Maryland Department of the Environment Guidance to Community Water and Sewerage Systems on Senate Bill 871 (SB0871: Cybersecurity Planning and Assessments)

Compliance Checklist for SB0817 Cybersecurity Requirements

All Community Water and Sewerage Systems

- ☐ ***Notify MDE of Cybersecurity Point of Contact (water.cyber@maryland.gov)***
- ☐ ***Conduct Annual Cybersecurity Training (MDE/EPA/CISA resources)***
- ☐ ***Complete Cybersecurity Awareness Training for New/Renewing Water Operator Licenses (EPA's Cybersecurity Training)***
- ☐ ***Report Cybersecurity Incidents to State Security Operations Center (website/soc@maryland.gov/410-697-9700)***
- ☐ ***Revise Emergency Response Plans to Address Cybersecurity Incidents (utility plan)***
  - ***On or before July 1, 2026, and every 2 years thereafter***

Additional Requirements for Community Water and Sewerage Systems Serving Over 3,300 Customers

- ☐ ***Adopt Maryland Cybersecurity Standards Contained in DoIT Policy Suite (DoIT website)***
- ☐ ***Commit to Adopting a Zero-Trust Cybersecurity Approach (CISA website)***
- ☐ ***Conduct a Cybersecurity Program Maturity Assessment (MDE/DoIT Tool)***
  - ***On or before July 1, 2026, and every 2 years thereafter***
- ☐ ***Submit Completed Cybersecurity Maturity Assessment and Certification Statement to MDE/DoIT by Established Deadlines (MDE/DoIT secure website/email)***

MDE – Maryland Department of the Environment; DoIT – Department of Information Technology; EPA – Environmental Protection Agency; CISA – Cybersecurity and Infrastructure Security Agency

Maryland Department of the Environment Guidance to Community Water and Sewerage Systems on Senate Bill 871 (SB0871: Cybersecurity Planning and Assessments)

1.0 Introduction

This guidance document provides an overview of the regulatory requirements established under SB0871, *Community Water and Sewerage System - Cybersecurity Planning and Assessments*, and outlines expectations for achieving and maintaining compliance. Its purpose is to support consistent understanding, interpretation, and implementation of cybersecurity requirements by translating regulatory obligations into practical, actionable guidance. The document is intended for use by water utility management, compliance personnel, and operational staff responsible for information technology (IT), operational technology (OT), and emergency preparedness. While this guidance does not replace statute or regulation, it is intended to clarify how regulated systems can align their policies, procedures, and practices with Maryland cybersecurity expectations.

Where applicable, this guidance also identifies relevant State and federal partners, tools, and resources that utilities may use to support compliance efforts.

2.0 Planning & Implementation

This guidance supports community water and sewerage systems in implementing SB0871 for cybersecurity preparedness, which relies on coordination across multiple local, State and federal agencies. At the State level, systems should be prepared to coordinate with the Maryland Department of the Environment (MDE), the Department of Information Technology (DoIT), the State Security Operations Center (SSOC), the Maryland Department of Emergency Management (MDEM), and local emergency managers. At the federal level, utilities are encouraged to leverage guidance, alerts, and tools provided by the Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and related water sector-specific partners.

3.0 Cybersecurity Point of Contact

☐ ***Notify MDE of Cybersecurity Point of Contact (water.cyber@maryland.gov)***

All community water and community sewerage systems are required to appoint a primary point of contact (POC) for cybersecurity. The water system cybersecurity POC is responsible for serving as a liaison with MDE, DoIT, SSOC, MDEM, and local emergency management agencies on cybersecurity-related issues. The cybersecurity POC name, title, phone number, and email address should be documented and communicated to relevant stakeholders, included in emergency response and incident response documents, and kept current. Updates to the cybersecurity POC personnel assignment or contact information should be made promptly and MDE must be notified of any changes.

Cybersecurity POCs are responsible for submitting required cybersecurity incident reports, coordinating compliance with Maryland cybersecurity requirements, and facilitating communications during incidents. To ensure timely awareness of threats and vulnerabilities, cybersecurity POCs are expected to enroll in the following free cybersecurity information-sharing and alerting services:

- Maryland Information Sharing and Analysis Center (MD-ISAC)
- Cybersecurity & Infrastructure Security Agency Alerts

MDE recommends that utilities include links and instructions within internal documents to support enrollment and ongoing participation in these programs.

4.0 Cybersecurity Training and Exercises

☐ ***Conduct Annual Cybersecurity Training (MDE/EPA/CISA resources)***

All community water and community sewerage systems are required to attend annual training to improve cybersecurity awareness. The water system cybersecurity POC or their designee should monitor and track staff training completion and retain records to demonstrate compliance. Training should be appropriate to staff roles and address topics such as phishing awareness, incident reporting, basic cyber hygiene, and OT-specific risks where applicable.

Training and exercises may be discussion-based (seminars, workshops, tabletops, games) to familiarize personnel with cybersecurity plans and policies, or operations-based (drills, functional, full-scale) to validate existing cybersecurity plans by enacting real-time responses, identifying resource gaps, and clarifying roles and responsibilities.

Below is a list of free water sector cybersecurity training resources.

- EPA Cybersecurity Exercises and Technical Assistance Courses
- CISA Cybersecurity Awareness & Training
- MassDEP Basic Cybersecurity Measures for Water and Wastewater Systems in Massachusetts
- Idaho National Laboratory Industrial Control Systems Cybersecurity Training
- AWWA Cybersecurity Micro-Learning

5.0 Cybersecurity Awareness Component for New and Renewing Operator Certification

☐ ***Complete Cybersecurity Awareness Training for New/Renewing Water Operator Licenses (EPA's Cybersecurity Training)***

Effective July 1, 2025, all Maryland water and wastewater operators must complete EPA's Cybersecurity Training for Water and Wastewater Systems as a mandatory requirement for license renewal. Additional information can be found on the MDE Cybersecurity Website or the Board of Waterworks and Waste System Operators page.

6.0 Enhanced Requirements

☐ ***Adopt Maryland Cybersecurity Standards Contained in DoIT Policy Suite (DoIT website)***

☐ ***Commit to Adopting a Zero-Trust Cybersecurity Approach (CISA website)***

☐ ***Conduct a Cybersecurity Program Maturity Assessment (MDE/DoIT Tool)***
- ***On or before July 1, 2026, and every 2 years thereafter***

☐ ***Submit Completed Cybersecurity Maturity Assessment and Certification Statement to MDE/DoIT by Established Deadlines (MDE/DoIT secure website/email)***

Community water systems and community sewerage systems serving over 3,300 customers are subject to the following enhanced cybersecurity requirements:

- Cybersecurity Standards. Adopt and implement cybersecurity standards that meet or exceed the cybersecurity standards established by MDE and the DoIT for community water systems and community sewerage systems. Maryland cybersecurity standards are contained in the DoIT Cybersecurity Policy Suite, which translates the State's strategic cybersecurity mission into specific, actionable requirements. These cybersecurity standards align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0/NIST 800-53 and CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) 2.0 and consist of controls that contribute to an organization's overall cybersecurity maturity while mitigating or reducing cybersecurity risk and vulnerabilities.

  - Maryland Cybersecurity Standards for Community Water Systems and Community Sewerage Systems
  - CISA's Cross-Sector CPGs 2.0

- Zero Trust Approach. Commit to adopting a Zero-Trust (ZT) cybersecurity approach and begin planning and implementing the ZT approach, as appropriate for each system. The NIST defines ZT as *"…a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised*." Community water and sewerage systems should model their ZT approach after CISA's Zero Trust Maturity Model for on-premises services and cloud-based services.

  The ZT Maturity Model is comprised of five pillars that are briefly described below; see CISA document for additional details.

  - *Identity*: attribute or set of attributes that uniquely describe an agency user or entity, including non-person entities.
  - *Devices*: any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, Internet of Things (IoT) devices, networking equipment, and more.
  - *Networks*: an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.
  - *Applications*: agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments.

- *Data*: all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.

Utilities shall document a ZT Roadmap with milestones for identity, devices, networks, applications, and data controls, as well as OT segmentation and remote access protections. The DoIT will publish minimum milestone expectations and evidence requirements.

