**SB 871**

# Department of Legislative Services

Maryland General Assembly
2025 Session

## FISCAL AND POLICY NOTE
**First Reader**

Senate Bill 871 (Senator Hester)
Education, Energy, and the Environment

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

This bill establishes various requirements for the Maryland Department of the Environment (MDE), the Department of Information Technology (DoIT), the Maryland Department of Emergency Management (MDEM), and community water system (CWS) and community sewerage system (CSS) providers, related to planning and preparing for cybersecurity attacks on CWS and CSS and the water and wastewater sector. The bill also amends Maryland's Public Information Act (PIA) to prohibit the inspection of public records relating to the security of "critical infrastructure."

## Fiscal Summary

**State Effect:** General fund expenditures for DoIT and MDEM increase by at least $1.0 million in FY 2026; out-years reflect annualization, inflation, and ongoing costs. State expenditures (multiple fund types) for any affected State-owned systems may increase beginning as early as FY 2026. State revenues are not affected.

| ($ in millions) | FY 2026 | FY 2027 | FY 2028 | FY 2029 | FY 2030 |
|---|---|---|---|---|---|
| Revenues | $0 | $0 | $0 | $0 | $0 |
| GF Expenditure | 1.0 | 1.1 | 1.2 | 1.2 | 1.3 |
| Exp. (Mult. Funds) | - | - | - | - | - |
| Net Effect | (-) | (-) | (-) | (-) | (-) |

*Note:() = decrease; GF = general funds; FF = federal funds; SF = special funds; - = indeterminate increase; (-) = indeterminate decrease*

**Local Effect:** Potential significant increase in local expenditures beginning as early as FY 2026 for affected local systems to comply with the bill's requirements. Local revenues are not affected. **This bill imposes a mandate on a unit of local government.**

**Small Business Effect:** Meaningful.

## Analysis

**Bill Summary:**

*Maryland Department of the Environment – New Requirements*

In coordination with DoIT and MDEM, MDE must coordinate cybersecurity efforts within CWS and CSS. In consultation with DoIT, MDE must:

- update regulations governing CWS and CSS to include comprehensive cybersecurity standards for water and wastewater treatment facilities and require CWS and CSS providers to report cyber incidents, as specified;
- promulgate minimum cybersecurity standards for established CWS and CSS that that meet or exceed the federal Cybersecurity and Infrastructure Security Agency's cross-sector cybersecurity performance goals;
- require CWS and CSS to plan for service disruptions due to cyber incidents, as specified;
- establish a list of approved cybersecurity training programs for staff that are responsible for maintaining or operating water or wastewater facilities; and
- implement measures to protect its active certified operators list on its website while ensuring legitimate access for necessary purposes.

The bill expresses the General Assembly's intent that MDE, in consultation with DoIT, conduct a comprehensive education campaign targeted at the water and wastewater sector that emphasizes the economic value of cybersecurity prevention over remediation. The education campaign must include mention of specified information and materials. By July 1, 2026, MDE must report to the General Assembly on its efforts related to the education campaign.

MDE must also include cybersecurity awareness components for all new and renewing operator and superintendent certifications issued under Title 12 of the Environment Article (which governs waterworks and waste system operators).

*Department of Information Technologies – New Requirements*

DoIT must:

- employ a person who is trained in the cybersecurity of operational technology to work with the State Chief Information Security Officer (SCISO) and the Cyber Preparedness Unit (CPU) within MDEM to support efforts related to operational technology in critical infrastructure;

- allow members of the State's water and wastewater sector to join the Maryland Information Sharing and Analysis Center to strengthen cybersecurity efforts and information sharing;
- in consultation with MDE, develop and promote a cybersecurity guidance document that meets specified requirements; and
- provide resources for cybersecurity sprint targeting for CWS and CSS providers to identify weaknesses and assist with security improvements.

