MIIA Risk Management Advisory

Cybersecurity

August 5, 2026

Dear Member,

Recent news of hackers targeting, and in some cases, infiltrating critical infrastructure i.e. municipal water and wastewater operations has been concerning for many of our members.

The Cybersecurity and Infrastructure Security Agency **(CISA)** urges critical infrastructure owners, operators, and integrators to remove publicly exposed PLCs (Programmable Logic Controllers) and other operational technology (OT) from the internet as soon as possible.

CISA recommends organizations implement the following mitigations:

- Disconnect the PLC from the internet. Remote access for operational purposes should go through a VPN or gateway device, not directly to the PLC.
- Enable password protection and change default passwords.
- Allow list IPs to only allow remote access from known engineering laptops or other critical OT assets."

CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCS

CISA and Partners Release Updated Advisory on Iranian-Affiliated Cyber Actors Exploiting Program Logic Controllers Across Critical Infrastructure

Any MIIA member experiencing a cyber loss should immediately notify MIIA at (800) 526 – 6442 so that the proper Cyber Response resources from Tokio Marine can be deployed.

Members may use the links below to register for cyber alerts from CISA or to receive Fusion Center updates.

To register for CISA Alerts
To be added to the **Commonwealth Fusion Center** cybersecurity updates list send an email to the **Massachusetts Cybersecurity Program (MCP)** at **MCPPOL@pol.state.ma.us.**

Additional Municipal Cyber Resources

[Office of Municipal and School Technology (OMST)]
[MassCyber Center]

Please note, [MIIA 's Risk Management Grant] offers up to $10,000 for cyberrelated equipment and services. We encourage you to share the information below with your water department for possible use toward enhancing cyber security of this and other critical infrastructure operations.

Cyber		
Cyber risk prevention — assessments, social engineering training, multi-factor authentication (initial installation only), software patches, software backup, endpoint detection and response (EDR) and behavior-based malware and governance software		
CyberTrust Massachusetts programs and services — Critical Security Controls Assessment, Managed Detection and Response (MDR), Extended Detection and Response, Application Control, ZeroTrust Solutions and MS-ISAC membership.		
Payment of MS-ISAC annual dues		
Subscriptions to Tyler Technologies Endpoint, MDR, and Continuous Vulnerability Scanning services from EOTSS/OMST, extending the initial 60-day pilot.		

The MIIA Risk Management Team

@ 2025 MIIA. Solely for the benefit of MIIA members.
Disclaimer: The material contained herein is intended for general informational purposes only. It is not intended as legal advice and should not be construed as such. Any inquiries concerning Massachusetts law should be directed to a city solicitor, town counsel or other licensed attorney.

MIIA Risk Management

Massachusetts Interlocal Insurance Association
617-426-7272 • www.emiia.org
Nonprofit, Locally based, Member driven

FOLLOW US:

MIIA | 3 Center Plaza Suite 610 | Boston, MA 02108 US

Unsubscribe | Update Profile | Constant Contact Data Notice