CYBERSECURITY PROGRAM CERTIFICATION TEMPLATE

Version: February 05, 2026

New York State Department of Health
Bureau of Water Supply Protection

INTRODUCTION

10 NYCRR Part 5, Subpart 5-1 requires suppliers of water to ensure that public water systems are properly supervised, operated, and protected to prevent public health hazards. Conditions that pose an obvious risk to public health include cybersecurity vulnerabilities and cyber-attacks that may compromise the treatment, storage, monitoring, or distribution of potable water. The addition of Appendix 5-E to Subpart 5-1 establishes a required cybersecurity certification for community water systems serving a combined wholesale and retail population of more than 50,000 people. This certification documents a community water system's review of cybersecurity risks and attests to the implementation and maintenance of reasonable and appropriate safeguards to protect public water system operations.

PURPOSE

The purpose of this document is to provide a standardized template for the cybersecurity certification required under Appendix 5-E. This template identifies the minimum elements necessary to demonstrate that a community water system has:

- Developed a cybersecurity program in accordance with Appendix 5-E, Section 5-E.6;
- Conducted an annual review of cybersecurity vulnerabilities; and
- Addressed cybersecurity conditions that could pose a public health hazard or constitute a significant deficiency.

The format of this template may be modified as necessary to reflect system size, complexity and operational structure provided all required elements of Appendix 5-E are included.

AUDIENCE

This template is intended for use by community water system owners:

1. Suppliers of water who service populations greater than 50,000, as defined by 10 NYCRR Subpart 5-1; and
2. Designated individuals responsible for cybersecurity, Supervisory Control and Data Acquisition (SCADA) policies, information technology or operational technology supporting public water systems.

DISCLAIMER

This template represents the minimum required content for a cybersecurity certification pursuant to Appendix 5-E. Each community water system is unique and additional internal documentation, controls, or procedures may be necessary based on system specific risks.

NOTE: Bracketed text throughout this document is instructional and does not need to be included in the final certification.

Cybersecurity Program Certification Checklist

[Instructions: Use this checklist to assess completeness of the certification required by Appendix 5-E.]

☐ Public Water System Identification

☐ System Location and Ownership

☐ Authorized Certifier Information

☐ Date of Certification

☐ Identification of Cyber Relevant System Components

☐ Cybersecurity Program and Controls Attestation

☐ Cybersecurity Reviews or Assessments

☐ Identified Vulnerabilities and Corrective Actions

☐ Cybersecurity Incidents or Events

☐ Final Certification and Signature

This page was intentionally left blank.

Cybersecurity Program Certification

10 NYCRR, Part 5, Subpart 5-1, Appendix 5-E

Prepared for:

Prepared by:

Effective Date:

Version:

Contents

Section 1: Public Water System Information

Public water System Identification

Public Water System Name:
PWS ID Number:
System Type:
Population Served:
Street Address:
City/Town/Village:
County:

System's Designated Individual Information

Company or Organization Name:
Point of Contact Name:
Title:
Phone (Office):
Phone (Mobile):
Email Address:
Street Address:
City, State, ZIP Code:

Date of Certification

Date:

Cyber-Relevant System Information

[*Indicate which systems are applicable*]

☐ Treatment Process Control Systems

☐ Supervisory Control and Data Acquisition (SCADA) or Industrial Control Systems

☐ Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), or Field Devices

☐ Operator Workstations or Human Machine Interfaces

☐ Remote Access Technologies

☐ Business or Administrative Information Technology (IT) systems Supporting Operations

☐ Data Storage, Monitoring or Reporting Systems

Other Cyber Relevant System Information

[*Optional narrative to supplement Section 1 information.*]

Section 2: Cybersecurity Program and Controls

Does a cybersecurity program, policy or set of cybersecurity controls exist for this community water system?

☐ Yes

☐ No

The undersigned attests that cybersecurity controls appropriate to the system have been implemented and maintained during the certification period consistent with the requirements of Appendix 5-E.

☐Cybersecurity controls consider the system's size, complexity and operational role.

Summary of Deviations

[*Describe any deviations from established cybersecurity policies or controls required under Appendix 5-E including the justification.*]

Section 3: Cybersecurity Assessments and Reviews

1. Was an annual cybersecurity vulnerability analysis conducted or reviewed during the certification period?
   ☐Yes
   ☐No

2. Date(s) the most recent cybersecurity vulnerability analysis was reviewed or conducted:

Date:

3. Who conducted or oversaw the cybersecurity review?
   ☐System Owner or Designated Individual
   ☐Certified Operator
   ☐Municipal Staff
   ☐Consultant or Contractor
   ☐Other (describe):

4. Did the cybersecurity review include systems that support treatment, storage, or distribution of potable water?
   ☐Yes
   ☐No
   ☐N/A

5. Which of the following system areas were included in the review?
   ☐ Operational Technology
   ☐ Supervisory Control and Data Acquisition (SCADA) or Industrial Control Systems
   ☐ Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) or Field Devices
   ☐ Operator Workstations or Human Machine Interfaces
   ☐ Remote Access to Operational Systems
   ☐ Business or Administrative System Supporting Operations
   ☐ Backup and Recovery Capabilities

6. Were any cybersecurity-related vulnerabilities or concerns identified during the review?
   ☐Yes
   ☐No

7. If yes, did any identified vulnerability pose a potential risk to system operations or public health as per Section 5-E.5(e)?
   ☐Yes
   ☐ No

8. Were corrective actions identified or implemented in response to the review findings?

   ☐ Yes
   ☐ No
   ☐ N/A

9. If corrective actions were identified, what is their status?

   ☐ Completed
   ☐ In Progress
   ☐ Planned
   ☐ Not Required

10. Is documentation of the cybersecurity vulnerability analysis, or review and any corrective actions, retained by the water supply?

    ☐ Yes
    ☐ No

11. Is such documentation available for review upon request by the Department?

    ☐ Yes
    ☐ No

Additional Narrative (optional)

[*Describe any additional explanation as necessary to clarify responses above.*]

Section 5: Certification

By signing below, I attest that:

- The information contained in this document is true and accurate to the best of my knowledge.
- A cybersecurity review has been conducted in accordance with Appendix 5-E;
- Cybersecurity vulnerabilities that could pose a public health hazard or constitute a significant deficiency have been addressed or are being addressed; and
- I am authorized to submit this certification on behalf of the covered water system.

Certifier Printed Name:
Title:
Company:
Signature:
Date: