

HOUSE BILL 1062

M3, S2

5lr3261
CF SB 871

By: **Delegate Harrison**

Introduced and read first time: February 5, 2025

Assigned to: Environment and Transportation and Health and Government Operations

Committee Report: Favorable with amendments

House action: Adopted

Read second time: March 22, 2025

CHAPTER _____

1 AN ACT concerning

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

4 FOR the purpose of requiring the Department of the Environment to coordinate, in
5 coordination with the Department of Information Technology and the Maryland
6 Department of Emergency Management, cybersecurity efforts within community
7 water systems and community sewerage systems; establishing the responsibilities of
8 the Department of the Environment, the Department of Information Technology,
9 and the Maryland Department of Emergency Management with respect to
10 regulating, assessing, and promoting cybersecurity efforts within the water and
11 wastewater sector; requiring certain community water system and community
12 sewerage system providers in the State to take certain cybersecurity measures and
13 report certain cybersecurity incidents; prohibiting the inspection of public records
14 related to the security of operational technology and certain critical infrastructure;
15 and generally relating to cybersecurity planning and assessments for community
16 water systems and community sewerage systems.

17 BY adding to

18 Article – Environment

19 Section ~~9-2701~~ through ~~9-2707~~ 9-2708 to be under the new subtitle “Subtitle 27.

20 Community Water and Sewerage System Cybersecurity”

21 Annotated Code of Maryland

22 (2014 Replacement Volume and 2024 Supplement)

23 BY repealing and reenacting, with amendments,

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.

Underlining indicates amendments to bill.

~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.



1 Article – General Provisions
2 Section 4–338
3 Annotated Code of Maryland
4 (2019 Replacement Volume and 2024 Supplement)

5 BY repealing and reenacting, with amendments,
6 Article – Public Safety
7 Section 14–104.1
8 Annotated Code of Maryland
9 (2022 Replacement Volume and 2024 Supplement)

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

12 **Article – Environment**

13 **SUBTITLE 27. COMMUNITY WATER AND SEWERAGE SYSTEM CYBERSECURITY.**

14 **9–2701.**

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

17 (B) “COMMUNITY SEWERAGE SYSTEM” HAS THE MEANING STATED IN §
18 9–501 OF THIS TITLE.

19 (C) “COMMUNITY WATER SYSTEM” HAS THE MEANING STATED IN § 9–401 OF
20 THIS TITLE.

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

24 (E) “EMERGENCY MANAGER” HAS THE MEANING STATED IN § 14–101 OF
25 THE PUBLIC SAFETY ARTICLE.

26 (F) (1) “OPERATIONAL TECHNOLOGY” MEANS PROGRAMMABLE SYSTEMS
27 OR DEVICES THAT INTERACT WITH THE PHYSICAL ENVIRONMENT BY DETECTING OR
28 CAUSING A DIRECT CHANGE THROUGH THE MONITORING OR CONTROL OF DEVICES,
29 PROCESSES, AND EVENTS.

30 (2) “OPERATIONAL TECHNOLOGY” INCLUDES:

31 (I) INDUSTRIAL CONTROL SYSTEMS;

1 (II) BUILDING MANAGEMENT SYSTEMS;

2 (III) FIRE CONTROL SYSTEMS; AND

3 (IV) PHYSICAL ACCESS CONTROL MECHANISMS.

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

6 ~~(G)~~ (H) "ZERO-TRUST" MEANS A CYBERSECURITY APPROACH:

7 (1) FOCUSED ON CYBERSECURITY RESOURCE PROTECTION; AND

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

10 9-2702.

11 THE DEPARTMENT SHALL:

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

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

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

21 (i) UPDATE REGULATIONS GOVERNING COMMUNITY WATER
22 SYSTEMS AND COMMUNITY SEWERAGE SYSTEMS TO:

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

26 2. REQUIRE COMMUNITY WATER SYSTEM AND
27 COMMUNITY SEWERAGE SYSTEM PROVIDERS TO REPORT CYBER INCIDENTS
28 CONSISTENT WITH DEPARTMENT OF INFORMATION TECHNOLOGY GUIDANCE ~~TO~~
29 ~~UTILITIES REGARDING CYBER INCIDENTS~~ IN ACCORDANCE WITH § 9-2707(B) OF
30 THIS SUBTITLE;

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

5 (III) REQUIRE COMMUNITY WATER SYSTEMS AND COMMUNITY
6 SEWERAGE SYSTEMS TO PLAN FOR DISRUPTIONS OF SERVICE DUE TO CYBER
7 INCIDENTS, INCLUDING RANSOMWARE ATTACKS AND OTHER EVENTS RESULTING IN
8 ROOT-LEVEL COMPROMISE;

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

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

15 9-2703.

