

SB0871- Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments

Senator Katie Fry Hester



Recent Water Cyberattacks

EPA Memo: 9% of public drinking water systems scanned had “critical” or “high” priority cybersecurity vulnerabilities.

Economic Impact: A 2020 U.S. Water Alliance report estimated that a nationwide water system disruption could result in **\$43.5 billion** in lost sales and **\$22.5 billion** in GDP damage.

Regulatory Failures: According to the EPA, **70% of inspected utilities** recently violated federal standards designed to prevent cyber breaches.

Rising Threats: **33% of surveyed water utilities** reported at least one cyber incident in 2023, up from **21% in 2021**.

Recent Cyberattacks:

- **American Water Cyberattack** – November 2024
- **Arkansas City Water Plant Attack** – October 2024

Russian hacking group claims responsibility for cyberattack on Indiana wastewater plant

A video from the "People's Cyber Army of Russia" claims responsibility for last week's cyberattack on the Tipton West Wastewater Treatment Plant in Indiana.

‘Critical’ cyber vulnerabilities found in many water utilities, warns EPA inspector general

The Environmental Protection Agency’s Office of Inspector General said a recent assessment uncovered an urgent need for cyber remediation.

Fears of Weakness in Water Cybersecurity Grow After Kansas Attack

White House plans a new push to boost cybersecurity in water sector after an aborted attempt last year

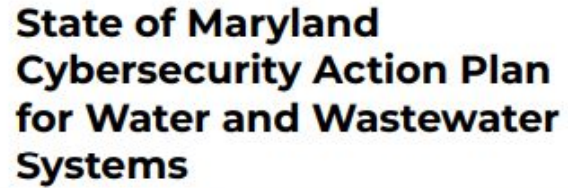
CYBER REPORT

America’s largest water utility hit by cyberattack at time of rising threats against U.S. infrastructure

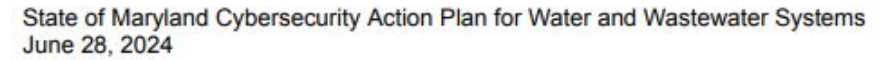
PUBLISHED TUE, OCT 8 2024•12:28 PM EDT | UPDATED TUE, OCT 8 2024•4:14 PM EDT

Recommendations

01	Governance & Policy	• Officially designate MDE as State Sector Risk Management Agency. • Supplement the Modernize Maryland Act of 2022 with a follow-on Act. • Update Reporting Requirements, reporting incidents within 24 hours. • WWS facilities appoint a primary point of contact for cybersecurity. • Cyber Adoption May Require Regulation.
02	Foundational Cybersecurity	• Ensure cyber hygiene and best practices are adopted by the WWS sector. • Adopt cybersecurity frameworks. • OT cybersecurity • Entities should adopt a Zero Trust strategy, tailored to fit their operation.
03	Risk Management & Resilience	• Encourage organizations to understand their risk; ensure continuity of operations • Host regular tabletop exercises. • Awareness of 3rd party risks. • Cybersecurity is not only digital, ensure physical security as well.
04	Resource Management	• Leverage DoIT Local Cyber • Highlight value of prevention of incidents. • Ensure awareness of cyber resources, esp. free. • Help connect financial resources.
05	Education & Awareness	• Upskilling and training • Recommend MDE & DoIT host tailored training to improve cybersecurity awareness. • Leverage universities and water trade groups knowledge and expertise. • Certify cybersecurity training programs.



June 28, 2024



The Maryland Cybersecurity Action Plan for Water and Wastewater Systems aims to address critical cybersecurity vulnerabilities within Maryland's water and wastewater infrastructure. This initiative is driven by the urgent need to protect these essential systems from increasingly sophisticated cyber threats, as outlined by recent federal advisories, the Modernize Maryland Act of 2022 (HB1205)¹, and in direct response to the letter from the White House dated March 21, 2024.²

COVERAGE AND APPLICABILITY

KEY ACTIONS

- 1. Cybersecurity Assessment for Covered Systems-** Compile a list of covered systems by September 1, 2024, notify systems of their obligations by October 1, 2024, and provide guidance for conducting assessments aligned with the NIST Cybersecurity Framework (CSF).

