



Dear System Operator/Utility Director:

As the frontline stewards of your community's drinking water, you already understand the importance of vigilance. Cyber threats to drinking water systems are not hypothetical. Recent incidents across the country confirm that malicious actors are deliberately targeting water utilities of all sizes, including small community systems, mobile home parks, and municipal systems. Attackers rely on common assumptions systems have, such as:

- "We're too small to be a target."
- "City officials won't care, so why bring up the topic?"
- "We've never had an attack on our water system before. If it isn't broken, why fix it?"

The threats are not about stealing data; the threats are about disrupting operations, damaging equipment, and instilling fear in your constituents, thereby undermining their confidence in their drinking water. For you, that could mean serious health, fiscal, and reputational damage. **We urge you to take immediate action to evaluate and strengthen your cybersecurity. Please do not wait.**

The department, along with our federal and third-party partners, is ready to support you. You do not have to approach this alone.

1. We recommend that your system participate in the [U.S. EPA Water Cybersecurity Evaluation Program](#). After you submit a request for this free cybersecurity assessment, an EPA contractor will schedule a time to review a cyber risk checklist with you and anyone else you deem appropriate, and recommend actions to address gaps, if any. Your assessment results are not shared with WDNR.
2. I also invite you to view the list of cybersecurity offerings to inform your security decisions by visiting the department's webpage:

[Cybersecurity Resources for Public Water Systems](#)



If you have additional questions or need help finding the right cyber security resource for you, email our staff expert, Marty Pollard, P.E. at Martin.Pollard@wisconsin.gov.

Sincerely,

Steve Elmore
Director, DNR Drinking Water & Groundwater Program