Additionally, by October 1, 2026, and every two years thereafter, DoIT's Office of Security Management (OSM) must (1) collect certifications of compliance from each CWS and CSS provider for compliance with standards used in the assessments conducted under the bill for cybersecurity-related policies and procedures and (2) submit a report to the SCISO or the officer's designee. The report must include specified information.

*Maryland Department of Emergency Management – New Requirements*

MDEM's CPU, in coordination with the SCISO, must:

- assist local governments in planning for incidents against water and wastewater facilities, including ensuring that there are plans for alternative water supplies and mutual aid agreements if water services become unavailable;
- 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
- develop a crisis and emergency risk communication plan for CWS and CSS.

MDEM must also include cybersecurity attack information on its "Know the Threats" website and consider using MD Ready as an alert system if necessary.

*Community Water Systems and Community Sewerage Systems – New Requirements*

All CWS and CSS providers in the State must (1) appoint a primary cybersecurity point of contact to interact with MDEM and DoIT regarding cybersecurity-related matters and (2) attend annual trainings to improve cybersecurity awareness.

CWS and CSS providers that serve more than 3,000 customers or utilize information technology (IT) and operational technology as part of their operations must:

- adopt and implement cybersecurity standards that meet or exceed the standards adopted by MDE under the bill;

- adopt a zero-trust cybersecurity approach for on-premises service and cloud-based services; and
- by July 1, 2026, and annually thereafter, engage a third party to assess their operational technology and IT devices based on the minimum cyber security standards established by MDE under the bill.

*Reporting of Cybersecurity Incidents*

The SCISO, in consultation with MDE, must establish a process for CWS and CSS providers and other members of the water and wastewater sector to report cybersecurity incidents. The process must include specified components.

Each CWS and CSS must report a cybersecurity incident, including an attack on an IT system used by the CWS or CSS, to the SCISO. The State Security Operations Center must immediately notify the appropriate State and local government agencies of a cybersecurity incident reported pursuant to these provisions.

By January 1, 2027, and annually thereafter, OSM must publish a report that describes the number and type of cybersecurity incidents reported by CWS and CSS in the preceding calendar year, as specified.

*Maryland's Public Information Act*

The bill amends PIA to provide that a custodian must deny inspection of the part of a public record that contains information about the security of "critical infrastructure" as defined in § 1-101 of the Public Utilities Article. "Critical infrastructure" is defined in § 1-101 of the Public Utilities Article to mean assets, systems, and networks, whether physical or virtual, considered by the U.S. Department of Homeland Security (DHS) to be so vital to the United States that their incapacitation or destruction would have a debilitating effect on one or more of the following: (1) security; (2) national economic security; (3) national public health; or (4) safety. The term includes a hospital or health care facility and a data center.

DHS identifies 16 sectors as critical infrastructure sectors, including the water and wastewater systems sector.

**Current Law:**

*State and Local Cybersecurity – Generally*

Chapters 241, 242, and 243 of 2022 expanded and enhanced the State's regulatory framework for State and local government cybersecurity. Among other things, the Acts required additional funding for cybersecurity, established leadership positions in

State government for cybersecurity, and codified existing cybersecurity requirements from a previous executive order. Together, the Acts:

- codified and expanded the duties of OSM within DoIT;
- established the positions of Director of State Cybersecurity and Director of Local Cybersecurity within OSM;
- established CPU within MDEM and required the unit to, among other duties, support local governments in developing a vulnerability assessment and cyber assessment and develop and regularly update an online database of cybersecurity training resources, including specified resources;
- required State and local governments to conduct cybersecurity preparedness assessments within specified timeframes; and
- required DoIT to develop a centralization transition strategy toward cybersecurity centralization for State and local governments.

Chapter 243 also required, by December 1, 2023, a public or private water or sewer system that serves a minimum of 10,000 users and receives financial assistance from the State to (1) assess its vulnerability to a cyberattack; (2) if appropriate, develop a cybersecurity plan; and (3) submit a report to the General Assembly on the findings of the assessment and any recommendations for statutory changes needed for the system to appropriately address its cybersecurity. Chapter 243 also authorized MDE's Maryland Water Quality Financing Administration (now called the Maryland Water Infrastructure Financing Administration) to provide financial assistance to a public water or wastewater system to assess cybersecurity vulnerabilities and develop a cybersecurity plan.

