INSTITUTE FOR CYBER SECURITY

The Cybersecurity State of the Water Sector

The current state

The water sector remains one of the most cyber-vulnerable U.S. critical infrastructure sectors due to widespread under-resourcing (especially in small and medium systems), legacy OT systems, and persistent exposure of remote access pathways, despite improving federal awareness and a growing set of guidance and assessment mechanisms. (Office, n.d.) Currently, the Institute for Cyber Security at Marshall University translates cybersecurity policy into practical, utility-ready actions, reinforced by Marshall University's targeted microcredential in water sector cybersecurity, which equips professionals with implementable, real-world skills.

Common Water Facility systems

Community water systems across the United States operate a predictable set of facility types and process trains, regardless of size or geography. (Agency, n.d.) These systems typically include source water intakes, treatment plants, distribution networks, and supporting information systems. What differs dramatically is not the underlying technology, but the degree of digitalization, integration, and cybersecurity maturity that supports those processes.

Most facilities rely on Supervisory Control and Data Acquisition (SCADA) platforms, Programmable Logic Controllers (PLCs), sensors, and remote telemetry units to manage treatment operations such as coagulation, filtration, disinfection, and pumping. Even very small utilities now use internet-connected devices to monitor tank levels, pump stations, or chemical dosing. Billing, customer information, and financial systems, often cloud-hosted or consolidated under a single vendor, sit adjacent to or intertwined with operational networks, expanding the attack surface. Across the country, common system elements include:

- Surface-water and/or groundwater intakes with automated pumps and valve controls
- Treatment processes (coagulation/flocculation, sedimentation, filtration, chlorine/UV disinfection) governed by PLC-driven instrumentation
- Chemical storage and feed systems where cyber-manipulation could directly impact public-health-critical dosing
- Storage tanks and remote pump stations, typically monitored through remote terminal units (RTU) or cellular/Internet-based SCADA
- Distribution system booster stations, modeled and controlled to maintain pressure and system integrity
- Business and administrative systems, often vendor-hosted or cloud-based, sometimes sharing infrastructure with operations

However, the sector is marked by extreme variability in system sophistication. Large, investor-owned utilities often maintain modernized control systems, dedicated cybersecurity staff, segmented networks, vendor governance processes, and lifecycle management for OT assets. These systems operate with enterprise-grade cybersecurity capabilities, formal risk assessments, and access-control frameworks that resemble those in the energy sector.

By contrast, most water systems are small municipal utilities or rural co-ops, sometimes serving only a few hundred or a few thousand customers. (State Policy Options for Small and Rural Water Systems, 2022) Many of these systems operate with:

- Minimal or no dedicated IT staff
- Legacy SCADA is reachable through outdated remote-access tools

- Shared or default credentials
- Single-vendor cloud platforms providing billing, finance, and sometimes even remote operational access
- Limited ability to patch, replace, or securely configure PLCs and control hardware

This disparity means that while the physical components of water treatment are broadly similar across the country, the cyber-risk profile varies radically by resource level. A technique that would be easily contained in a highly resourced utility can cause prolonged operational impacts in a small system with limited monitoring, limited segmentation, and no dedicated cybersecurity personnel. This asymmetry is one of the most urgent structural challenges in the water sector today: adversaries scale effortlessly, while most local systems cannot. (Director & Agriculture, 2024) Because these systems share common architectures and common vendor ecosystems, vulnerabilities also repeat across hundreds or thousands of facilities. (Cybersecurity for Rural Water and Wastewater Systems, 2025) This uniformity, combined with inconsistent cybersecurity maturity, makes water infrastructure one of the most attractive targets for both opportunistic and state-linked cyber actors.

Overall posture

Three structural realities define the water sector's cybersecurity baseline:

1. Fragmentation: The U.S. has tens of thousands of water systems with widely varying maturity and budgets; many are small, local-government entities with limited cyber staff. (Water and Wastewater Systems | Cybersecurity and Infrastructure Security Agency CISA, 2024)
2. OT modernization without matching security uplift: Digital transformation (remote operations, telemetry, automation) often outpaces security engineering and governance.
3. Resilience depends on "manual fallback," not assured cyber resilience: Many utilities can revert to manual operations as a short-term safety valve, but extended outages, loss of telemetry, or compromised billing/IT systems can still impose high public and economic costs.

The water sector faces rapidly evolving cyber threats, particularly in operational technology environments. Traditional cybersecurity measures are no longer sufficient, as the emergence of AI-enabled threats has fundamentally changed the dynamics of cyberattacks.

To address this, the water sector should shift toward preemptive cybersecurity measures that act before an attack occurs, rather than merely preparing for one.

- *Preemptive cybersecurity measures are proactive actions and strategies implemented to identify, prevent, and mitigate potential cyber threats before they can cause harm to systems or data.*

The goal is to improve detection of advanced threats, leverage emerging technologies for proactive prevention, and accelerate the transition to post-quantum cryptography.

- *Advanced threats are sophisticated, targeted cyberattacks that use complex tactics and technologies to evade detection and compromise sensitive systems or data.*
  Proactive prevention refers to the ongoing implementation of strategies and technologies designed to anticipate, identify, and block potential cyber threats before they can cause harm.

- *Post-quantum cryptography is the development and use of cryptographic algorithms designed to be secure against attacks from quantum computers, which could break traditional encryption methods.*

Advances in quantum computing will render conventional asymmetric cryptography unsafe. (Baseri et al., 2025) In accordance with NIST standards, the water sector must develop a post-quantum cryptography transition plan and establish a roadmap to a quantum-safe environment as soon as practicable.

- National Institute of Standards and Technology

Known vulnerabilities

AI is already being used to power sophisticated cyberattacks, and the frequency of AI-enabled, scalable, automated cyber espionage will only increase. (Microsoft: Russia, China increasingly using AI to escalate cyberattacks on the US, 2025) This trend will drive the demand for **preemptive countermeasures** and **autonomous cyber-immune systems**.

- *Preemptive countermeasures are proactive actions or strategies implemented to detect, prevent, or neutralize cyber threats before they can compromise systems or data.*
- *Autonomous cyber-immune systems are self-operating security solutions that continuously detect, analyze, and respond to cyber threats by mimicking the adaptive and self-healing properties of biological immune systems.*

The barrier to entry for AI-driven attacks will continue to fall, making sophisticated, large-scale cyberattack campaigns more common. (AI-Powered Cyberattacks Surge as Detection Capabilities Lag, 2024).

Future cybersecurity requirements must focus on active deception, denial, and disruption as non-negotiable architectural principles to preemptively break autonomous attack chains.

- *Autonomous attack chains are sequences of cyberattacks that are automatically executed by intelligent systems or malware with minimal or no human intervention, enabling rapid and adaptive exploitation of vulnerabilities.*

Seek opportunities to reduce spending on misaligned cyber tools, avoid duplicative pilot projects, and accelerate compliance with Zero Trust and post-quantum cryptography mandates.

- Zero Trust is a security framework that requires strict verification of every user and device attempting to access resources, assuming no implicit trust regardless of location or credentials.

Ultimately, the water sector must adopt preemptive cybersecurity solutions and establish autonomous cyber-immune systems to avoid potentially catastrophic losses from these rapidly evolving threats. (Gartner Says That in the Age of GenAI, Preemptive Capabilities, Not Detection and Response, Are the Future of Cybersecurity, 2025).

Across incident reporting, federal advisories, and field assessments, the most common weaknesses are well understood and often preventable:

1. **Internet-exposed operational interfaces and weak remote access controls**
   Joint EPA–CISA guidance specifically warns that internet-exposed human machine interfaces (HMI) create direct pathways to operational disruption and emphasizes hardening remote access, inventorying exposed devices, and improving credential and access controls. (CISA. 2024)
2. **Insecure-by-default industrial components and unaddressed device exposures**
   CISA has warned of active exploitation of PLCs used in water and wastewater

environments, including widely deployed device ecosystems where poor exposure management and weak configuration control magnify risk. (CISA. 2023)

3. **Legacy OT, constrained patch windows, and fragile vendor dependencies**
   Many utilities operate OT with long lifecycles, limited maintenance windows, and vendor-controlled access arrangements. This creates persistent risk where known vulnerabilities remain unmitigated longer than in other sectors.
4. **Identity and access control gaps (no MFA, shared accounts, default credentials)**
   Water-sector compromises repeatedly involve credential weaknesses, poor privilege management, and insufficient segmentation between business IT and operational networks.
5. **Low detection visibility in OT environments**
   Smaller systems often lack continuous monitoring and logging that would enable rapid detection, containment, and forensic understanding of incidents.

Recent compromises and operationally relevant incidents

Recent activity demonstrates that water systems face both criminal and state-linked threats:

1. **Municipal water facility disruption (Kansas, September 22, 2024):** Arkansas City, Kansas reported a cybersecurity incident affecting its water treatment facility, with the city indicating operations remained safe but required precautionary measures (including shifting operating posture). This incident prompted broader federal warnings about ongoing water-sector exposure. (City of Arkansas City faces cybersecurity incident, n.d.)
2. **State-linked OT targeting (Pennsylvania, late 2023)**: The Municipal Water Authority of Aliquippa, Pennsylvania publicly reported an intrusion associated with an IRGC-aligned campaign that impacted a remote pumping station monitoring/control capability (widely cited as OT-focused harassment/defacement but still operationally meaningful). (Water ICS exposures highlight vulnerabilities in Critical Infrastructure Security, 2024)
3. **Broader state-linked targeting patterns (2023–2024):** U.S. government advisories document the targeting and exploitation of PLCs used in water and wastewater and associated campaigns spanning multiple sectors, underscoring that water systems are squarely within adversary target sets. (CISA, 2023)
4. **Evidence of advanced actor interest in water/OT environments (2024):** Independent reporting (including Mandiant/Google reporting cited by media) has likely linked Russian military-intelligence-aligned activity to attacks affecting water utilities. (Vicens & Vasquez, 2024)

Current Policies, Directives, and Government Actions Already Underway

1. **Statutory and regulatory foundation for water-sector cyber risk management**
   - America's Water Infrastructure Act (AWIA) / Safe Drinking Water Act (SDWA)
     - Under SDWA (as amended by AWIA), covered community water systems must prepare and periodically update Risk and Resilience Assessments (RRAs) that include electronic/computer/automated systems security (cybersecurity), and must develop Emergency Response Plans informed by those assessments. EPA's program materials explicitly identify

cybersecurity within scope. (EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems, 2023)

- **Implication**: The law creates a baseline expectation that utilities treat cybersecurity as part of operational risk management, not as an optional IT enhancement.

- **EPA oversight posture and enforcement emphasis (2024)**
  - In May 2024, EPA issued an enforcement alert emphasizing that cyber threats are increasing and urging immediate steps for community water systems to reduce vulnerabilities and align with SDWA §1433 obligations. (Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities, 2024)

2. **Federal operational guidance and advisories (CISA + EPA + sector partners)**
   - **CISA alerts/advisories specific to water and wastewater**
     - CISA has published water-relevant advisories addressing active exploitation of commonly used industrial components and campaigns affecting multiple sectors, including water and wastewater. (Exploitation of unitronics plcs used in water and wastewater systems | CISA 2023)

- **EPA–CISA joint guidance on exposed HMIs (December 2024)**
  - EPA and CISA jointly released guidance specifically warning that internet-exposed HMIs pose a material risk to water/wastewater operations and providing concrete mitigation steps (inventory, access control hardening, remote access restrictions). (CISA and EPA release Joint Fact Sheet detailing risks internet-exposed HMIS pose to WWS sector | cisa, 2024)
  - **Implication**: The federal government is increasingly publishing "operator-usable" technical guidance aimed at the most common, highest-risk exposure patterns.

3. **Federal oversight and risk governance (GAO, 2024)**
   - **U.S. Government Accountability Office (GAO) — Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems (August 2024)**
     - GAO found that the water sector faces increasing cyber risk, documented active foreign and criminal targeting of water utilities, and concluded that EPA has not yet conducted a comprehensive sector-wide cyber risk assessment or developed a national cybersecurity strategy for the sector. GAO further noted that EPA plans to increase inspections and enforcement activity focused on cybersecurity under existing SDWA authority. (Critical Infrastructure Protection: EPA urgently needs a strategy to address cybersecurity risks to water and Wastewater Systems, 2024)

     - **Implication**: Independent federal oversight formally recognizes water-sector cybersecurity as a systemic national risk and identifies EPA's regulatory and inspection authority as the primary mechanism for managing that risk, reinforcing cybersecurity as a governance and compliance obligation rather than a voluntary best practice.

   - **Executive-branch critical infrastructure cybersecurity directive (NSM-22, 2024)**

- **National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) — April 2024**
  - NSM-22 designates EPA as the Sector Risk Management Agency for water and wastewater systems, directs federal agencies to identify, assess, and prioritize sector cyber risks, and instructs agencies to use regulatory authorities to establish minimum security and resilience requirements for critical infrastructure, consistent with the National Cybersecurity Strategy. (The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience, 2026)
  - **Implication**: Executive-branch policy now explicitly frames water-sector cybersecurity as part of national critical infrastructure security and authorizes the use of regulatory mechanisms to impose minimum cybersecurity requirements, signaling a shift from voluntary guidance toward enforceable sector-wide resilience standards.

Marshall University's Institute for Cyber Security's Impact on Water Sector Cybersecurity

Through the community-embedded work of the Institute for Cyber Security (ICS), in partnership with CISA, West Virginia water utilities are receiving hands-on cybersecurity support that directly addresses the most persistent risks facing small and mid-sized systems nationwide. These engagements demonstrate how federally aligned expertise can be translated into practical, operational improvements at the local level, where cybersecurity gaps are often greatest, and resources are most constrained.

Strengthening Small-Town Water Systems: Town of Ansted

In Ansted, the ICS is guiding the town through a critical transition from paper-based processes to modern digital systems supporting billing, finance, and a new sewer treatment plant. With no in-house IT staff, Ansted faces the same challenge as thousands of rural utilities across the country: modernization without the internal expertise to manage cyber risk. ICS, in coordination with CISA, provided structured risk framing, vendor-focused cybersecurity due diligence, and practical guidance on separating operational technology (OT) from business systems, controlling remote access, establishing asset inventories, and improving staff cyber awareness.

As the project progressed, the ICS helped town leadership recognize the expanded risk profile created by consolidated financial, payroll, and billing data within a single vendor platform. The ICS translated cybersecurity from an abstract concern into concrete governance questions, data hosting, responsibility boundaries, backup and recovery, testing environments, and compliance obligations, empowering the town to engage vendors from a position of informed oversight. Importantly, the ICS also began developing scalable training and micro-credential models tailored to small municipalities. Reinforcing that cybersecurity resilience depends on every department, not just water operators.

Supporting Critical Infrastructure Modernization: Huntington Water System

At a larger scale, the ICS is supporting the Huntington Water System as it prepares a major operational upgrade, transitioning part of its treatment process to a digitally controlled ultraviolet

(UV) system. This modernization introduces new automation, sensors, and control dependencies, exactly the conditions that increase cyber-physical risk if security is not addressed early.

The ICS conducted on-site technical engagements with Huntington Water leadership, operational staff, and National Guard cyber units to review the existing OT environment and the planned system architecture. These collaborative walkthroughs established a shared understanding of how new digital components will integrate with legacy infrastructure and identify cybersecurity considerations before full implementation, rather than after deployment. Huntington Water has expressed a strong interest in continuing assessments with the ICS as the project advances, embedding cybersecurity into the lifecycle of infrastructure modernization.

In parallel, ICS is supporting workforce readiness by helping design cybersecurity training pathways that provide baseline awareness for all employees and specialized OT-focused guidance for operators, mirroring the approach taken in Ansted and reinforcing a consistent regional model.

Demonstrated National Value

Together, these engagements illustrate Marshall University's role as a trusted intermediary between federal guidance and local execution. Rather than issuing recommendations, the Institute for Cyber Security (ICS) embeds cybersecurity into vendor governance, workforce training, IT/OT separation, and modernization efforts in ways utilities can sustain. This approach is reinforced through Marshall University's dedicated microcredential in water sector cybersecurity, which equips practitioners with applied, utility-ready skills and ensures guidance is translated into consistent, repeatable practice.

In an environment where water systems are increasingly targeted yet unevenly resourced, Marshall University's Institute for Cyber Security demonstrates how academic expertise, federal partnerships, and community-focused engagement can materially strengthen the cybersecurity posture of critical infrastructure at the point of greatest vulnerability, while providing a scalable model for rural and Appalachian communities nationwide.

Resources:

Agency, U. E. (n.d.). America's Water Infrastructure Act (AWIA) – Section 2003. https://www.epa.gov/system/files/documents/2023-02/8296_AWIA%20Study%20on%20Intractable%20PWS_RTC_Transmitted_08-30-22.pdf

Baseri, Y., Chouhan, V., Ghorbani, A. & Chow, A. (2025). Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity—Threats, Mitigations, and Solutions. ScienceDirect. https://doi.org/10.1016/j.cose.2025.01.001

Censys. (2024, February 8). Water ICS exposures highlight vulnerabilities in Critical Infrastructure Security. Water ICS Exposures Highlight Vulnerabilities in Critical Infrastructure Security. https://censys.com/blog/water-ics-exposures-highlight-vulnerabilities-in-critical-infrastructure-security

CISA. (2023, November 28). Exploitation of unitronics plcs used in water and wastewater systems | CISA. Exploitation of Unitronics PLCs used in Water and Wastewater Systems. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

CISA. (2024, December 13). CISA and EPA release Joint Fact Sheet detailing risks internet-exposed HMIS pose to WWS sector | cisa. CISA and EPA Release Joint Fact Sheet Detailing Risks Internet-Exposed HMIs Pose to WWS Sector. https://www.cisa.gov/news-events/alerts/2024/12/13/cisa-and-epa-release-joint-fact-sheet-detailing-risks-internet-exposed-hmis-pose-wws-sector

EPA Office of Water (4608T). (2023, March 23). EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems . https://www.epa.gov/system/files/documents/2024-08/epa-guidance-on-improving-cybersecurity-at-drinking-water-and-wastewater-systems-1.pdf

Environmental Services Administration. (n.d.). City of arkansas city faces cybersecurity incident. Arkansas City Kansas. https://www.arkcity.org/environmental-services/page/city-arkansas-city-faces-cybersecurity-incident

EPA. (2024, May). Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities. https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities

Office, U. G. (n.d.). Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems. https://www.gao.gov/products/gao-24-106744

The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience. (2026, January 29). https://www.congress.gov/crs-product/IF12716

U.S. Government Accountability Office. (2024, August 1). Critical Infrastructure Protection: EPA urgently needs a strategy to address cybersecurity risks to water and Wastewater Systems.

Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems | U.S. GAO. https://www.gao.gov/products/gao-24-106744

Vicens, A., & Vasquez, C. (2024, April 17). Mandiant: Notorious Russian hacking unit linked to breach of Texas Water Facility. CyberScoop. https://cyberscoop.com/sandworm-apt44-texas-water-facility/

(2022). State Policy Options for Small and Rural Water Systems. National Conference of State Legislatures. https://www.ncsl.org/environment-and-natural-resources/state-policy-options-for-small-and-rural-water-systems

Director, W. H. & Agriculture, U. S. (September 30, 2024). Cybersecurity Circuit Rider Program Study. National Rural Water Association. https://nrwa.org/cybersecurity-circuit-rider-program/

(2025). Cybersecurity for Rural Water and Wastewater Systems. U.S. Department of Agriculture Rural Development. https://www.rd.usda.gov/about-rd/initiatives/cybersecurity-rural-water-and-wastewater-systems

(2024). Water and Wastewater Systems | Cybersecurity and Infrastructure Security Agency CISA. CISA. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector

(October 14, 2025). Microsoft: Russia, China increasingly using AI to escalate cyberattacks on the US. Associated Press. https://apnews.com/article/ad678e5192dd747834edf4de03ac84ee

(April 4, 2024). AI-Powered Cyberattacks Surge as Detection Capabilities Lag. MSPAA. https://mspaa.net/detection-capabilities/

(September 17, 2025). Gartner Says That in the Age of GenAI, Preemptive Capabilities, Not Detection and Response, Are the Future of Cybersecurity. Gartner. https://www.gartner.com/en/newsroom/press-releases/2025-09-18-gartner-says-that-in-the-age-of-genai-preemptive-capabilities-not-detection-and-response-are-the-future-of-cybersecurity