¹ Modernize Maryland Act of 2022, https://legis.maryland.gov/factsheets/legislation/DocumentDetails.aspx?mode=detail&docId=2022_0001

Maryland Water Sector - Community Water Systems

		System Size	Number of Systems	Population Served	Population Percentage	Name	Population Served	Population Percentage
96.5%		Very Large	5	4,181,331	76.19%	WSSC & City of Baltimore	3.5 million	63.77%
		Large	26	888,866	16.20%	City of Hagerstown & Frostburg	933,000	1.88%
3.5%		Medium	40	225,748	4.11%	Town of Mount Airy & Centreville	13,212	0.24%
		Small	105	141,528	2.58%			
		Very Small	292	50,526	0.92%			
		Total	468	5,487,999	100%			

What SB 871 Accomplishes

- 1) **Cybersecurity Coordination:** Strengthening cybersecurity oversight by designating MDE as the lead regulatory agency and requiring coordination with DoIT and MDEM to establish standards and best practices.
- 2) **Regulatory Updates:** Mandates updated regulations for community water and sewerage systems.
- 3) **Incident Reporting:** Requires water and sewerage systems to report cybersecurity incidents.
- 4) **Stronger Standards:** Ensures systems adopt cybersecurity standards meeting or exceeding those of the Department of Information Technology.
- 5) **Security Protections:** Prohibits public access to critical infrastructure security records.

Cyber Resilience Equals Water Resilience

REPORT- Maryland's Community
Water and Wastewater Systems:
Analysis and Recommendations

This report is unanimously supported
by the Maryland Cybersecurity Council
Subcommittee on Critical
Infrastructure



Cyber Resilience Equals Water Resilience

Thank you

Questions?



Why we need increased cybersecurity

CRITICAL

“Water is the only utility that you ingest. So, if a bad actor gets into and wreaks havoc on a water system, the consequences could be very dire”

Jennifer Kocher, VP of Communications and Marketing, the National Water Companies Association

VULNERABILITY

Cyberattacks against CWSs are increasing in frequency and severity across the country.

Based on actual incidents we know that a cyberattack on a vulnerable water system may allow an adversary to manipulate operational technology, which could cause significant adverse consequences for both the utility and drinking water consumers.

