



Water and Wastewater Cybersecurity Overview

About the Speaker

- Brandon M. Carter, Sr. *Cybersecurity Analyst*
 - Carter.Brandon@epa.gov
- EPA's Office of Water Emergency Response and Cybersecurity (OWERC)
 - Cybersecurity Division



The Evolving Cyber Threat Landscape

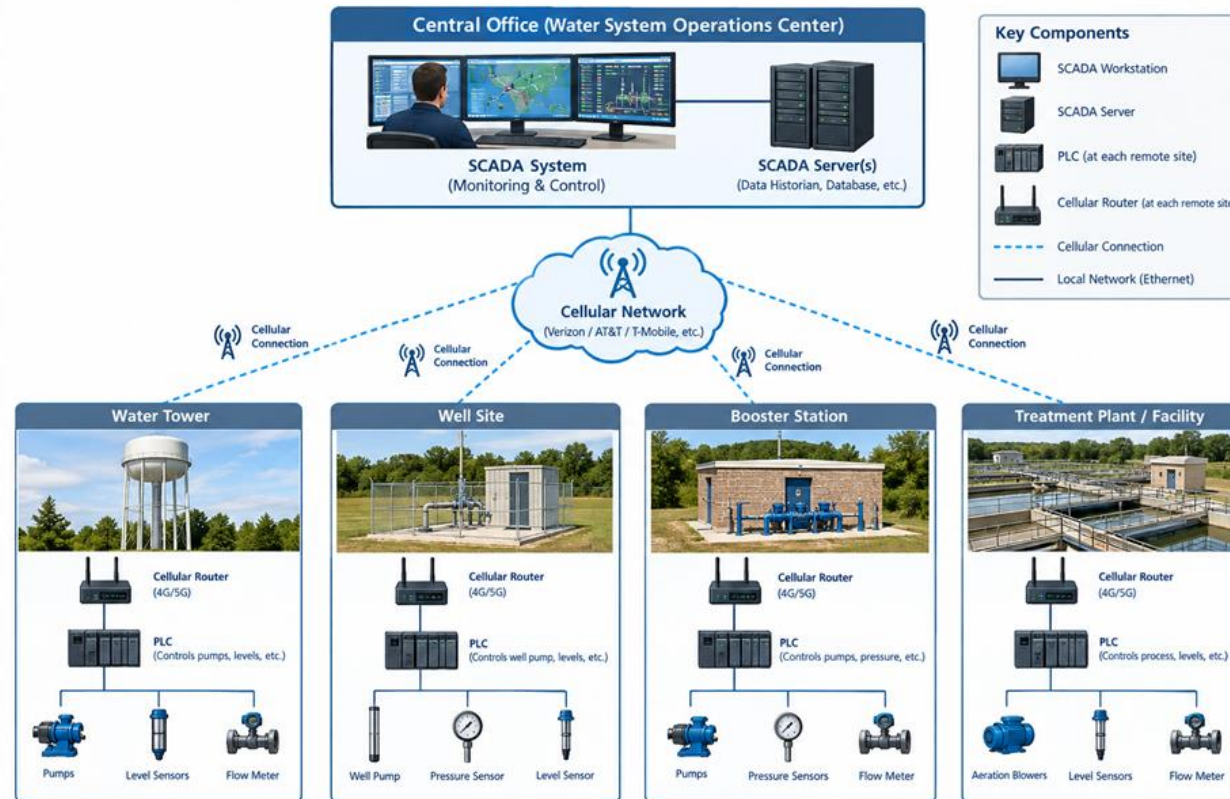
- Increase in frequency and severity of unauthorized remote access attacks
 - Many of these attacks are malware-free and target internet-exposed devices with vulnerabilities
- Groups associated with foreign states have disrupted services at US water and wastewater utilities, resulting in operational impacts
- Cyberattacks have evolved from largely IT-based ransomware to OT-focused attacks



Reported Cyberattacks & Impacts (Water/Wastewater)

