SENATE BILL 871

M3, S2 5lr2110
CF 5lr3261

By: **Senator Hester**
Introduced and read first time: January 28, 2025
Assigned to: Education, Energy, and the Environment

A BILL ENTITLED

AN ACT concerning

Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments

FOR the purpose of requiring the Department of the Environment to coordinate, in coordination with the Department of Information Technology and the Maryland Department of Emergency Management, cybersecurity efforts within community water systems and community sewerage systems; establishing the responsibilities of the Department of the Environment, the Department of Information Technology, and the Maryland Department of Emergency Management with respect to regulating, assessing, and promoting cybersecurity efforts within the water and wastewater sector; requiring certain community water system and community sewerage system providers in the State to take certain cybersecurity measures and report certain cybersecurity incidents; prohibiting the inspection of public records related to the security of critical infrastructure; and generally relating to cybersecurity planning and assessments for community water systems and community sewerage systems.

BY adding to
Article – Environment
Section 9–2701 through 9–2707 to be under the new subtitle "Subtitle 27. Community Water and Sewerage System Cybersecurity"
Annotated Code of Maryland
(2014 Replacement Volume and 2024 Supplement)

BY repealing and reenacting, with amendments,
Article – General Provisions
Section 4–338
Annotated Code of Maryland
(2019 Replacement Volume and 2024 Supplement)

BY repealing and reenacting, with amendments,

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

Article – Public Safety
Section 14–104.1
Annotated Code of Maryland
(2022 Replacement Volume and 2024 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Environment

SUBTITLE 27. COMMUNITY WATER AND SEWERAGE SYSTEM CYBERSECURITY.

9–2701.

(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(B) "COMMUNITY SEWERAGE SYSTEM" HAS THE MEANING STATED IN § 9–501 OF THIS TITLE.

(C) "COMMUNITY WATER SYSTEM" HAS THE MEANING STATED IN § 9–401 OF THIS TITLE.

(D) "CYBERSECURITY" MEANS PROCESSES OR CAPABILITIES WHEREIN SYSTEMS, COMMUNICATIONS, AND INFORMATION ARE PROTECTED AND DEFENDED AGAINST DAMAGE, UNAUTHORIZED USE OR MODIFICATION, AND EXPLOITATION.

(E) (1) "OPERATIONAL TECHNOLOGY" MEANS PROGRAMMABLE SYSTEMS OR DEVICES THAT INTERACT WITH THE PHYSICAL ENVIRONMENT BY DETECTING OR CAUSING A DIRECT CHANGE THROUGH THE MONITORING OR CONTROL OF DEVICES, PROCESSES, AND EVENTS.

(2) "OPERATIONAL TECHNOLOGY" INCLUDES:

(I) INDUSTRIAL CONTROL SYSTEMS;

(II) BUILDING MANAGEMENT SYSTEMS;

(III) FIRE CONTROL SYSTEMS; AND

(IV) PHYSICAL ACCESS CONTROL MECHANISMS.

(F) "WATER AND WASTEWATER SECTOR" MEANS ALL PROVIDERS, INCLUDING PRIVATE AND PUBLIC, OF WATER SUPPLY OR SEWERAGE SERVICES.

(G) "ZERO–TRUST" MEANS A CYBERSECURITY APPROACH:

(1) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION; AND

(2) BASED ON THE PREMISE THAT TRUST IS NEVER GRANTED IMPLICITLY BUT MUST BE CONTINUALLY EVALUATED.

9–2702.