- Maturity Assessments. *On or before July 1, 2026, and every 2 years thereafter*, conduct a Maturity Assessment of the water system's cybersecurity program for OT and IT, based on Maryland's cybersecurity standards for community water systems and community sewerage systems and in alignment with NIST Cybersecurity Framework 2.0. Utilities shall also implement applicable controls and outcomes from the CISA CPGs as sector-appropriate minimum outcomes. DoIT will publish mappings, minimum outcomes, and evidence requirements.

  Community water and sewerage systems subject to enhanced requirements should follow the following steps:

  - Access the MDE/DoIT Cybersecurity Maturity Assessment Tool and complete the maturity assessment for each cybersecurity standard based on your current program capabilities by the established deadlines.
  - MDE has partnered with EPA to provide free cybersecurity maturity assessments through EPA's Cybersecurity Evaluation Program. Water utilities should visit the EPA Cybersecurity Assessment Registration website to schedule the assessment.
  - Alternatively, water utilities can use in-house resources to conduct maturity assessments using the Cybersecurity Maturity Assessment Tool.
  - Water utilities may also arrange for outside consultants to perform assessments using other accepted approaches, including those utilizing the NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), the International Organization for Standards/ International Electrotechnical Commission standard 27001 (ISO 27001), and the American Water Works Association Cybersecurity Assessment Tool (AWWA).
  - Submit the completed Cybersecurity Maturity Assessment Tool to MDE/DoIT via secure website/email, which is currently under development and will be shared with water systems once available. *Water systems do not need to submit the completed Cybersecurity Maturity Assessment Tool until the secure submission method is in place*.
  - Submit the completed Cybersecurity Maturity Assessment Certification Statement (Attachment) to water.cyber@maryland.gov by the established deadlines.

7.0 Cybersecurity Incident Reporting

☐ ***Report Cybersecurity Incidents to State Security Operations Center (website/soc@maryland.gov/410-697-9700)***

Utilities shall report cybersecurity incidents or a receipt of system-generated indications of compromise within 1 hour to the SSOC using the following methods specified by DoIT:

- Access the Maryland Incident Reporting System
- Send an email with the information below to soc@maryland.gov
- Call the DoIT Service Desk at 410-697-9700

A security incident is a confirmed event or violation that causes harm or poses an imminent threat of violation of security policies or practices. Incident reports should include, at a minimum, the following information:

- Organization Name
- Reporter's name and title, email address, mobile and office phone numbers
- Date and time of incident detection
- How was it detected; observations of what happened/is happening
- Whether the incident is confirmed or suspected
- If the cybersecurity incident is ongoing
- If any life-safety or critical infrastructure systems are impacted or suspected to be impacted
- A brief description of the business impact of the event
- Whether the organization is requesting assistance, and the nature of the assistance requested
- What, if any, action has been taken
- Who has been notified
- Any additional information material to the incident response

The SSOC will coordinate notifications to MDE, MDEM, and other partners. Utilities shall follow SSOC direction for follow-up reporting and situational updates no later than 24 hours after discovery.

8.0 Emergency Response Plan Updates

☐ ***Revise Emergency Response Plans to Address Cybersecurity Incidents (utility plan)***
  - ***On or before July 1, 2026, and every 2 years thereafter***

By July 1, 2026, and during each required update cycle thereafter, all community water and sewerage systems must revise their Emergency Response Plans (ERPs) to explicitly address cybersecurity incidents. Cyber-related ERP updates should be integrated into existing emergency planning frameworks rather than treated as standalone documents.

At a minimum, ERPs should include procedures for maintaining or restoring critical services following a cyber disruption, including contingencies for loss of visibility or control of OT systems. Utilities must also document alternative water supply or service arrangements developed in coordination with local emergency managers, where applicable.

In addition, ERPs should incorporate crisis and emergency risk communication protocols that align with MDEM guidance, addressing both internal communications and external communications with customers, regulators, and the public. Training and exercise plans should be updated to reflect cybersecurity scenarios, including participation in State or regional tabletop exercises when available.

9.0 Compliance

During sanitary surveys and compliance inspections, MDE may review cybersecurity-related documentation to include verification of cybersecurity POCs, evidence of required cybersecurity training, and review of ERPs for cybersecurity-related response and reporting actions. These documents must be available for review upon request. Updated ERPs must also be available for MDE review during sanitary surveys or compliance inspections.

MDE and DoIT may also perform scheduled cybersecurity inspections to review the water system cybersecurity program as it relates to ZT architecture and the Cybersecurity Maturity Assessment. MDE, DoIT, and MDEM may also inspect the ERP to ensure cybersecurity response actions are incorporated. Water system cybersecurity and ERP staff must be made available for these inspections, along with appropriate cybersecurity and response plan designs, procedures, and training programs.

Utilities subject to enhanced requirements shall submit completed Cybersecurity Maturity Assessment Tool spreadsheets and Cybersecurity Maturity Assessment compliance certifications to MDE/DoIT by the established deadlines. MDE/DoIT will review submissions for completeness and retain authority to request supporting documentation for validation. DoIT will provide an aggregated sector report to the State Chief Information Security Officer.

10.0 State and Federal Contacts

- MDE: Conducts sanitary surveys and compliance inspections within its statutory authority. Coordinates with DoIT on cybersecurity-related certification and inspection elements.
    - Water Supply Program: 410-537-3702 or email water.cyber@maryland.gov
- DoIT Office of Security Management: Publishes baseline cybersecurity standards, assessment criteria, certification templates, and incident reporting procedures. Receives certifications. Conducts validation reviews. Coordinates sector cybersecurity oversight.
    - Service Desk: 410-697-9700 or email service.desk@maryland.gov
- SSOC: Receives incident reports. Coordinates response support and partner notifications.
    - Service Desk: 410-697-9700 or email soc@maryland.gov
- MDEM: Leads consequence management and exercise planning. Maintains ERP storage process, as appropriate. Coordinates with SSOC, MDE and DoIT during incidents.
    - Maryland Joint Operations Center (MJOC): 410-517-3660 or email mjoc.mdem@maryland.gov
- CISA: Provides national guidance and support for cybersecurity across all critical infrastructures. Provides local and regional Protective Security Advisors (PSAs) and Cyber Security Advisors (CSAs) to assess, advise, and assist cybersecurity risk management activities and responses.
    - Websites: cisa.gov/water; cisa.gov/about/regions/security-advisors
- EPA: Provides national guidance, direction and support for cybersecurity resilience within the Water and Wastewater Systems Sector.
    - Website: epa.gov/waterresilience; epa.gov/cyberwater

11.0 Additional Resources

Below are additional resources available to community water and sewerage systems for cybersecurity program development and assessment.

- CISA: Cyber Resilience Review
- CISA: Cybersecurity Advisor
- CISA: Free Cyber Vulnerability Scanning for Water Utilities
- CISA: Cyber Hygiene Services
- CISA: Cyber Security Evaluation Tool (CSET)
- EPA: Water Sector Cybersecurity Evaluation Program
- EPA: Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems (Cybersecurity Checklist in Appendix)
- EPA: Cybersecurity Incident Action Checklist
- EPA: Assessing if a Water & Wastewater System has Operational Technology
- MDE: MDE Cybersecurity Website
- MD-DoIT: Maryland Cybersecurity Policy Suite
- Idaho National Laboratory: Operational Technology Cybersecurity
- American Water Works Association (AWWA): Water Sector Cybersecurity Risk Management Tool

References

Senate Bill 0871 Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments

Attachment: Certification Statement

Community Water and Sewerage System Cybersecurity Maturity Assessment for Senate Bill 871: Cybersecurity Planning and Assessments

Part (A): Water System Identification

Community Water / Sewerage System Name: _____

Complete Mailing Address: _____

Water System Identification Number: _____

Population served: _____

Part (B): Cybersecurity Maturity Assessment Date

Date of Cybersecurity Maturity Assessment: _____

Part (C): Certification Statement Date

I, [Name of certifying official]

_____

hereby certify that the community water or sewerage system named under Part A, above, has conducted a Cybersecurity Maturity Assessment for operational technology and information technology, based on Maryland's Cybersecurity Policy Suite for community water systems and community sewerage systems and in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals 2.0.