16 THE DEPARTMENT OF INFORMATION TECHNOLOGY SHALL:

17 (1) EMPLOY A PERSON TRAINED IN THE CYBERSECURITY OF
18 OPERATIONAL TECHNOLOGY TO ~~WORK~~:

19 (I) WORK WITH THE STATE CHIEF INFORMATION SECURITY
20 OFFICER AND THE CYBER PREPAREDNESS UNIT IN THE MARYLAND DEPARTMENT
21 OF EMERGENCY MANAGEMENT TO SUPPORT EFFORTS RELATED TO ~~OPERATIONAL~~
22 ~~TECHNOLOGY IN~~ WATER SYSTEMS AND OTHER CRITICAL INFRASTRUCTURE; AND

23 (II) COORDINATE WITH THE MARYLAND DEPARTMENT OF
24 EMERGENCY MANAGEMENT AND LOCAL GOVERNMENT INFORMATION SECURITY
25 OFFICERS TO ASSIST IN PROTECTING COMMUNITY WATER SYSTEMS AND
26 COMMUNITY SEWERAGE SYSTEMS;

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

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

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

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

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

11 9-2704.

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

14 (1) APPOINT A PRIMARY POINT OF CONTACT FOR CYBERSECURITY TO
15 INTERACT WITH THE ~~MARYLAND DEPARTMENT OF EMERGENCY MANAGEMENT~~
16 APPROPRIATE LOCAL EMERGENCY MANAGER AND THE DEPARTMENT OF
17 INFORMATION TECHNOLOGY REGARDING CYBERSECURITY-RELATED MATTERS;
18 AND

19 (2) ATTEND ANNUAL TRAININGS TO IMPROVE CYBERSECURITY
20 AWARENESS.

21 9-2705.

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

24 ~~(1) SERVES SERVES OVER 3,300 CUSTOMERS; OR~~

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

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

29 (1) ADOPT AND IMPLEMENT CYBERSECURITY STANDARDS THAT ARE
30 EQUAL TO OR EXCEED THE STANDARDS ADOPTED BY THE DEPARTMENT UNDER §
31 9-2702(3)(II) OF THIS SUBTITLE;

1 (2) ~~ADOPT COMMIT TO ADOPTING A ZERO-TRUST CYBERSECURITY~~
 2 ~~APPROACH, SIMILAR TO AND BEGIN PLANNING AND IMPLEMENTING THE~~
 3 ~~ZERO-TRUST APPROACH, AS APPROPRIATE FOR EACH SYSTEM, MODELED AFTER~~
 4 ~~THE FEDERAL CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S~~
 5 ~~ZERO-TRUST MATURITY MODEL, FOR ON-PREMISES SERVICES AND CLOUD-BASED~~
 6 ~~SERVICES; AND~~

7 (3) ~~ON OR BEFORE JULY 1, 2026, AND EACH JULY 1 EVERY 2 YEARS~~
 8 ~~THEREAFTER, ENGAGE WITH A THIRD PARTY TO CONDUCT AN A MATURITY~~
 9 ~~ASSESSMENT OF THE ITS CYBERSECURITY PROGRAM FOR OPERATIONAL~~
 10 ~~TECHNOLOGY AND INFORMATION TECHNOLOGY DEVICES OF THE COMMUNITY~~
 11 ~~WATER SYSTEM OR COMMUNITY SEWERAGE SYSTEM, BASED ON THE MINIMUM~~
 12 ~~CYBERSECURITY STANDARDS ESTABLISHED UNDER § 9-2702(3)(II) OF THIS~~
 13 ~~SUBTITLE.~~

14 ~~9-2706.~~

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

18 (1) COLLECT CERTIFICATIONS OF EACH COMMUNITY WATER SYSTEM
 19 AND COMMUNITY SEWERAGE SYSTEM PROVIDER'S COMPLIANCE WITH STANDARDS
 20 USED IN THE ASSESSMENTS CONDUCTED UNDER ~~§ 9-2705(B)(4)~~ § 9-2705(B)(3) OF
 21 THIS SUBTITLE FOR CYBERSECURITY-RELATED POLICIES AND PROCEDURES; AND

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

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

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

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

33 ~~9-2707.~~

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

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

13 (2) THE REPORTING PROCESS SHALL SPECIFY:

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

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

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

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

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

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

32 9-2708.

33 ON OR BEFORE JULY 1, 2026, AND EVERY 2 YEARS THEREAFTER, THE
34 DEPARTMENT SHALL REPORT TO THE GENERAL ASSEMBLY, IN ACCORDANCE WITH

1 § 2-1257 OF THE STATE GOVERNMENT ARTICLE, ON WATER SYSTEM COMPLIANCE
 2 AND THE PROGRESS MADE REGARDING THE IMPLEMENTATION OF THE
 3 REQUIREMENTS SET FORTH IN THIS SUBTITLE.

4 **Article – General Provisions**

5 4-338.

6 ~~(A) IN THIS SECTION, “CRITICAL INFRASTRUCTURE” HAS THE MEANING~~
 7 ~~STATED IN § 1-101 OF THE PUBLIC UTILITIES ARTICLE.~~

8 (A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS
 9 INDICATED.