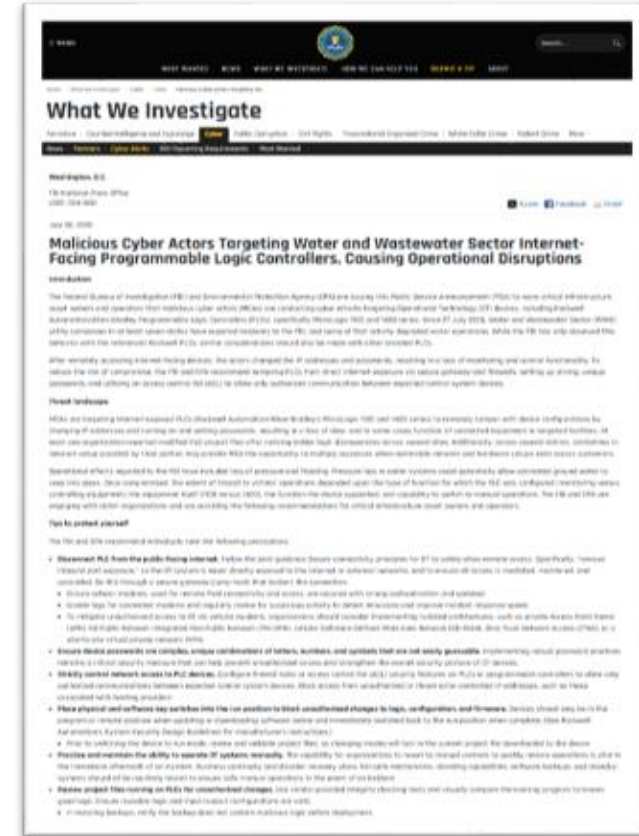
- EPA is aware of reported cyberattacks impacting water and wastewater systems nationwide
- Reported operational disruptions include **loss of communications** with remote sites
- Affected remote assets may include:
 - wells
 - pump stations
 - lift stations
 - water towers
- Unidentified threat actors are exploiting **internet-exposed, minimally secured equipment (PLCs)**

Common Water-System Configuration Example



Key Mitigations & Actions

- Recommended Mitigations
 - Remove publicly exposed PLCs from the internet as soon as possible
 - Enable password protection, change default passwords, and use complex passwords.
 - Place physical and software key switches into the run position
 - Strictly control network access to PLC devices
 - Practice and maintain the ability to operate OT systems manually
 - Review project files running on PLCs
 - Plan for end-of-life (EOL) replacements
- Report suspected activity
 - FBI [ic3.gov](https://www.fbi.gov/ic3)
 - CISA contact@cisa.dhs.gov
 - EPA OWERC-IncidentResponseTeam@epa.gov



[Joint FBI & EPA Advisory](#)

Cyber Alerts & Advisories

- CISA
 - **Alert:** [CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs](#)
 - **Advisory:** [AA26-097A](#)
 - Co-sealed by EPA, CISA, FBI, NSA, DOE, U.S. CYBERCOM, and Treasury
- FBI
 - **Alert:** [Malicious Cyber Actors Targeting Water and Wastewater Sector Internet- Facing Programmable Logic Controllers, Causing Operational Disruptions](#)
 - Co-sealed by EPA and FBI
- NSA
 - **Advisory:** [Defending Against an Active Threat to Siemens S7 Series PLCs](#)
 - Co-sealed by CISA, NSA, FBI, DOE, and EPA