THE DEPARTMENT SHALL:

(1) IN COORDINATION WITH THE DEPARTMENT OF INFORMATION TECHNOLOGY AND THE MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT, COORDINATE CYBERSECURITY EFFORTS WITHIN COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS;

(2) INCLUDE CYBERSECURITY AWARENESS COMPONENTS FOR ALL NEW AND RENEWING OPERATOR AND SUPERINTENDENT CERTIFICATIONS UNDER TITLE 12 OF THIS ARTICLE; AND

(3) IN CONSULTATION WITH THE DEPARTMENT OF INFORMATION TECHNOLOGY:

(I) UPDATE REGULATIONS GOVERNING COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS TO:

1. INCLUDE COMPREHENSIVE SECTIONS REGARDING CYBERSECURITY STANDARDS FOR WATER AND WASTEWATER TREATMENT FACILITIES; AND

2. REQUIRE COMMUNITY WATER SYSTEM AND COMMUNITY SEWERAGE SYSTEM PROVIDERS TO REPORT CYBER INCIDENTS CONSISTENT WITH DEPARTMENT OF INFORMATION TECHNOLOGY GUIDANCE TO UTILITIES REGARDING CYBER INCIDENTS;

(II) PROMULGATE MINIMUM CYBERSECURITY STANDARDS FOR ESTABLISHED COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS THAT MEET OR EXCEED THE FEDERAL CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S CROSS–SECTOR CYBERSECURITY PERFORMANCE GOALS;

(III) REQUIRE COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS TO PLAN FOR DISRUPTIONS OF SERVICE DUE TO CYBER

INCIDENTS, INCLUDING RANSOMWARE ATTACKS AND OTHER EVENTS RESULTING IN ROOT–LEVEL COMPROMISE;

(IV) ESTABLISH A LIST OF APPROVED CYBERSECURITY TRAINING PROGRAMS FOR STAFF RESPONSIBLE FOR MAINTAINING OR OPERATING WATER AND WASTEWATER FACILITIES; AND

(V) IMPLEMENT MEASURES TO PROTECT THE ACTIVE CERTIFIED OPERATORS LIST MAINTAINED ON THE DEPARTMENT'S WEBSITE WHILE ENSURING LEGITIMATE ACCESS FOR NECESSARY PURPOSES.

9–2703.

THE DEPARTMENT OF INFORMATION TECHNOLOGY SHALL:

(1) EMPLOY A PERSON TRAINED IN THE CYBERSECURITY OF OPERATIONAL TECHNOLOGY TO WORK WITH THE STATE CHIEF INFORMATION SECURITY OFFICER AND THE CYBER PREPAREDNESS UNIT IN THE MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT TO SUPPORT EFFORTS RELATED TO OPERATIONAL TECHNOLOGY IN CRITICAL INFRASTRUCTURE;

(2) ALLOW ALL MEMBERS OF THE WATER AND WASTEWATER SECTOR IN THE STATE TO JOIN THE MARYLAND INFORMATION SHARING AND ANALYSIS CENTER TO FURTHER STRENGTHEN CYBERSECURITY EFFORTS AND INFORMATION SHARING WITHIN THE SECTOR;

(3) IN CONSULTATION WITH THE DEPARTMENT, DEVELOP AND PROMOTE A GUIDANCE DOCUMENT THAT:

(I) PROVIDES STANDARDS THAT MEET OR EXCEED THE FEDERAL CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S CROSS–SECTOR CYBERSECURITY PERFORMANCE GOALS; AND

(II) OUTLINES THE BEST PRACTICES BEYOND MINIMUM STANDARDS THAT CAN SERVE AS A POINT OF REFERENCE FOR ENHANCING THE CYBERSECURITY POSTURE OF COMMUNITY WATER SYSTEM AND COMMUNITY SEWERAGE SYSTEM PROVIDERS; AND

(4) PROVIDE RESOURCES FOR CYBERSECURITY SPRINT TARGETING OF COMMUNITY WATER SYSTEM AND COMMUNITY SEWERAGE SYSTEM PROVIDERS TO IDENTIFY WEAKNESSES AND ASSIST WITH SECURITY IMPROVEMENTS.

9–2704.

ALL COMMUNITY WATER SYSTEM AND COMMUNITY SEWERAGE SYSTEM PROVIDERS IN THE STATE SHALL:

(1) APPOINT A PRIMARY POINT OF CONTACT FOR CYBERSECURITY TO INTERACT WITH THE MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT AND THE DEPARTMENT OF INFORMATION TECHNOLOGY REGARDING CYBERSECURITY–RELATED MATTERS; AND

(2) ATTEND ANNUAL TRAININGS TO IMPROVE CYBERSECURITY AWARENESS.

9–2705.

(A) THIS SECTION APPLIES TO A COMMUNITY WATER SYSTEM OR COMMUNITY SEWERAGE SYSTEM IN THE STATE THAT:

(1) SERVES OVER 3,300 CUSTOMERS; OR

(2) UTILIZES INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY AS PART OF ITS OPERATIONS.

(B) EACH COMMUNITY WATER SYSTEM AND COMMUNITY SEWERAGE SYSTEM PROVIDER SHALL:

(1) ADOPT AND IMPLEMENT CYBERSECURITY STANDARDS THAT ARE EQUAL TO OR EXCEED THE STANDARDS ADOPTED BY THE DEPARTMENT UNDER § 9–2702(3)(II) OF THIS SUBTITLE;

(2) ADOPT A ZERO–TRUST CYBERSECURITY APPROACH, SIMILAR TO THE FEDERAL CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S ZERO–TRUST MATURITY MODEL, FOR ON–PREMISES SERVICES AND CLOUD–BASED SERVICES; AND

(3) ON OR BEFORE JULY 1, 2026, AND EACH JULY 1 THEREAFTER, ENGAGE WITH A THIRD PARTY TO CONDUCT AN ASSESSMENT OF THE OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICES OF THE COMMUNITY WATER SYSTEM OR COMMUNITY SEWERAGE SYSTEM, BASED ON THE MINIMUM CYBERSECURITY STANDARDS ESTABLISHED UNDER § 9–2702(3)(II) OF THIS SUBTITLE.

9–2706.

(A) ON OR BEFORE OCTOBER 1, 2026, AND EVERY 2 YEARS THEREAFTER, THE OFFICE OF SECURITY MANAGEMENT IN THE DEPARTMENT OF INFORMATION TECHNOLOGY SHALL:

(1) COLLECT CERTIFICATIONS OF EACH COMMUNITY WATER SYSTEM AND COMMUNITY SEWERAGE SYSTEM PROVIDER'S COMPLIANCE WITH STANDARDS USED IN THE ASSESSMENTS CONDUCTED UNDER § 9–2705(B)(4) OF THIS SUBTITLE FOR CYBERSECURITY–RELATED POLICIES AND PROCEDURES; AND

(2) SUBMIT A REPORT TO THE STATE CHIEF INFORMATION SECURITY OFFICER, OR THE OFFICER'S DESIGNEE.

(B) THE REPORT REQUIRED UNDER SUBSECTION (A)(2) OF THIS SECTION SHALL INCLUDE:

(1) A GENERAL OVERVIEW OF CYBERSECURITY TECHNOLOGY AND POLICIES USED BY COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS IN THE STATE, GROUPED BY NUMBER OF CUSTOMERS SERVED; AND

(2) GENERAL RECOMMENDATIONS FOR IMPROVING CYBERSECURITY TECHNOLOGY AND POLICIES USED BY COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS IN THE STATE, GROUPED BY NUMBER OF CUSTOMERS SERVED.

9–2707.

(A) EACH COMMUNITY WATER SYSTEM AND COMMUNITY SEWERAGE SYSTEM SHALL REPORT, IN ACCORDANCE WITH THE PROCESS ESTABLISHED UNDER SUBSECTION (B) OF THIS SECTION, A CYBERSECURITY INCIDENT, INCLUDING AN ATTACK ON AN INFORMATION TECHNOLOGY SYSTEM BEING USED BY THE COMMUNITY WATER SYSTEM OR COMMUNITY SEWERAGE SYSTEM PROVIDER, TO THE STATE SECURITY OPERATIONS CENTER IN THE DEPARTMENT OF INFORMATION TECHNOLOGY.

(B) (1) THE STATE CHIEF INFORMATION SECURITY OFFICER, IN CONSULTATION WITH THE DEPARTMENT, SHALL ESTABLISH A PROCESS FOR COMMUNITY WATER SYSTEM PROVIDERS, COMMUNITY SEWERAGE SYSTEM PROVIDERS, AND OTHER MEMBERS OF THE WATER AND WASTEWATER SECTOR TO REPORT CYBERSECURITY INCIDENTS.

(2) THE REPORTING PROCESS SHALL SPECIFY:

(I) THE CIRCUMSTANCES UNDER WHICH AN INCIDENT MUST BE REPORTED;

(II) THE MANNER IN WHICH AN ENTITY MUST REPORT AN INCIDENT; AND

(III) THE TIME PERIOD WITHIN WHICH AN ENTITY MUST REPORT AN INCIDENT.

(C) THE STATE SECURITY OPERATIONS CENTER SHALL IMMEDIATELY NOTIFY THE APPROPRIATE STATE AND LOCAL GOVERNMENT AGENCIES OF A CYBERSECURITY INCIDENT REPORTED UNDER THIS SECTION.

(D) (1) ON OR BEFORE JANUARY 1, 2027, AND EACH YEAR THEREAFTER, THE OFFICE OF SECURITY MANAGEMENT IN THE DEPARTMENT OF INFORMATION TECHNOLOGY SHALL PUBLISH A REPORT THAT DESCRIBES THE NUMBER AND TYPE OF INCIDENTS REPORTED BY COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS IN THE PRECEDING CALENDAR YEAR.

(2) THE REPORT REQUIRED UNDER THIS SUBSECTION MAY NOT IDENTIFY THE IMPACTED COMMUNITY WATER SYSTEMS OR COMMUNITY SEWERAGE SYSTEMS.

Article – General Provisions

4–338.

(A) IN THIS SECTION, "CRITICAL INFRASTRUCTURE" HAS THE MEANING STATED IN § 1–101 OF THE PUBLIC UTILITIES ARTICLE.

(B) A custodian shall deny inspection of the part of a public record that contains information about the security of an information system **OR CRITICAL INFRASTRUCTURE**.

Article – Public Safety

14–104.1.

(a) (1) In this section the following words have the meanings indicated.

(2) "COMMUNITY SEWERAGE SYSTEM" HAS THE MEANING STATED IN § 9–501 OF THE ENVIRONMENT ARTICLE.

(3) "COMMUNITY WATER SYSTEM" HAS THE MEANING STATED IN § 9–401 OF THE ENVIRONMENT ARTICLE.

(4) "CRISIS AND EMERGENCY RISK COMMUNICATION PLAN" MEANS A PLAN FOR COMMUNICATING DURING AN EMERGENCY.

[(2)**] (5)** "Local government" includes local school systems, local school boards, and local health departments.

[(3)**] (6)** "Unit" means the Cyber Preparedness Unit.

(b) (1) There is a Cyber Preparedness Unit in the Department.

(2) In coordination with the State Chief Information Security Officer, the Unit shall:

(i) support local governments in developing a vulnerability assessment and cyber assessment, including providing local governments with the resources and information on best practices to complete the assessments;

(ii) develop and regularly update an online database of cybersecurity training resources for local government personnel, including technical training resources, cybersecurity continuity of operations templates, consequence management plans, and trainings on malware and ransomware detection;

(iii) assist local governments in**[**:

1.**]** the development of cybersecurity preparedness and response plans**[**;**], INCLUDING:**

[2.**] 1.** implementing best practices and guidance developed by the State Chief Information Security Officer; **[**and**]**

[3.**] 2.** identifying and acquiring resources to complete appropriate cybersecurity vulnerability assessments; **AND**

3. PLANNING FOR INCIDENTS AGAINST WATER AND WASTEWATER FACILITIES, INCLUDING ENSURING THAT THERE ARE PLANS FOR ALTERNATIVE WATER SUPPLIES AND MUTUAL AID AGREEMENTS SHOULD WATER SERVICES BECOME UNAVAILABLE;

