6 NYCRR PART 750 CYBERSECURITY AMENDMENTS

750-1.2(a) Definitions is amended to include:

(25) Cyber asset inventory means an inventory of:

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

(ii) information technology assets that are:

('a') physically or logically connected to operational technology; or

('b') the system of record for SPDES program data.

(26) Cybersecurity event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse the permittee's operational or information technology or SPDES program data.

(27) Cybersecurity incident means a cybersecurity event that, directly or indirectly:

(i) has an adverse impact on the normal operations of the permittee's sewer system or treatment facility;

(ii) has a reasonable likelihood of harming any part of the normal operations of the permittee's sewer system or treatment facility;

(iii) compromises the confidentiality, integrity, or availability of SPDES program data or results in loss or damage to the permittee's sewer system or treatment facility; or

(iv) delays or prevents the permittee from complying with all provisions of its SPDES permit.

(52) Information technology means hardware, software, systems, or devices, used for collection, storage, processing, use, dissemination, sharing, or disposition of data for business, administrative, or informational purposes.

(53) Least privilege means the principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.

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

(i) something the user knows; or

(ii) something the user has; or

(iii) something the user is

(65) Operational technology means hardware, software, and firmware used to detect or cause changes in, or manage devices 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 or sewer system.

(94) SPDES program data means all current or historical electronic information needed to comply with any reporting requirements pursuant to this Part and/or with any SPDES permit.

750-1.25 References is amended to add:

(j) EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems,EPA 817-B-23-001 (August 2024).

(k) Wastewater Utility Emergency Response Plan: Template and Instructions, EPA 817-B-21-

003 (July 2021).

(l) Incident Action Checklist – Cybersecurity, EPA 810-B-17-004 (February 2021).

(m) Guide to Operational Technology (OT) Security, NIST SP 800-82r3 (September 2023).

(n) Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-

53 (December 10, 2020).

(o) Drinking Water and Wastewater Systems Cybersecurity Incident Response Plan Template Instructions (April 2025)

750-2.7 Incident reporting and notification requirements is amended to add a new subdivision (h):

(h) Reporting of cybersecurity incidents:

(1) The permittee shall report orally, to the regional water engineer, any cybersecurity incident, as soon as possible, but no later than 24 hours from the time the permittee

becomes aware of the cybersecurity incident. The oral report shall include, to the extent known by the permittee at the time of the report, all the information required by subparagraphs 750-2.7(h)(2)(i) through (viii) of this section.

(2) The permittee shall also provide a written report of any cybersecurity incidents to the regional water engineer within 30 days from the time the permittee becomes aware of the cybersecurity incident. The written report shall include:

(i) the date and time of discovery of the cybersecurity incident;

(ii) the person who discovered the cybersecurity incident;

(iii) a brief description of the cybersecurity incident;

(iv) whether the cybersecurity incident impacted information technology, operational technology, or both;

(v) a description of how normal operations of the permittee's sewersystem or treatment facility were or may be disrupted, or a statement that there was no disruption, and no disruption is anticipated;

(vi) a description of the expected duration or end time of any disruption identified under subparagraph (v) of this paragraph, if known;

(vii) a description of any loss of or damage, or a statement that there is no loss of or damage, to:

('a') the confidentiality, integrity, or availability of the permittee's SPDES program data;

('b') the permittee's operational technology; and;

('c') the permittee's sewer system or treatment facility; and

(viii) a brief description of the measures taken, and/or planned, to remediate or mitigate any disruption, loss, or damage described under subparagraphs (v) and/or (vii) of this paragraph;

(3) The permittee shall comply with all other reporting and notification requirements under section 750-2.7 of this Subpart.

750-2.9 Additional conditions applicable to a publicly owned treatment works (POTW) is amended to add new subdivision (d):

(d) Emergency Response Plan:

(1) The POTW shall establish, maintain, and implement, or cause to be established, maintained, and implemented, a written Emergency Response Plan (ERP) using:

(i) a plan, existing prior to effective date of this subdivision, that:

('a') describes the POTW's strategies, resources, plans, and procedures to prepare for, and respond to, a natural or human-made incident, that threatens health, safety, property, or the environment; and;

('b') includes titles and contact information for persons with responsibilities in the ERP referenced in subparagraph (i) of this paragraph; or;

(ii) the Wastewater Utility Emergency Response Plan: Template and Instructions (see section 750-1.25 of this Part).

(2) The POTW shall update the ERP, required by paragraph (1) of this subdivision, within 30 days of changes to the titles and contact information in the ERP.

(3) The POTW shall ensure that printed copies of the ERP, required by paragraph (1) of this subdivision, are:

(i) in secure locations, both on and off the POTW premises; and

(ii) accessible only to appropriate persons, in accordance with the access control rules and/or procedures established pursuant to subclause 2.9(e)(1)(i)('a')('4') of this Subpart.

(4) Annually, by March 28, the POTW shall certify to the department that the POTW is complying with the requirements of paragraphs (1), (2), and (3) of this subdivision.