10 (2) “COMMUNITY SEWERAGE SYSTEM” HAS THE MEANING STATED IN
 11 § 9-501 OF THE ENVIRONMENT ARTICLE.

12 (3) “COMMUNITY WATER SYSTEM” HAS THE MEANING STATED IN §
 13 9-401 OF THE ENVIRONMENT ARTICLE.

14 (4) (I) “CRITICAL INFRASTRUCTURE” HAS THE MEANING STATED
 15 IN § 1-101 OF THE ENVIRONMENT ARTICLE.

16 (II) “CRITICAL INFRASTRUCTURE” INCLUDES:

17 1. A COMMUNITY SEWERAGE SYSTEM; AND

18 2. A COMMUNITY WATER SYSTEM.

19 (5) “OPERATIONAL TECHNOLOGY” HAS THE MEANING STATED IN §
 20 9-2701 OF THE ENVIRONMENT ARTICLE.

21 (B) A custodian shall deny inspection of the part of a public record that contains
 22 information about the security of an information system, OPERATIONAL TECHNOLOGY,
 23 OR CRITICAL INFRASTRUCTURE, INCLUDING ANY RECORDS OF A COMMUNITY
 24 WATER SYSTEM OR COMMUNITY SEWERAGE SYSTEM.

25 **Article – Public Safety**

26 14-104.1.

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

28 (2) “COMMUNITY SEWERAGE SYSTEM” HAS THE MEANING STATED IN
 29 § 9-501 OF THE ENVIRONMENT ARTICLE.

1 **(3) “COMMUNITY WATER SYSTEM” HAS THE MEANING STATED IN §**
 2 **9-401 OF THE ENVIRONMENT ARTICLE.**

3 **(4) “CRISIS AND EMERGENCY RISK COMMUNICATION PLAN” MEANS A**
 4 **PLAN FOR COMMUNICATING DURING AN EMERGENCY.**

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

7 **[(3)] (6)** “Unit” means the Cyber Preparedness Unit.

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

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

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

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

18 (iii) assist local governments in[:

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

21 **[2.] 1.** implementing best practices and guidance
 22 developed by the State Chief Information Security Officer; [and]

23 **[3.] 2.** identifying and acquiring resources to complete
 24 appropriate cybersecurity vulnerability assessments; **AND**

25 **3. PLANNING PROVIDING GUIDANCE TO LOCAL**
 26 **EMERGENCY MANAGEMENT ORGANIZATIONS FOR INCIDENTS AGAINST WATER AND**
 27 **WASTEWATER FACILITIES, INCLUDING ENSURING THAT THERE ARE PLANS FOR**
 28 **ALTERNATIVE WATER SUPPLIES AND MUTUAL AID AGREEMENTS SHOULD WATER**
 29 **SERVICES BECOME UNAVAILABLE;**

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

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

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

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

9 ~~(VIII) DEVELOP A~~ GUIDANCE FOR CRISIS AND EMERGENCY RISK
 10 COMMUNICATION PLAN FOR COMMUNITY WATER SYSTEMS AND COMMUNITY
 11 SEWERAGE SYSTEMS LOCAL EMERGENCY MANAGEMENT ORGANIZATIONS IN THE
 12 STATE.

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

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

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

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

23 (ii) the manner in which to report; and

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

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

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

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

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

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

3 **(E) THE DEPARTMENT SHALL:**

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

6 ~~(2) CONSIDER USING MD READY AS AN ALERT SYSTEM IF NECESSARY~~
7 ~~DEPARTMENT'S WEBSITE.~~

8 SECTION 2. AND BE IT FURTHER ENACTED, That:

9 (a) It is the intent of the General Assembly that:

10 (1) the Department of the Environment, in consultation with the
11 Department of Information Technology, conduct a comprehensive education campaign
12 targeted at leaders within the water and wastewater sector, emphasizing the economic
13 value of cybersecurity prevention over remediation;

14 (2) the Maryland Department of Emergency Management prioritize
15 tabletop exercises focused on water cybersecurity; and

16 (3) the Department of the Environment work closely with the U.S.
17 Environmental Protection Agency, the U.S. Department of Defense, and other relevant
18 organizations to identify and access resources available for local community water systems
19 and community sewerage systems.

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

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

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

25 (i) Cybersecurity Framework 2.0;

26 (ii) Special Publication 800–82r3; and

27 (iii) security recommendations;

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

30 (4) best practices, including network segmentation;

1 (5) the federal Cybersecurity and Infrastructure Security Agency’s “Top
2 Cyber Actions for Securing Water Systems” fact sheet;

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

5 (7) information on third-party risks to water and wastewater facilities and
6 networks; and

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

9 (i) Cross-Sector Cybersecurity Goals; and

10 (ii) Cybersecurity Evaluation Tool.

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

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

Approved:

Governor.

Speaker of the House of Delegates.

President of the Senate.