(iv) connect local governments to appropriate resources for any other purpose related to cybersecurity preparedness and response;

(v) as necessary and in coordination with the National Guard, local emergency managers, and other State and local entities, conduct regional cybersecurity preparedness exercises; **[**and**]**

(vi) establish regional assistance groups to deliver and coordinate support services to local governments, agencies, or regions**;**

(VII) ANNUALLY HOST AT LEAST ONE TABLETOP EXERCISE, TAILORED TO THE STATE'S WATER AND WASTEWATER SECTOR, TO CONTINUE REFINING STATE AND LOCAL GOVERNMENT RESPONSES TO CYBER INCIDENTS; AND

(VIII) DEVELOP A CRISIS AND EMERGENCY RISK COMMUNICATION PLAN FOR COMMUNITY WATER SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS IN THE STATE.

(3) The Unit shall support the Office of Security Management in the Department of Information Technology during emergency response efforts.

(c) (1) Each local government shall report a cybersecurity incident, including an attack on a State system being used by the local government, to the appropriate local emergency manager and the State Security Operations Center in the Department of Information Technology and to the Maryland Joint Operations Center in the Department in accordance with paragraph (2) of this subsection.

(2) For the reporting of cybersecurity incidents under paragraph (1) of this subsection, the State Chief Information Security Officer shall determine:

(i) the criteria for determining when an incident must be reported;

(ii) the manner in which to report; and

(iii) the time period within which a report must be made.

(3) The State Security Operations Center shall immediately notify appropriate agencies of a cybersecurity incident reported under this subsection through the State Security Operations Center.

(d) (1) Five Position Identification Numbers (PINs) shall be created for the purpose of hiring staff to conduct the duties of the Maryland Department of Emergency Management Cybersecurity Preparedness Unit.

(2) For fiscal year 2024 and each fiscal year thereafter, the Governor shall include in the annual budget bill an appropriation of at least:

(i) $220,335 for 3 PINs for Administrator III positions; and

(ii) $137,643 for 2 PINs for Administrator II positions.

(E) THE DEPARTMENT SHALL:

(1) INCLUDE CYBERSECURITY ATTACK INFORMATION ON THE DEPARTMENT'S "KNOW THE THREATS" WEBSITE; AND

(2) CONSIDER USING MD READY AS AN ALERT SYSTEM IF NECESSARY.

SECTION 2. AND BE IT FURTHER ENACTED, That:

(a) It is the intent of the General Assembly that the Department of the Environment, in consultation with the Department of Information Technology, conduct a comprehensive education campaign targeted at leaders within the water and wastewater sector, emphasizing the economic value of cybersecurity prevention over remediation.

(b) The education campaign under subsection (a) of this section shall include mention of the following information and materials:

(1) the U.S. Environmental Protection Agency's Incident Action Checklist – Cybersecurity for all water and wastewater systems in the State;

(2) the National Institute of Standards and Technology's:

(i) Cybersecurity Framework 2.0;

(ii) Special Publication 800–82r3; and

(iii) security recommendations;

(3) reference models appropriate to the State's water and wastewater sector's operational technology networks to guide security improvements;

(4) best practices, including network segmentation;

(5) the federal Cybersecurity and Infrastructure Security Agency's "Top Cyber Actions for Securing Water Systems" fact sheet;

(6) the U.S. Department of Energy's Supply Chain Cybersecurity Principles;

(7) information on third–party risks to water and wastewater facilities and networks; and

(8) free resources available from federal agencies, including the Cybersecurity and Infrastructure Security Agency's:

(i) Cross–Sector Cybersecurity Goals; and

(ii) Cybersecurity Evaluation Tool.

(c) On or before July 1, 2026, the Department of the Environment shall report to the General Assembly, in accordance with § 2–1257 of the State Government Article, on its efforts under subsection (a) of this section.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2025.