TESTIMONY PRESENTED TO THE
HOUSE ENVIRONMENT AND TRANSPORTATION COMMITTEE

SENATE Bill 871
DEPARTMENT OF THE ENVIRONMENT - COMMUNITY WATER AND SEWERAGE SYSTEMS - CYBERSECURITY PLANNING AND ASSESSMENTS

DR. GREG VON LEHMEN
MARCH 26, 2025

Mr. Chair, Madam Vice Chair, and members of the committee, thank you for the opportunity to provide testimony on behalf of SB 871. I am Dr. Greg von Lehmen, special assistant for cybersecurity at UMGC and staff to the Maryland Cybersecurity Council. My comments today are my own and are not intended to represent the views of these organizations.

This is a well-informed bill, supported as it is by a year's worth of research by a member of the NSA community and stakeholder input. It is a necessary bill. The cyber threat to critical infrastructure will accelerate as AI is increasingly leveraged to launch attacks at scale. "Scale" means that there will be no place to hide.

This bill does three very important things.

- First, it sets in motion a process of cybersecurity continuous improvement for the community water sector serving Maryland. A program of continuous improvement works by setting goals, measuring progress against those goals, and undertaking steps to close the gaps.

  As it stands, the bill does this by (1) setting standards consistent with or exceeding the NIST-informed Cross-sector Cybersecurity Performance Goals published by CISA in answer to the very threats mentioned today, (2) providing for assessments against those or more stringent standards, and (3) providing a self-certification regime for closing gaps.

- Second, the bill provides the State with information to gauge the cyber risk to community water and wastewater providers serving the State. Under the bill, this risk profile is informed by information gleaned from the assessments and from required incident reporting by providers to OSM.

- Third, a strength of the bill is that in its requirements and in the way in which it works it borrows broadly from the State's Critical Infrastructure Act of 2023. This statute empowers the PSC to address cybersecurity as one of its oversight responsibilities. Borrowing from this precedent is a strength because many of the lessons learned in the rulemaking working group in resolving stakeholder issues that remained after the law was passed would certainly be of benefit to the implementation of this bill.

As a clarifying note, the requirement of a maturity assessment "based on" the minimum cybersecurity standards and the certification of compliance or remediation will not reveal sensitive information that could be of tactical use to an attacker. A maturity assessment looks at *organizational capacity*—governance, policies, processes, staffing against a framework or standards. The maturity assessment does **not** ask the question does software X or device Y have vulnerabilities. It asks whether an organization has policies requiring cybersecurity awareness training, whether the organization has a routine of vulnerability scanning and patching, whether that scanning includes all mission-critical devices on the network, and so forth. There are a number of maturity models with the assessments for each maturity area summarized using some scale (e.g., 1 to 5, where 5 is optimal).

This bill is responsive to urgent calls by CISA, the FBI, EPA, and other federal agencies for greater cybersecurity by community water service providers. I urge a favorable report.

Thank you.