*Maryland Cybersecurity Council*

The Maryland Cybersecurity Council is required to work with the National Institute of Standards and Technology (NIST), as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State cybersecurity issues. The council's responsibilities include, among other things:

- for critical infrastructure not covered by federal law, reviewing and conducting risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures;
- using federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or unauthorized cyber access to the infrastructure could reasonably result in catastrophic consequences, including (1) interruption in the provision of energy, water, transportation, emergency services, food, or other life-sustaining services sufficient to cause a mass casualty event or mass evacuations; (2) catastrophic economic damage; or (3) severe degradation of State or national security;

- assisting specified infrastructure entities in complying with federal cybersecurity guidance;
- assisting private-sector cybersecurity businesses in adopting, adapting, and implementing the NIST cybersecurity framework of standards and practices; and
- examining inconsistencies between State and federal cybersecurity laws.

*Cybersecurity and Public Service Companies*

As noted above, "critical infrastructure" is defined in § 1-101 of the Public Utilities Article to mean assets, systems, and networks, whether physical or virtual, considered by DHS to be so vital to the United States that their incapacitation or destruction would have a debilitating effect on one or more of the following: (1) security; (2) national economic security; (3) national public health; or (4) safety. The term includes a hospital or health care facility and a data center.

Chapter 499 of 2023 established cybersecurity requirements for the Public Service Commission (PSC) and public service companies. Among other things, PSC is required to have at least one cybersecurity expert on its staff, and, in supervising and regulating public service companies, PSC must also consider the protection of a public service company's infrastructure against cyberattack threats. PSC must collaborate with OSM to establish cybersecurity standards and best practices for regulated entities, taking into account utility needs and capabilities based on size. PSC must periodically share information on cybersecurity initiatives and best practices with municipal electric utilities.

Among other requirements, each public service company, except common carriers and telephone companies, must adopt and implement cybersecurity standards that are equal to or exceed the standards adopted by PSC, adopt a zero-trust cybersecurity approach for on-premises services and cloud-based services, and establish minimum security standards for each operational technology and IT device.

"Public service company" means a common carrier company, electric company, gas company, sewage disposal company, telegraph company, telephone company, water company, or any combination of public service companies.

PSC adopted regulations in December 2024 to implement Chapter 499. (See DLS Control No. 24-070P).

*Safe Drinking Water Act and Community Water Systems*

MDE is responsible for the primary enforcement (primacy) of the federal Safe Drinking Water Act (SDWA) in Maryland. This means MDE is charged with ensuring that the water quality and quantity at all public water systems meet the needs of the public and are in compliance with federal and State regulations. According to MDE's Safe Drinking Water

Act Annual Compliance Report for Calendar Year 2023 to the U.S. Environmental Protection Agency (EPA), routine compliance activities include regular on-site inspections of water systems to identify any sanitary defects in the systems, technical assistance, and a permitting process that helps ensure that systems obtain the best possible source of water.

A "CWS" means a public water system that serves at least 15 service connections used by year-round residents of the area served by the system, or that regularly serves at least 25 year-round residents. Maryland regulates 3,233 public water systems (461 CWS, 539 non-transient non-CWS, and 2,233 transient non-CWS).

Under SDWA, EPA sets standards for drinking water quality and oversees the states, localities, and water suppliers who implement those standards. In 2018, SDWA was amended by the America's Water Infrastructure Act of 2018 (AWIA). AWIA § 2013 requires CWS serving more than 3,300 people to develop or update risk assessments and emergency response plans (ERPs). The law specifies the components of the risk assessments and ERPs, including the physical and cybersecurity of the systems, and establishes deadlines by which water systems must certify to EPA completion of the risk assessment and ERP.