750-2.9 Additional conditions applicable to a publicly owned treatment works (POTW) is amended to add a new subdivision (e):

(e) Cybersecurity:

(1) Using the cybersecurity documents accepted by the department in paragraph (4) of this subdivision, the POTW shall establish, maintain, and implement or cause to be established, maintained, and implemented:

(i) Written rules and/or procedures for access control and authentication that:

('a') consistent with the principle of least privilege, control access to:

('1') operational technology;

('2') SPDES Program Data;

('3') information technology that may directly or indirectly allow access to operational technology or SPDES Program Data; and

('4') the Emergency Response Plan required by subdivision 750-2.9(d) of this Subpart;

('b') address password security, complexity, and management;

('c') require multi-factor authentication for remote access to operational technology that is allowed under the access control rules and/or procedures;

('d') disallow use of preset or default credentials;

('e') are reviewed at least annually, by March 28; and

('f') are updated within 90 days after a:

('1') cybersecurity incident; or

('2') cybersecurity assessment or audit.

(ii) A written cybersecurity vulnerability management process that:

('a') includes a cyber asset inventory;

('b') identifies which assets, included within the cyber asset inventory, developed pursuant to clause (‘a’) of this subparagraph, can be accessed remotely;

('c') identifies known cybersecurity vulnerabilities in assets included within the cyber asset inventory developed pursuant to clause (‘a’) of this subparagraph;

('d') assesses the risks of the known cybersecurity vulnerabilities, identified pursuant to clause (‘c’) of this subparagraph, based on the likelihood that the vulnerability will be exploited and the consequences to the POTW’s normal operations that could occur if the vulnerability were exploited;

('e') prioritizes the cybersecurity vulnerabilities according to the risks identified pursuant to clause (‘d’) of this subparagraph;

('f') mitigates and/or remediates cybersecurity vulnerabilities according to the priority established pursuant to clause (‘e’) of this subparagraph;

('g') is reviewed at least annually, by March 28; and

('h') is updated when:

('1') assets within the cyber asset inventory, developed pursuant to clause (‘a’) of this subparagraph, are added or decommissioned; or

('2') a new cybersecurity vulnerability is identified for an asset within the cyber asset inventory developed pursuant to clause (‘a’) of this subparagraph.

(iii) A written description of network structure that protects operational technology by:

(‘a’) physically and logically separating it from information technology and external networks; or

(‘b’) securing necessary connections by using appropriate cybersecurity controls

referenced in the cybersecurity documents accepted by the department pursuant to paragraph (4) of this subdivision.

(2) POTWs, with a design flow greater than or equal to 10 million gallons per day (MGD), shall implement, manage, and maintain, or cause to be implemented, managed, and maintained, procedures, products, and/or services that monitor and log the POTW’s network activity.

(i) Paragraph (2) of this subdivision does not apply where the POTW either:

('a') has neither physical nor logical connections between operational technology and either:

('1') information technology; or

('2') external networks; or

('b') 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:

('1') information technology; or

('2') external networks.

(3) The POTW shall:

(i) establish, maintain, and implement, or cause to be established, maintained, and implemented, a cybersecurity incident response plan (IRP) using:

('a') a plan, existing prior to the effective date of this subdivision, that describes the POTW's strategies, resources, plans, and procedures to prepare for, and respond to, a cybersecurity incident; or

('b') one of the following:

('1') the Incident Action Checklist—Cybersecurity (see section 750-1.25 of this Part); or

('2') Drinking Water and Wastewater Systems Cybersecurity Incident Response Plan Template Instructions (see section 750-1.25 of this Part).

(ii) incorporate the IRP into the ERP required by paragraph 750-2.9(d)(1) of this Subpart.

(4) The following cybersecurity documents are accepted by the department (see section 750-1.25(j)-(o) of this Part):

(i) EPA Guidance on Improving Cybersecurity at Drinking Water and WastewaterSystems.

(ii) Wastewater Utility Emergency Response Plan: Template and Instructions.

(iii) Incident Action Checklist – Cybersecurity.

(iv) Guide to Operational Technology (OT) Security.

(v) Security and Privacy Controls for Information Systems and Organizations.

(vi) Drinking Water and Wastewater Systems Cybersecurity Incident Response Plan Template Instructions.

(5) Annually, by March 28, the municipality shall certify to the department that the municipality is complying with the provisions of paragraphs (1) through (3) of this subdivision.

750-2.9 Additional conditions applicable to a publicly owned treatment works (POTW) is amended to add a new subdivision (f):

(f) Certification

(1) Certifications, required pursuant to subdivisions (d) through (f) of this section, shall be filed on forms supplied to the POTW by the department, substitute forms approved by the department, or by the electronic transfer of data as approved by the department. Electronic submissions shall conform to the format, standards and other conditions specified by the department.

(2) Certifications, required pursuant to subdivisions (d) through (f) of this section, shall be signed by the principal executive officer or ranking elected official of any municipality subject to this section, or by a duly authorized representative of that person. A person is a duly authorized representative under this section only if:

(i) the authorization is made in writing by the principal executive officer or ranking elected official of any municipality subject to this section;

(ii) the authorization specifies an executive-level municipal official having responsibility for oversight of information technology, operational technology, or cybersecurity functions (a duly authorized representative may be either a named individual or any individual occupying a named position); and

(iii) the written authorization is submitted to the department.

(3) Any person signing a certification pursuant to this section shall make the following certification:

"I certify, under penalty of law, that this document and all attachments were prepared under

my direction or supervision in accordance with a system designed to assure that qualified personnel properly gather and evaluate the information submitted. Based on my inquiry of the person or persons who manage the system, or those persons directly responsible for gathering the information, the information submitted is, to the best of my knowledge and belief, true, accurate, and complete. I am aware that there are significant penalties for submitting false information, including the possibility of fine and imprisonment for knowing violations."