Water and Wastewater SCADA Assessment Planning Pack

Edition November 18, 2026

New York water summaries, PSC test acceptance and the PSC adoption source were checked on November 18, 2026. Unrelated authorities retain their earlier verification dates.

For security, engineering and compliance teams at drinking water and wastewater utilities. Use it to confirm which cybersecurity rules apply, name the evidence owners and agree the methods before an assessment starts.

Fill in the worksheets by hand or copy them into your own records.

America’s Water Infrastructure Act

Section 2013 of AWIA, which amended Section 1433 of the Safe Drinking Water Act, requires community water systems serving more than 3,300 people to complete a risk and resilience assessment and an emergency response plan, certify them to EPA and review them at least every five years. The assessment covers the electronic, computer and automated systems the utility relies on, so the SCADA and process control network belong in it. The certification applies to drinking water systems; the wastewater rules come from the states and are covered below.

Certification dates in the current five year cycle

EPA lists these deadlines, which assume the risk and resilience assessment was certified on its final due date. The emergency response plan certification is due six months after the date the assessment is certified, so an early assessment moves the plan date earlier.

Population served	Risk and resilience assessment	Emergency response plan
100,000 or more	March 31, 2025	September 30, 2025
50,000 to 99,999	December 31, 2025	June 30, 2026
3,301 to 49,999	June 30, 2026	December 31, 2026

New York Drinking Water and Wastewater Rules

New York adopted cybersecurity rules for both drinking water and wastewater in March 2026.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Confirm drinking water scope and duties

Begin with the system type, public water system identifier or SPDES permit, population served, combined wholesale and retail population, ownership and treatment design flow. Appendix 5-E generally covers community drinking water systems serving more than 3,300 people. Its personnel and network logging provisions use a combined wholesale and retail population greater than 50,000. All Subpart 5-4 certified drinking water treatment operators have the training duty, regardless of system size. Examine each exclusion against the actual architecture; an exclusion can leave incident reporting and response planning duties in place.

The remaining Appendix 5-E requirements have a January 1, 2027 compliance date; operator training and incident reporting took effect on adoption on March 11, 2026. Complete the cybersecurity vulnerability analysis using the DOH approved form, obtain the required approval and incorporate its findings into the emergency plan. Review and update the analysis at least annually and within 30 days after major water facility infrastructure changes become operational. The cybersecurity program follows those findings. Use the detailed Water requirements and Water tests records to examine each applicable program provision separately.

Personnel and program certification

For a covered system serving a combined wholesale and retail population greater than 50,000, subject to applicable exclusions, the owner designates a person with demonstrable cybersecurity knowledge and practical system protection or risk management experience. Section 5-E.4 does not require a professional cybersecurity certification. Record the designation, qualifications and contact in the emergency plan. That person reports confidentially to the governing body at least annually and submits the separate program compliance certification required by 5-E.6(b) with the emergency plan submission.

DOH vulnerability and incident reports

For a covered system, report to DOH as soon as possible and no later than 24 hours after determining that a cybersecurity incident as defined in 5-E.3(e) has occurred which has created or may create a public health hazard. Separately, vulnerabilities identified in the cybersecurity vulnerability analysis that may affect compliance with Subpart 5-1, or any situation that may pose a public health risk, must be reported within 48 hours of identification under 5-E.1(c)(2) and 5-E.5(e). Record each qualifying condition, its timestamp and the receipt. Other applicable State and Federal notices retain their own triggers.

Significant deficiency response

When the State notifies the system of a significant deficiency, consult the State within 30 days. Within 120 days of that notification, or an earlier period directed by the State because of a public health threat, correct the deficiency or comply with the applicable corrective action plan under 5-1.71(c) and (d). Opening a work ticket does not establish that condition. Keep the approved schedule, progress and completion evidence together. Public health hazards require the State directed or approved action and the applicable Tier 1 public notice.

© 2026 Global Digital Forensics, Inc. All rights reserved.

