**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.