U.S. EPA, June 2024

PRE-SECURITY

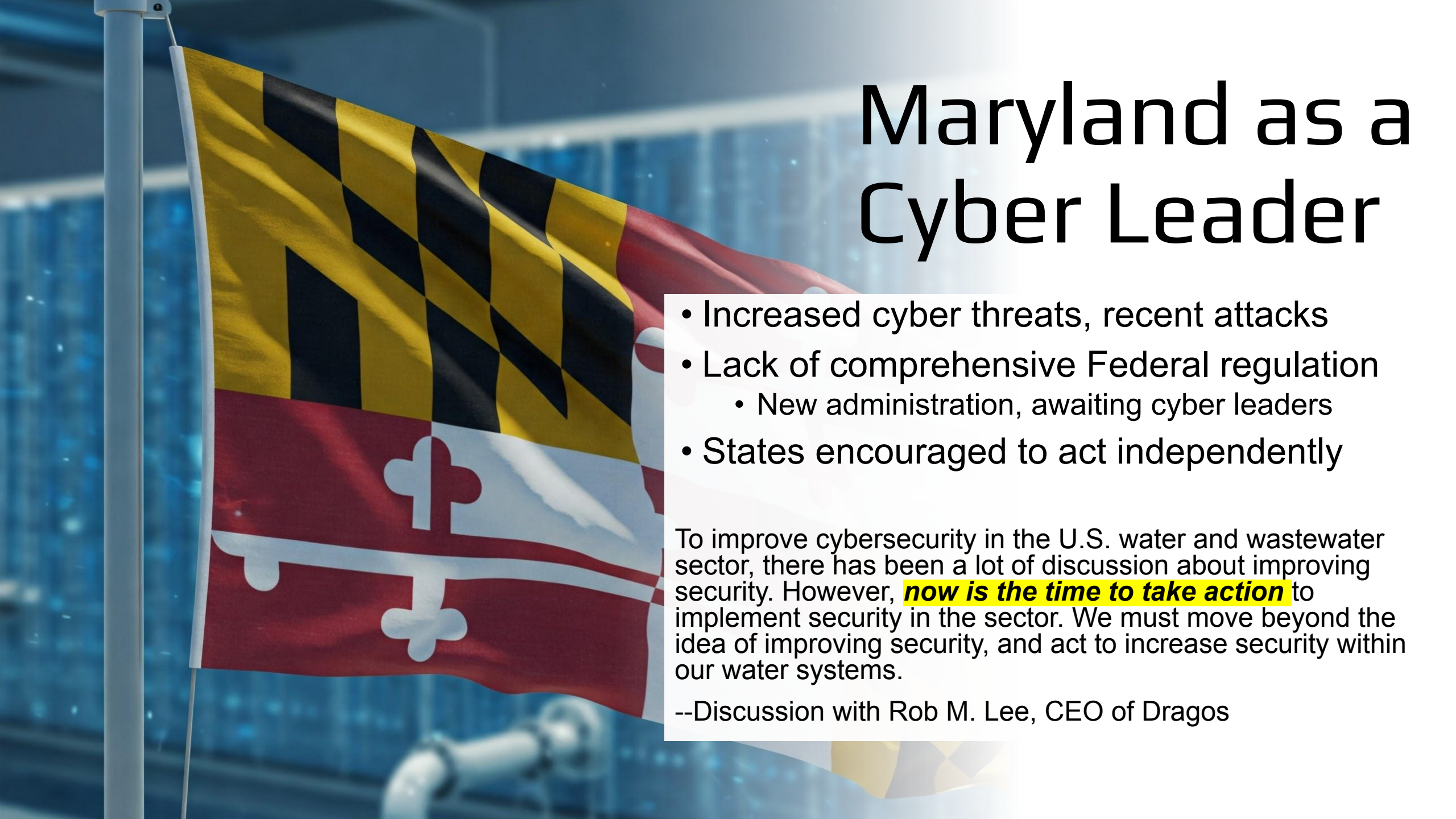
Water and wastewater systems in the U.S. are vital to public health and the environment, but they also suffer from chronic underfunding, legacy infrastructure and an expanding attack surface. **The reliance on OT systems, many of which lack modern security protections, has made these utilities particularly susceptible to cyber threats.**

Jonathan Reed, November 4, 2024

GEOPOLITICS

Critical infrastructure networks worldwide continue to be targeted by malicious cyber actors, including in conflict, where cyberspace is now an established domain of warfare and **cyberattacks are used for strategic, political, economic and national security objectives.**

Australian Signals Directorate

The background of the slide features the Maryland state flag, which has a yellow and black checkered upper half and a red and white lower half with a white cross. The flag is waving on a pole. In the background, a modern building with a curved glass facade is visible under a blue sky.

Maryland as a Cyber Leader

- Increased cyber threats, recent attacks
- Lack of comprehensive Federal regulation
 - New administration, awaiting cyber leaders
- States encouraged to act independently

To improve cybersecurity in the U.S. water and wastewater sector, there has been a lot of discussion about improving security. However, **now is the time to take action** to implement security in the sector. We must move beyond the idea of improving security, and act to increase security within our water systems.

--Discussion with Rob M. Lee, CEO of Dragos

How Do We Increase Security and Resilience?

Matthew Mitroka, PhD, CISSP presented findings and recommendations for the office of the attorney general and the MD Cybersecurity Council.

“Cyber security **legislation and regulation**, such as the new Cyber Security and Resilience Bill, are crucial steps.”

Regulations
Oversight &
Guidance

Awareness
&
Training

Resources:
Financial
Human
Information

“It’s not enough any more to talk about being resilient. We must all take the crucial steps that bolster our defences, that **improve and grow our capability** to contest.”

“We need all organizations – public and private – to see cyber security as both **an essential foundation** for their operations and a driver for growth, to view cyber security not just as a ‘necessary evil’ or compliance function but as a business investment, a catalyst for innovation and an integral part of achieving their purpose.”

Quotes from UK National Cyber Security Centre CEO Dr Richard Horne, 12/3/2024