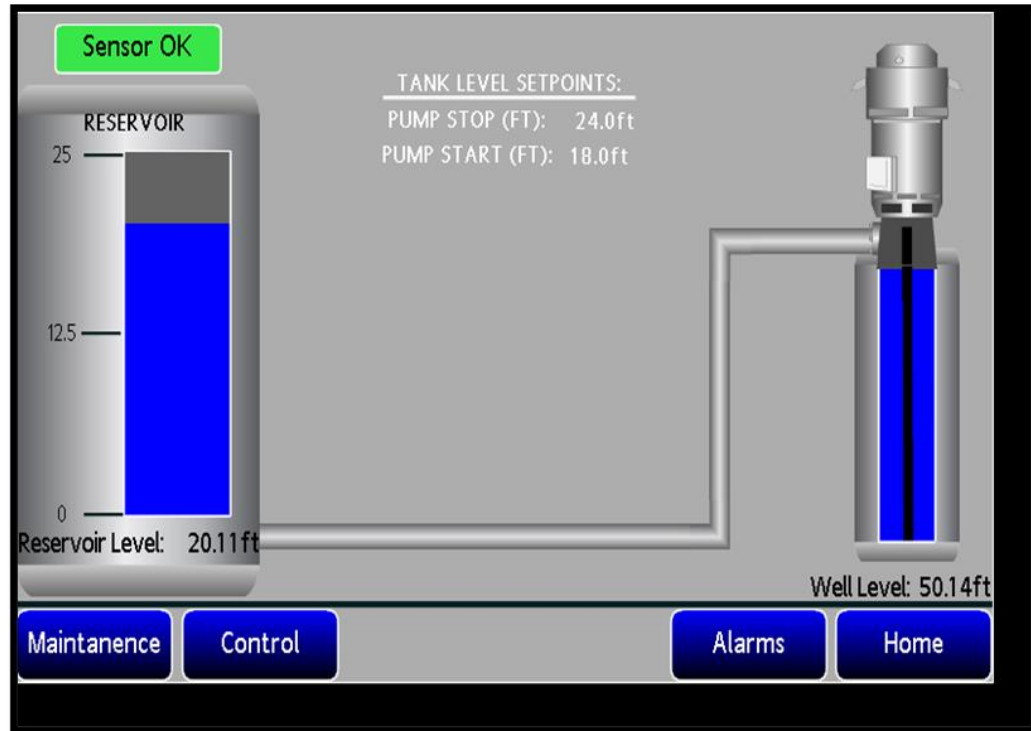
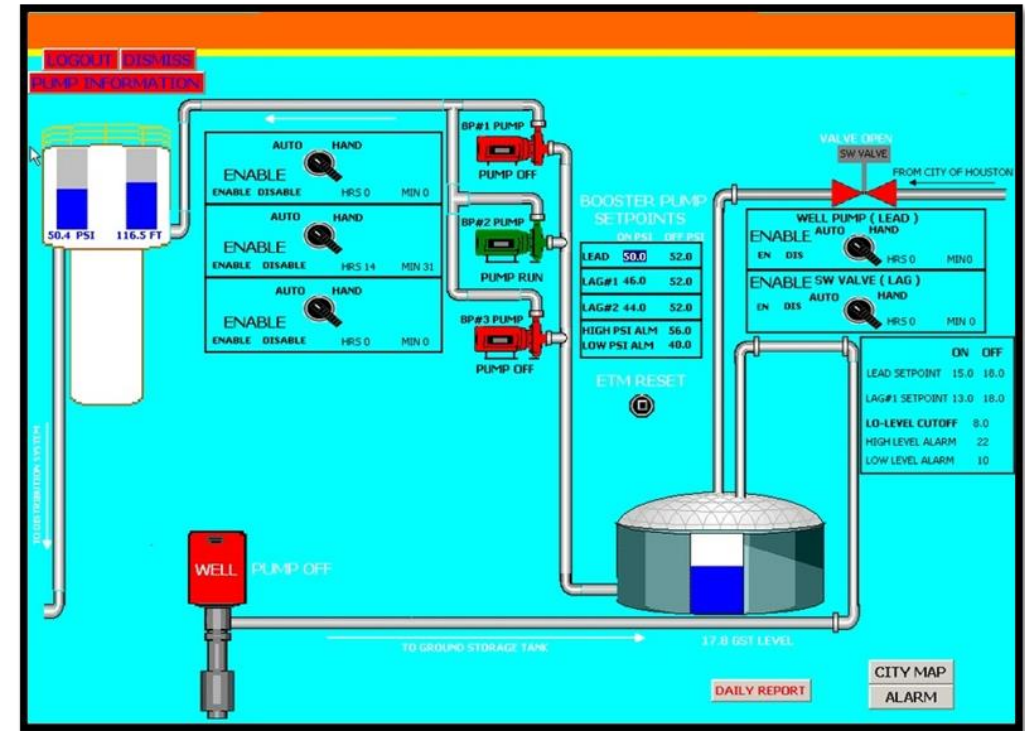


[CISA Alert](#)

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

- EPA and CISA often identify internet-exposed Human Machine Interfaces (HMIs) through scanning via publicly available web-based search platforms.
- In the absence of cybersecurity controls, unauthorized users can exploit HMIs to:
 - View the contents of the HMI
 - Make unauthorized changes and potentially disrupt the facility's water and/or wastewater treatment process

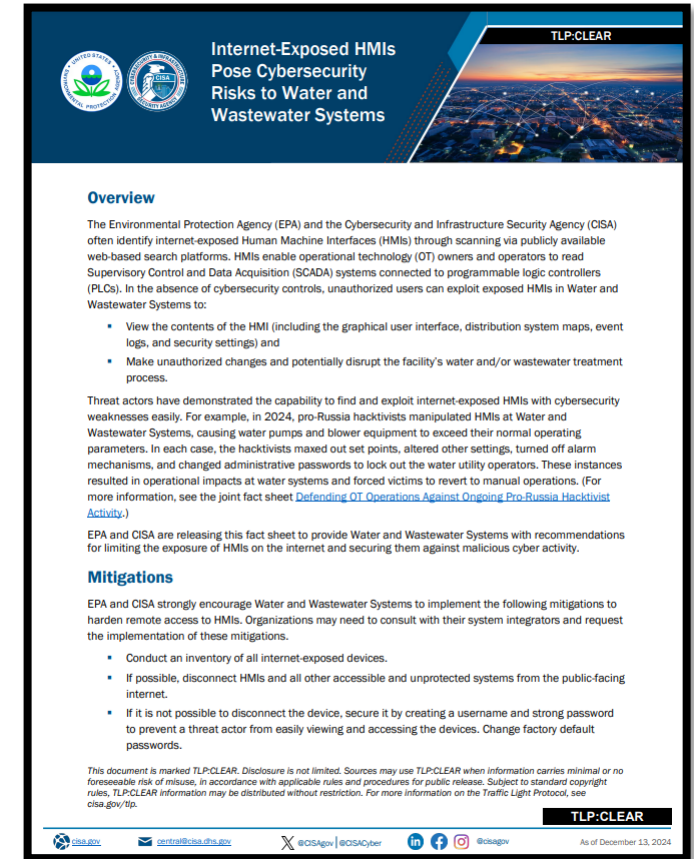
Examples of Exposed HMIs



December 2024 – Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Best Practices (Quick Wins) to Reduce Your Exposure

1. Conduct an inventory of all internet-exposed devices.
2. If possible, disconnect HMIs and all other accessible systems from the public internet. If this is not possible due to operational requirements, secure the HMI by using a strong password and ensure factory default passwords are never used.
3. Log remote logins to HMIs; be aware of failed attempts and unusual times.
4. Implement your vendor's recommendations for best securing your product.
5. Keep all systems and software up to date with patches and necessary security updates.
6. Implement multifactor authentication (MFA) for all access to the HMI and OT network.



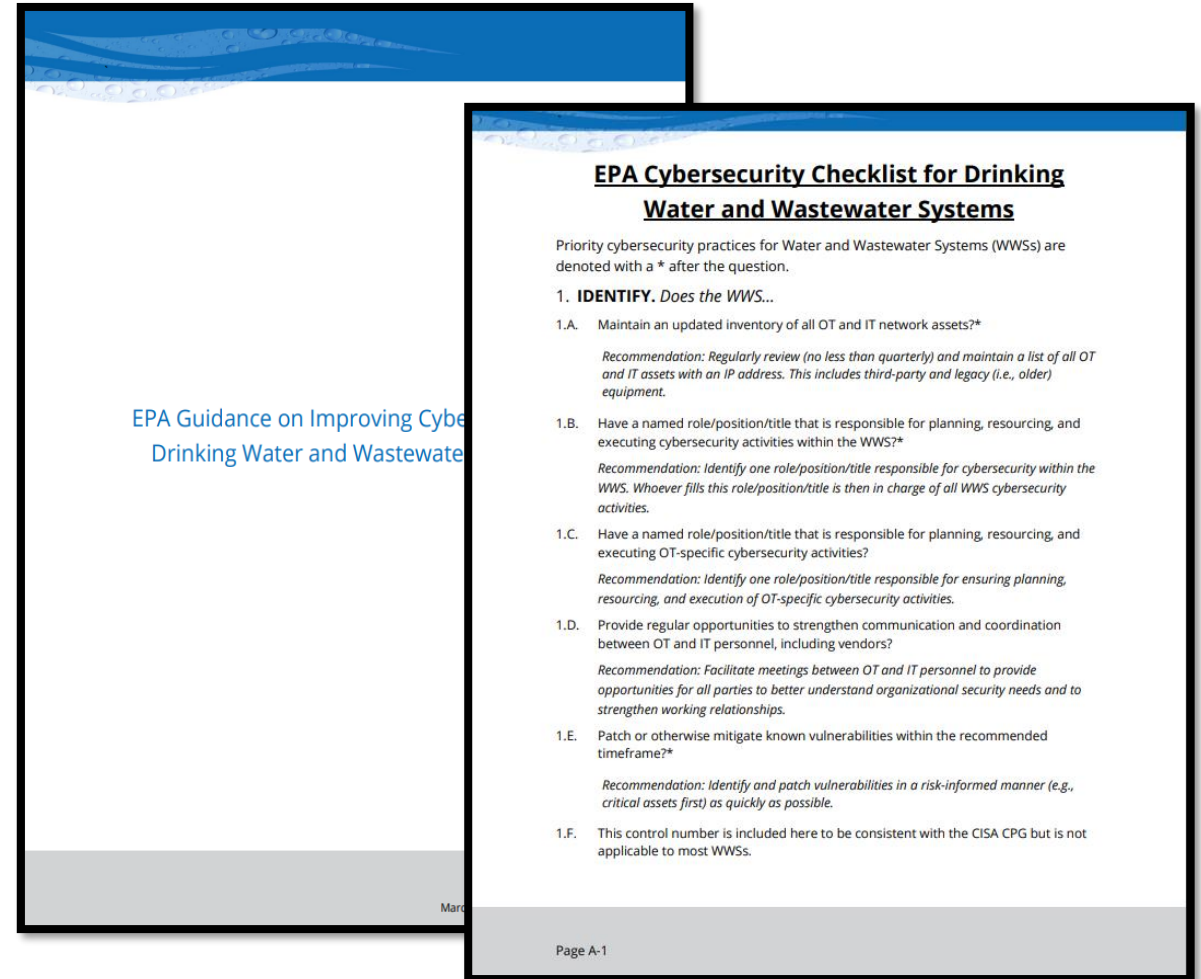


EPA's Cybersecurity Assessment Resources and Technical Assistance



EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems

- Assists owners and operators of drinking water and wastewater systems with assessing gaps in their current practices and identify actions that may reduce the risk from cyberattacks.
- Can be used to comply with RRA and ERP Requirements under SDWA Section 1433.
- Includes information on cybersecurity training, assessments, EPA's cybersecurity checklist and priority cybersecurity practices, technical assistance, and more.



EPA Cybersecurity Checklist Fact Sheets

- Fact Sheets are available for each question on the EPA Checklist and include:
 - Recommendations
 - Overview of why the control is important
 - Additional Guidance
 - Implementation Tips
 - Additional Resources
 - Estimate for Cost, Impact, and Complexity



EPA Water Sector Cybersecurity Evaluation Program



Free third-party cybersecurity assessments provided by EPA for Water and Wastewater Systems to evaluate cybersecurity practices at water and wastewater systems.



The program uses the EPA Cybersecurity Checklist which is derived from CISA's Cross-Sector Cybersecurity Performance Goals (CPGs).



Utilities receive an Assessment Report and a Risk Mitigation Plan template.

EPA Water Cybersecurity Assessment Tool (WCAT)

- Cybersecurity Self-Assessment Tool to evaluate cybersecurity practices at water and wastewater systems.
- The Tool Features:
 - Assessment Workbook
 - Assessment Report
 - Risk Mitigation Plan



Cybersecurity Technical Assistance Program for the Water Sector (Cybersecurity Help Desk)

- EPA provides direct cybersecurity technical assistance for members of the water sector including utilities, primacy agencies, technical assistance providers, and more.
- Cybersecurity Subject Matter Experts respond to requests for technical assistance by phone or email within two business days.



The screenshot shows a web form titled "water utility RISK assessment" in the top left and "CONTACT US" in the top right. The main heading is "Cybersecurity Technical Assistance Program for the Water Sector". Below this is a sub-heading: "Please share your information to request cybersecurity technical assistance." The form contains several input fields: "Contact Name *" (required), "Contact Name 2 (optional)", "Contact Email Address *" (required), "Contact Email Address 2 (optional)", "Contact Phone Number *" (required), "Contact Phone Number 2 (optional)", and "Preferred Method of Contact *" with radio buttons for "Phone" and "Email".

CISA's Free Cyber Vulnerability Scanning for Water Utilities

- **Benefits of this service include:**
 - Identifying internet-accessible assets.
 - Identifying vulnerabilities in internet-connected assets.
 - Weekly reports on scanning status and recommended mitigations.
 - Ongoing detection and reporting with continuous scanning for new vulnerabilities.

Email vulnerability@cisa.dhs.gov with the subject line “Requesting Vulnerability Scanning Services” to request this service.





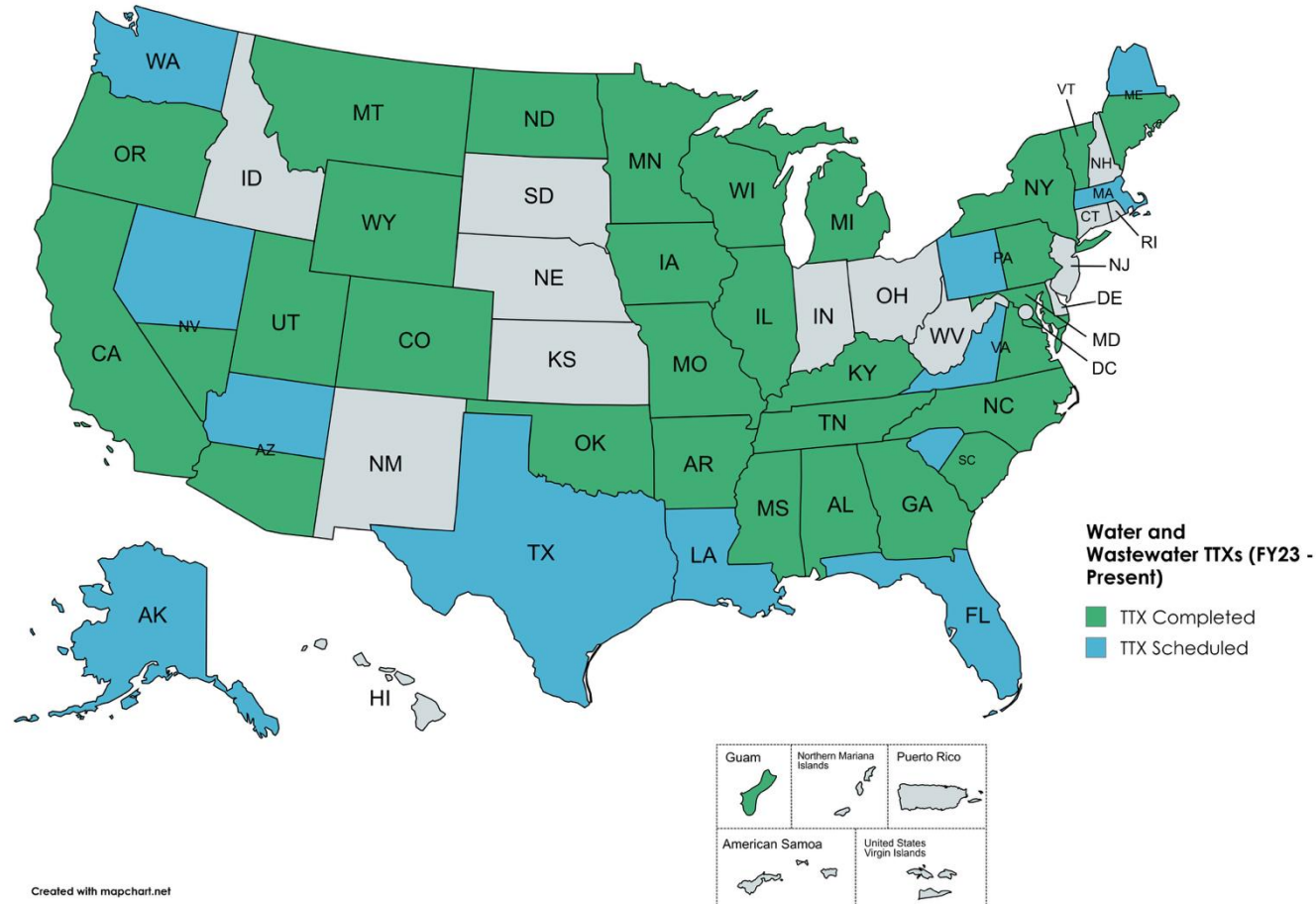
Upcoming Cybersecurity Exercises and Technical Assistance Courses

Upcoming Cybersecurity Exercises and Technical Assistance Courses

- **Cyber 102** – October 7th
- **Cyber 103** – October 14th
- **Cyber Refresher** – October 21st
- **WCAT** – October 28th
- **Cyber Procurement** – October 29th

Cybersecurity Tabletop Exercises

Email
WaterCyberTA@epa.gov to
sign up!





Cybersecurity Incident Response and Planning Resources



Drinking Water and Wastewater Systems CIRP Template

- Assists drinking water and wastewater systems with developing a CIRP
- Includes Instructions and a customizable CIRP template

Drinking Water and Wastewater Systems
Cybersecurity Incident Response Plan Template
Instructions

[Water/Wastewater System Name]

Cybersecurity Incident Response Plan

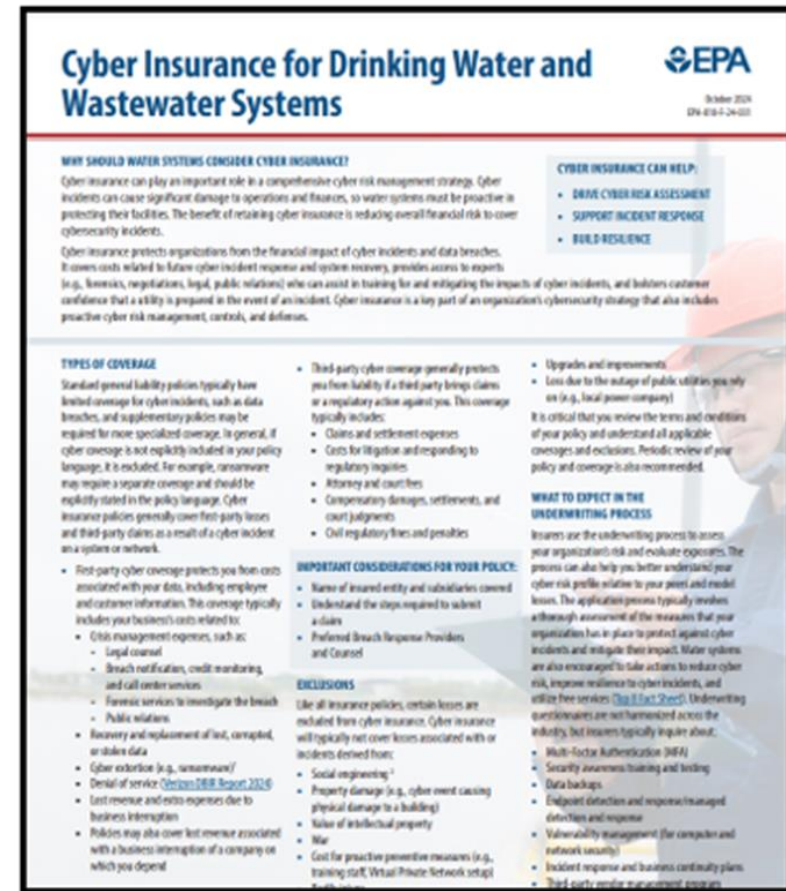
Version [X]

[Date]

This document and associated electronic files may contain sensitive or confidential information.
Please maintain the document/electronic files in a manner that will help safeguard the information.

Fact Sheet: Cyber Insurance for Drinking Water and Wastewater Systems

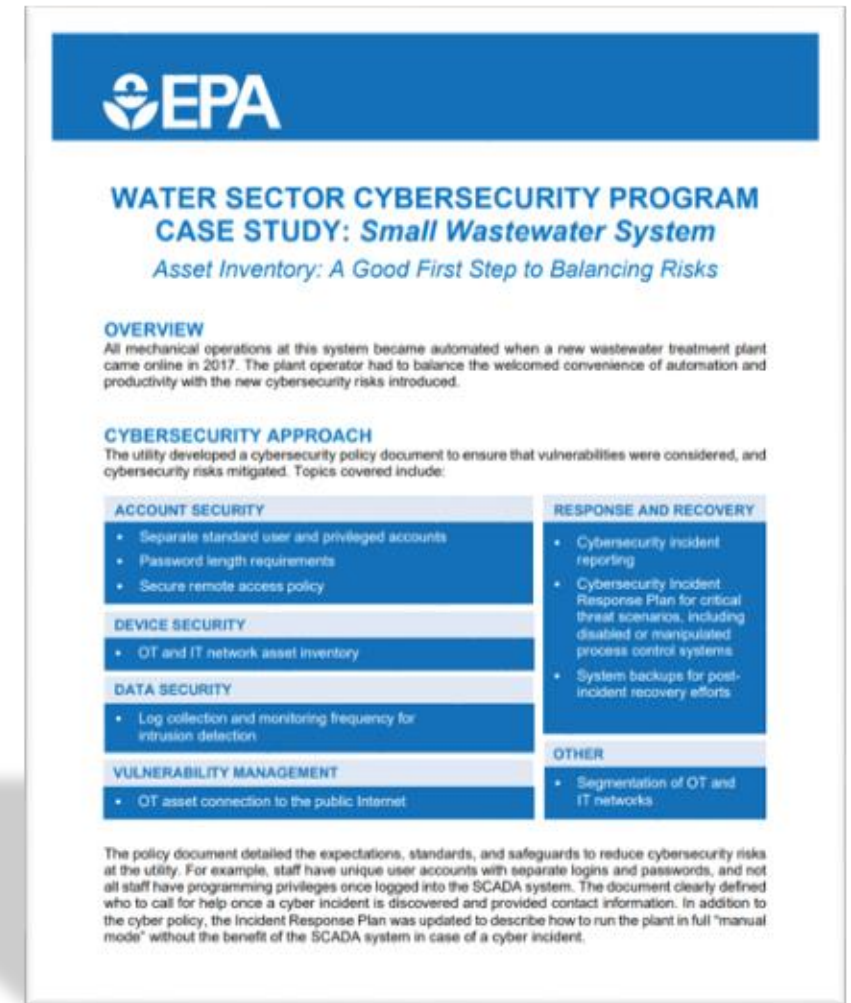
- Provides an in-depth overview of cybersecurity insurance for water and wastewater systems.
- Demonstrates the important role cyber insurance plays in a comprehensive cyber risk management strategy.



Water Sector Cybersecurity Program Case Studies

Case Studies highlighting the cybersecurity success stories at water and wastewater utilities.