DEC incident reporting

All SPDES permittees, public or private, report a cybersecurity incident meeting 750-1.2(a)(27) to the Regional Water Engineer orally as soon as possible and no later than 24 hours after becoming aware of it, followed by the written report within 30 days of awareness under 750-2.7(h). These duties took effect March 26, 2026. Current DEC instructions require the initial online incident report followed immediately by oral notification to the regional water engineer or manager; use DEC Dispatch if the regional contact cannot be reached. Record awareness, the affected operations or SPDES data, notification times, the written report and receipts separately from the DOH and PSC records.

POTW controls, planning and certification

Publicly owned treatment works must meet the cybersecurity control and emergency response plan requirements in 750-2.9(d) and (e) by March 11, 2027. The first annual certifications are due March 28, 2027. Network monitoring and logging under 750-2.9(e)(2) applies at a design flow of at least 10 million gallons per day, with the rule's exceptions for no physical or logical OT connections to IT or external networks, or solely devices capable only of one way traffic from OT. Other POTW duties still require their own assessment. Use the incorporated documents and specified editions listed in the rule, alongside separately identified guidance.

The municipal principal executive officer or ranking elected official signs the certifications, or a duly authorized executive level municipal official with the required oversight signs under the rule's written authorization provisions. Submit that authorization to DEC. A consultant's engagement does not itself confer filing authority. Retain the evidence supporting the signed certifications and the annual filing receipts.

Public Service Commission

Screen PSC Part 1200 separately against the utility entity and exact service connection definitions. Its information technology requirements and qualifying incident notices have their own scope, transitions and clocks. Population for DOH is not the PSC service connection count.

New Jersey Water Quality Accountability Act

The Water Quality Accountability Act, as amended by P.L.2021, c.262, applies to every water purveyor that owns a public community water system with more than 500 service connections.

What the Act requires

The purveyor maintains a cybersecurity program that applies to all of the system’s industrial control systems and reasonably conforms to the NIST Cybersecurity Framework, the CIS Critical Security Controls or the ISO/IEC 27000 family. It joins the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) and reports a cybersecurity incident to NJCCIC promptly after an employee is made aware of it. No later than 30 days after receiving that report, NJCCIC has the purveyor’s cybersecurity program and incident response audited by a qualified, independent cybersecurity company at the purveyor’s expense.

Board of Public Utilities

Utilities regulated by the Board of Public Utilities also report to the Board within six hours of becoming aware of a cyber attack resulting in outages or service issues, a confirmed breach or intrusion, or an attempted intrusion that slows or disrupts service, under N.J.A.C. 14:3-6.7(a)6 and 7.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Evidence Checklist

For each item, name the owner, the record that exists today, its date and what is still missing.

Item	What to gather
Operating dependency	The treatment or distribution function, its process owner and the effect of losing control or visibility, with observed facts kept apart from assumed consequences.
Vendor access	The account owner, approval, access group, permitted equipment, revocation procedure and session records.
IT and OT boundary	Current diagrams and the approved firewall and jump host configuration, with their dates and any mismatch with what the engineers know.
Legacy systems	Supported versions, operating constraints, compensating controls and configuration backups, with patching and scanning decisions set by engineering.
Monitoring and time	Log sources, time synchronization, retention and the person authorized to preserve the logs.
Recovery dependency	Controller and server configurations, software, licensing, spares, vendor support and restoration records, with untested recovery assumptions marked.
AWIA connection	The risk scenario, response action and restoration dependency the cyber evidence supports, and the owner who carries it into the assessment and plan.
State reporting	The incident reporting contacts and clocks for the Department of Health, DEC, the PSC, NJCCIC or the BPU that apply to the utility.

Illustrative Finding

A fictional example showing how a well documented finding is written.

Observed condition

A vendor support account belongs to an access group whose recorded policy reaches more control zone destinations than the documented support task needs.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Source evidence

Dated access approval, identity group membership, jump host policy and firewall configuration, each tied to the system owner and the date it was reviewed.

Operating consequence

If the account were compromised, an attacker could reach additional assets that support the process. Confirming that path needs an approved reachability check and the engineers' view of the operating dependencies.

Basis of the finding

The finding rests on dated configuration records; an approved reachability check confirms it in the live environment.

Corrective work

The operator assigns an owner to narrow the access to the support task, review revocation and session records, and agree the change with the equipment vendor and engineering team.

Verification

Agree the method, targets, maintenance dependency, stop authority and evidence needed to verify the corrected boundary, and track recommended, implemented and verified states separately.

Assessment Scope Worksheet

Use broad descriptions here and keep sensitive system details in your controlled records.

Operating process and boundary

Operations, engineering and security owners

Applicable program, requirement and evidence owner

Available records, their dates and gaps

© 2026 Global Digital Forensics, Inc. All rights reserved.

Approved passive methods and proposed active validation

Excluded systems, commands and actions

Operating window, stop authority and communications

Recovery arrangements and open dependencies

Corrective Action Worksheet

Record one action per copy, and keep implementation and verification evidence separate.

Finding, evidence reference and operating consequence

Corrective owner, dependency and target date

Status: recommended, implemented or verified, with supporting evidence

Verification method, result and date

Sources

Sources checked November 3, 2026.

© 2026 Global Digital Forensics, Inc. All rights reserved.

EPA

AWIA Section 2013 requirements and deadlines: https://www.epa.gov/waterresilience/awia-section-2013

New York State Department of Health

Cybersecurity requirements table for drinking water systems: https://healthweb-back.health.ny.gov/environmental/emergency/water/drinking/cybersecurity/cybersecurity_requirements_table.htm

New York State DEC

Wastewater cybersecurity resources: https://dec.ny.gov/environmental-protection/water/water-quality/wastewater-treatment-resources/wastewater-cybersecurity-resources

New Jersey Legislature

P.L.2021, c.262, Water Quality Accountability Act amendments: https://pub.njleg.gov/bills/2020/PL21/262_.HTM

New Jersey Register

54 N.J.R. 1612 (August 15, 2022), adopted amendments to N.J.A.C. 14:3-6.7, published by the Office of Administrative Law

New York Public Service Commission

Case 25-M-0302, order adopting 16 NYCRR Part 1200 (April 16, 2026), and the announcement: https://dps.ny.gov/node/29056

NIST

SP 800-82 Revision 3, Guide to Operational Technology Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final

New York water execution records

Use Water requirements for one record per duty, Water tests for the criterion and safe examination procedure, Water reporting for the separate clocks, and Water calendar for recurring work. Establish applicability before assigning a conclusion. Each result names its evidence, examiner, operating permission and reviewer. A completed record leads to a supported finding, corrective work and a separate retest. The New York water toolkit includes manager, operator and governing board guidance and two completed fictional examples.

Open https://evestigate.com/resources/ny-water-cybersecurity-toolkit/

Source	Exact locator	Link
NYDOH-APP5E	Sections 5-E.1 through 5-E.11	https://healthweb-back.health.ny.gov/regulations/nycrr/title_10/part_5/docs/appendix_5e.pdf

© 2026 Global Digital Forensics, Inc. All rights reserved.

Source	Exact locator	Link
NYDOH-SUBPART51	Sections 5-1.33, 5-1.71 and 5-1.77; agency compilation revised October 8, 2026	https://healthweb-back.health.ny.gov/regulations/nycrr/title_10/part_5/docs/subpart_5-1.pdf
NYDEC-750-2026	750-1.2(a), 750-1.25(j) through (o), 750-2.7(h), 750-2.9(d) through (f)	https://dec.ny.gov/sites/default/files/2026-03/6nycrr_part750_et_rev.pdf
NYDEC-COMPENDIUM	Pages 2 through 24 and regulatory appendices	https://dec.ny.gov/sites/default/files/2026-03/wastewatercyber_compendium.pdf
NYDEC-IMPLEMENTATION	Effective dates, applicability, reporting, plans, training and annual certification questions	https://dec.ny.gov/environmental-protection/water/water-quality/wastewater-treatment-resources/wastewater-cybersecurity-resources

Talk to a Senior OT Assessor

Global Digital Forensics plans OT assessments with the utility’s operations and engineering owners around physical safety and the real architecture, and maps the findings to the AWIA assessment and the state rules the compliance lead must answer. On the first call we review this checklist with your plant engineer and agree what can be examined safely.

© 2026 Global Digital Forensics, Inc. All rights reserved.