*Federal Clean Water Act and Community Sewerage Systems*

The federal Clean Water Act (CWA) establishes the basic structure for regulating discharges of pollutants into the waters of the United States. The National Pollutant Discharge Elimination System (NPDES), a component of CWA, is a permit program that addresses water pollution by regulating point sources that discharge pollutants to U.S. waters. In Maryland, EPA delegates authority to issue NPDES permits to MDE. MDE issues discharge permits to protect Maryland's water resources by controlling industrial and municipal wastewater discharges. Surface water discharges are regulated through combined State and federal permits under NPDES. Groundwater discharges are regulated through State-issued groundwater discharge permits.

A "CSS" means a publicly or privately owned sewerage system that serves at least two lots.

*County Water and Sewerage Plans*

Each county (including Baltimore City) must have an individual or group (with adjoining counties) plan that is approved by MDE that has a 10-year forecasted water and sewerage plan to demonstrate how safe and adequate water and sewerage facilities will be provided to support planned redevelopment and new growth that is outlined in their comprehensive land use plans.

*Maryland's Public Information Act*

PIA establishes that all persons are entitled to have access to information about the affairs of government and the official acts of public officials and employees. Each governmental unit that maintains public records must identify a representative whom a member of the public may contact to request a public record. The Office of the Attorney General (OAG) must post all such contact information on its website and in any *Public Information Act Manual* published by OAG.

*Duties of Custodians:* Generally, a custodian of a public record must permit inspection of any public record at any reasonable time. A custodian must designate types of public records that are to be made available to any applicant immediately on request and maintain a current list of the types of public records that have been so designated. Each custodian must adopt reasonable rules or regulations that, consistent with PIA, govern timely production and inspection of a public record. Chapter 658 of 2021, effective July 1, 2022, requires each official custodian to adopt a policy of proactive disclosure of public records that are available for inspection under PIA, as specified.

*Required Denials:* A custodian must deny inspection of a public record or any part of a public record if (1) the public record is privileged or confidential by law or (2) the inspection would be contrary to a State statute, a federal statute or regulation, the Maryland Rules, or an order of a court of record. PIA also requires denial of inspection for specified personal and confidential records and information, including, for example, personnel and student records, hospital records, specified medical and financial information, and shielded criminal and police records.

**State Expenditures:**

*Department of Information Technology*

DoIT advises that the bill significantly expands its duties within the State's cybersecurity framework. DoIT further advises that because MDE does not have significant cybersecurity expertise, many of the duties that the bill requires MDE to undertake in consultation with DoIT, are, in practice, likely to fall to DoIT. Thus, general fund expenditures for DoIT increase by at least $865,631 in fiscal 2026, which accounts for the bill's October 1, 2025 effective date. This estimate reflects the cost of hiring eight employees (one cyber policy and strategy planner manager (who fulfills the bill's requirement to employ a person trained in the cybersecurity of operational technology), three cyber policy and strategy planners, and four defense incident responders) to (1) work with MDE and MDEM to coordinate cybersecurity efforts within CWS and CSS and the water and wastewater sector; (2) work alongside the SCISO; (3) oversee statewide cybersecurity incident reporting for CWS and CSS; (4) draft and update statewide cybersecurity standards and cybersecurity best practices for CWS and CSS; (5) facilitate

sector-wide information sharing and share required incident reports; (6) develop and promote the required guidance document; (7) collect cybersecurity compliance certifications and submit required reports; and (8) generally facilitate the implementation of the bill. It includes salaries, fringe benefits, one-time start-up costs, and ongoing operating expenses.

| | |
|---|---|
| Positions | 8.0 |
| Salaries and Fringe Benefits | $806,681 |
| Operating Expenses | 58,950 |
| **Minimum FY 2026 DoIT Expenditures** | **$865,631** |

Future year expenditures – which also reflect minimum costs – reflect full salaries with annual increases and employee turnover as well as annual increases in ongoing operating expenses.

