**Maryland Department of the Environment**
**Guidance to Water and Wastewater Systems on the**
**Modernize Maryland Act of 2022**
**(HB1205: Information Technology and Cybersecurity-Related Infrastructure)**

**To:** Public or private water and wastewater systems that serve 10,000 or more users and receive financial assistance from the state.

**Purpose:** To provide guidance to the referenced public or private water and wastewater systems in developing a Cybersecurity Vulnerability Assessment to comply with the requirements of the Maryland Modernization Act of 2022 (HB1205).

A detailed breakdown of the Modernize Maryland Act of 2022 requirements, existing applicable regulatory requirements, and useful resources for water and wastewater systems are outlined below.

## 1. Deadlines

By December 1, 2023, a public or private water or wastewater system in Maryland that: A. has 10,000 or more users, **and** B. receives financial assistance from the state must: (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.

## 2. Existing Federal regulatory requirements

The federal America's Water Infrastructure Act (AWIA) of 2018 Section 2013(b) required each community water system serving a population of 3,300 or more users (thus all water systems impacted by HB1205) to assess risks to, and resilience of, its infrastructure, including electronic, computer and other security-based automated systems. These water systems were required to prepare or revise an emergency response plan (ERP) that incorporated the assessment findings and included strategies and resources to improve system resiliency, including cybersecurity.

AWIA required water systems to submit certification of their risk assessment and ERP directly to the U.S. Environmental Protection Agency (EPA) in 2021. These water systems need to review and update their assessment as well as their ERP every 5 years, then certify this update to EPA. EPA does not require water systems to submit an original or copy of the assessment. AWIA also did not apply to wastewater systems. However, the resources developed by EPA can be used by both drinking water and wastewater systems.

## 3. Resources for developing a Cybersecurity Vulnerability Assessment

The following resources are available to assist a public or private water and wastewater system with developing a Cybersecurity Vulnerability Assessment:

### A. AWIA Cybersecurity Assessments

Water systems serving over 3,300 people were required to assess cybersecurity vulnerabilities under AWIA. Water systems should assess whether these assessments are sufficient for meeting the requirements of the Modernize Maryland Act of 2022.

Wastewater systems were not required to conduct assessments under AWIA, but they are now covered under Modernize Maryland Act of 2022.

- America's Water Infrastructure Act: Risk Assessments and Emergency Response Plans website

**B. Free, confidential cybersecurity assessments and technical assistance from EPA** For a limited time, EPA is providing "free, confidential cybersecurity assessments and technical assistance to interested water and wastewater utilities." MDE recommends that all systems, even those not required to meet the provisions for funding, consider participation in this program to conduct a Cybersecurity Vulnerability Assessment.

- EPA Free Cybersecurity and Technical Assistance Flyer
- Cybersecurity Assessment and Technical Assistance for Water and Wastewater Utilities website

**C. Water Sector Cybersecurity Brief for States**

Water and wastewater utilities may want to consider using EPA's Water Sector Cybersecurity Brief for States. This guide can assist utilities with assessing cybersecurity practices and developing an improvement plan to reduce cyber risks.

- Cybersecurity Brief for States

**D.** Other useful resources

- Technical Cybersecurity Support Plan for Public Water Systems - Report to Congress has links to information to assist in performing self-assessments and facility assessments.
- Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Evaluation Tool
- CISA Cybersecurity Resilience Review
- CISA Cyber Hygiene Services
- The National Institute of Standards and Technology's (NIST) Cybersecurity Framework Policy Template Guide
- Water Information Sharing and Analysis Center (WaterISAC) 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- Infographic: Cyber Risks & Resources for the Water and Wastewater Systems Sector

For any questions on these resources, please contact water.supply@maryland.gov.

**4. Submission of Assessment Report to the General Assembly**
An assessment report is to be submitted to the General Assembly, in accordance with § 2–1257 of the State Government Article, on the findings of the assessment conducted under this subsection and any recommendations for statutory changes needed for the system to appropriately address its cybersecurity. See references below for additional information.

Sensitive documents should not be transmitted to the General Assembly or state agencies via email or other non-secure modes of communication. MDE strongly encourages water systems and their contractors to summarize the results of the Cybersecurity Vulnerability Assessment in a brief report that excludes any sensitive findings, and to submit this abridged document to fulfill the requirement.

The assessment report can be submitted through regular mail or email to Sarah Albert at:
Sarah T. Albert
Mandated Reports Specialist
Library and Information Services
Department of Legislative Services
90 State Circle
Annapolis, Maryland 21401
410-946-5415/301-970-5415
Sarah.Albert@mlis.state.md.us

State Government Article § 2-1257 requires submission to the Maryland Legislative Library of the Department of Legislative Services, five printed copies of all reports distributed or submitted to the General Assembly. For any questions on submitting, visit mlsd.ent.sirsi.net/client/en_US/default/

**5. Funding**
MDE's Water Infrastructure Financing Administration (WIFA) may be able to provide financial assistance to a public water or wastewater system to assess cybersecurity vulnerabilities and develop a cybersecurity plan.

Funding may also be available through:
- DHS Cybersecurity Grant Program for state, local and territorial governments

For any funding related questions, please contact Jeff Fretwell, MDE Director of WIFA, at jeff.fretwell@maryland.gov.

**References**

- Modernize Maryland Act of 2022 (Information Technology and Cybersecurity–Related Infrastructure)
- **Universal Citation:** MD State Govt Code § 2-1257 (2021)