GLOBAL DIGITAL FORENSICS

Water and Wastewater SCADA Assessment Planning Pack

AWIA, New York and New Jersey cybersecurity requirements and the evidence to gather before an OT assessment

Edition 2026-11-03 | November 3, 2026

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.

Questions about this document: call (800) 868-8189 or write to info@evestigate.com.

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

Contents

1. America’s Water Infrastructure Act
2. New York Drinking Water and Wastewater Rules
3. New Jersey Water Quality Accountability Act
4. Evidence Checklist
5. Illustrative Finding
6. Assessment Scope Worksheet
7. Corrective Action Worksheet
8. Sources

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

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.

Department of Health, 10 NYCRR Subpart 5-1, Appendix 5-E

Appendix 5-E applies to community water systems serving more than 3,300 people. Two duties took effect on adoption, March 11, 2026: certified operators complete one hour of cybersecurity training every three years (5-E.7), and a covered system notifies the Department of Health of a cybersecurity incident within 24 hours of identifying it (5-E.9). From January 1, 2027, the system also reports an identified vulnerability within 48 hours and maintains its annual cybersecurity vulnerability analysis and its cybersecurity program. Systems serving more than 50,000 people have additional certification duties.

Department of Environmental Conservation, 6 NYCRR Part 750

Every SPDES permittee, public or private, must report a cybersecurity incident to the Regional Water Engineer by phone within 24 hours of becoming aware of it and in writing within 30 days, under 6 NYCRR 750-2.7(h), effective March 26, 2026. Publicly owned treatment works must meet the cybersecurity control and emergency response plan requirements of 750-2.9(d) and (e) by March 11, 2027; network monitoring and logging applies to plants with a design flow of 10 million gallons per day or more. The first annual certification is due March 28, 2027 through DEC’s nForm platform.

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

Public Service Commission

Water utilities regulated by the Public Service Commission with 50,001 or more service connections also fall under the Commission's utility cybersecurity rules, 16 NYCRR Part 1200, effective June 1, 2026. Those rules cover information technology rather than OT and require notice of a qualifying incident within 72 hours.

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.

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.

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

Item	What to gather
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.

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

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

Applicable program, requirement and evidence owner

Available records, their dates and gaps

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

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

Sources

Sources checked November 3, 2026.

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

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

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.

Get a free consultation. The initial consultation is free, and requests are handled in confidence.

Call (800) 868-8189 at any hour, or write to info@evestigate.com.

Request a consultation online at evestigate.com/contact.

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