The bill also requires DoIT to provide resources for cybersecurity sprint targeting of CWS and CSS providers to identify weaknesses and assist with security improvements. The costs associated with this effort could be substantial but cannot be estimated at this time. Accordingly, costs are likely higher than the minimum estimate provided above.

*Maryland Department of Emergency Management*

MDEM advises that while it has staff that focus on planning, training, and exercises for cyber attacks, existing staff do not have expertise specific to CWS and CSS. Thus, general fund expenditures for MDEM increase by at least $100,000 annually beginning in fiscal 2026 for contractual support to develop the required planning documents and communication plans and to annually host tabletop exercises tailored to the State's water and wastewater sector, as required by the bill. MDEM notes that costs may be higher depending on the demand for its services.

*Maryland Department of the Environment*

As discussed above, this analysis assumes that DoIT takes the lead on many of the duties assigned to MDE under the bill. As a result, MDE advises that it can work with DoIT and MDEM to implement the bill with existing resources. As the bill envisions robust participation by MDE, to the extent that existing resources prove insufficient, MDE may need to request additional resources through the annual budget process.

*State Agencies as Owners/Operators of Community Water Systems and Community Sewerage Systems*

For a discussion of the potential impacts on State agencies as owners/operators of CWS and/or CSS, see the Additional Comments section below.

**Local Fiscal Effect:** For a discussion of the potential impacts on local governments as owners/operators of CWS or CSS, see the Additional Comments section below.

**Small Business Effect:** Small businesses that provide cybersecurity services, including cybersecurity assessments, benefit from an increase in the demand for their services. Consumers (which include small businesses) benefit from increased cybersecurity at CWS and CSS throughout the State.

For a discussion of the potential impacts on small businesses as owners/operators of CWS or CSS, see the Additional Comments section below.

**Additional Comments (Effect on the Regulated Community):** Affected CWS and CSS could be owned and operated by State agencies, local governments, and small businesses. Affected systems likely incur increased costs to comply with the bill's requirements. The costs could be significant for some systems depending on the size of the system, current cybersecurity measures in place (if any), and the standards adopted under the bill. The bill also requires CWS and CSS to conduct third-party compliance assessments, which further increases costs. Depending on the findings of those assessments, costs may also be incurred to address related findings. In addition, there could also be costs for staff training and to attend the tabletop exercises hosted by MDEM. It is assumed that the bill's requirement to submit incident reports can likely be accomplished with relatively minimal impact.

According to the Maryland Association of Counties (MACo), the bill is anticipated to impose a significant burden on local governments, who own and operate many CWS and CSS. For example, MACo reports that a third-party independent assessment of operational technology and IT devices for a CWS or CSS can cost between $30,000 to $40,000 each. The Department of Legislative Services is unable to independently verify this estimate. MACo further advises that for some counties, adopting a zero-trust cybersecurity model will require a complete restructuring of their networks.

On the other hand, CWS and CSS likely benefit from (1) the education, information, training, and resources provided under the bill through centralized communications, guidance documents, tabletop exercises, and assistance and (2) the coordination of statewide cybersecurity efforts for CWS and CSS to help avoid and plan for cybersecurity attacks.

## Additional Information

**Recent Prior Introductions:** Similar legislation has not been introduced in the last three years.

**Designated Cross File:** HB 1062 (Delegate Harrison) - Environment and Transportation and Health and Government Operations.

**Information Source(s):** Department of Information Technology; Maryland Association of County Health Officers; Maryland Environmental Service; Harford and Montgomery counties; Maryland Association of Counties; Washington Suburban Sanitary Commission; Maryland Department of Emergency Management; Office of the Attorney General; Maryland Department of the Environment; U.S. Department of Homeland Security; Department of Legislative Services

**Fiscal Note History:** First Reader - February 25, 2025
km/lgc

---

Analysis by: Kathleen P. Kennedy

Direct Inquiries to:
(410) 946-5510
(301) 970-5510