responsible for the organization'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 1 full-time equivalent will be required. It is expected that this position will require approximately $175,000 per year inclusive of salary, fringe 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 a qualified executive 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 and to report cybersecurity incidents within 24 hours, 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, community water systems that serve more than 3,300 people will be required to: conduct a cybersecurity vulnerability analysis (CVA) 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; train certified water operations staff on cybersecurity hygiene; 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 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 a qualified executive to implement a cybersecurity program and monitor and log network activities in order to detect cybersecurity incidents.

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 to serve as the water system's qualified executive responsible for the organization'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 a qualified executive to be responsible for the organization'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 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 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	Reporting,
Monroe County			

Recordkeeping and Other Compliance Requirements; and Professional Services

Water systems that serve more than 50,000 people must designate an individual qualified in training, experience, and expertise, to serve as the water system's qualified executive responsible for the organization'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. The Department anticipates the one-year implementation time frame included in the proposed rule 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.

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 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, 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 greater than 50,000 will also be required to designate a qualified executive to be responsible for the organization'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/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.