- [Small Combined System](#)
- [Small Wastewater System](#)
- [Medium Drinking Water System](#)
- [Medium Drinking Water System #2](#)
- [Medium Combined System](#)
- [Large Combined System](#)



Sign-up to Receive Important Cybersecurity Alerts



[Sign-up for EPA Water Sector Alerts](#)



[Sign-up for CISA Alerts](#)



[Become a member of Water ISAC to receive resources, alerts, and analysis](#)



Water Resilience

[Basics of Water Resilience](#)

[Water Resilience Tools](#)

[America's Water Infrastructure Act \(AWIA\)](#) ▼

[Cybersecurity](#) ^

[Cybersecurity Assessments](#)

[Cybersecurity Planning](#)

[Cybersecurity Exercises and Technical Assistance](#)

[Cybersecurity Response](#)

[Cybersecurity Funding](#)

[Contamination](#)

[Supply Chain Resilience](#) ▼

[Interdependencies](#) ▼

[Events and Assistance Resources](#)

Cybersecurity Funding

Learn about funding options available to support increasing cyber resilience.

[Clean Water State Revolving Fund \(CWSRF\)](#) | [US EPA](#): Provides assistance to any public, private, or nonprofit entity for measures to increase the security of publicly owned treatment works, including cybersecurity.

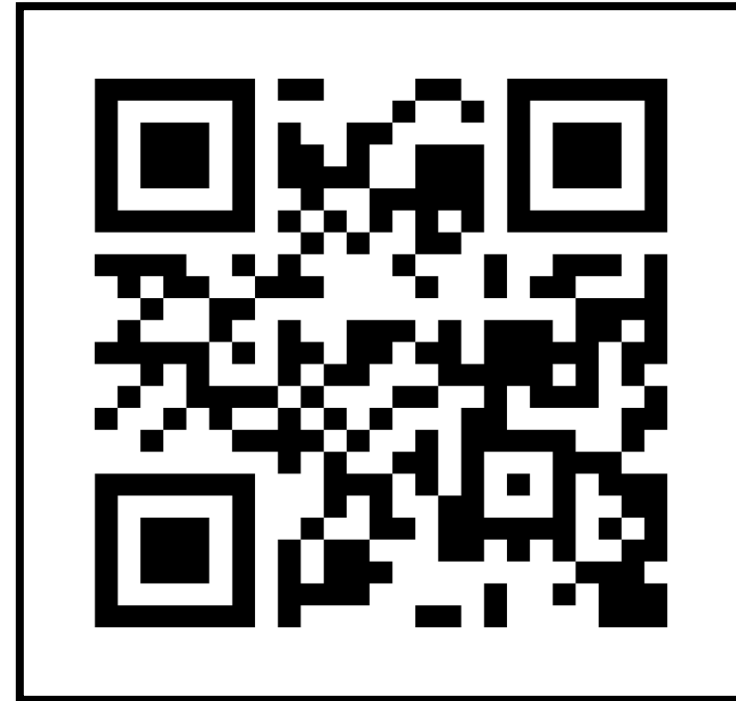
[Drinking Water State Revolving Fund \(DWSRF\)](#) | [US EPA](#): Provides assistance with All-Hazard Risk and Resilience Assessment, Technical Assistance, Equipment, and Infrastructure, including cybersecurity.

[Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program](#) | [US EPA](#): Provides assistance to medium and large sized public water systems to enhance protection of drinking water sources from all hazards, including cybersecurity. This program is coming FY25!

[CISA State and Local Cybersecurity Grant Program \(SLCGP\)](#) [🔗](#): Grant program for states, cities, counties and towns from state administrative agency. Sub-award applications for cities, counties and towns must be submitted to the respective state administrative agency. Find more information here on EPA's [SLCGP Fact Sheet \(pdf\)](#) (144.43 KB, 11/22, EPA-810-F-22-013)



EPA's Cybersecurity for the Water Sector Website



epa.gov/cyberwater

ANCHOR-CI

- **Strategic Federal Partnership:** Chartered by DHS in **June 2026** and administered by **CISA** to provide direct, actionable advice on securing national critical infrastructure and cyberspace.
- **Unified Defense Framework:** Bridges the gap between the federal government, **Sector Risk Management Agencies (SRMAs)**, and local stakeholders to review emerging threats like terrorism and cyberattacks.
- **Proactive Information Exchange:** Fosters the rapid sharing of **security best practices** and vulnerability data to build resilient local infrastructure.
- **Protected, Secure Collaboration:** Operates under a **FACA exemption**, allowing public and private sector leaders to share sensitive threat intelligence in a trusted, closed-door environment.
- Visit cisa.gov/anchor-ci to learn more



Questions?

About the Speaker

- **Brandon M. Carter, Sr.**
Cybersecurity Analyst
 - Carter.Brandon@epa.gov
- **EPA's Office of Water Emergency Response and Cybersecurity (OWERC)**
 - Cybersecurity Division

