TLP:CLEAR

Q2 2025

Water & Wastewater Sector

A Quarterly National Security Information-Sharing Bulletin from the U.S. Environmental Protection Agency and the Water Information Sharing and Analysis Center

In This Issue

Executive Order 14239: Achieving Efficiency Through State and Local Preparedness

On March 19, 2025, President Trump signed the Executive Order "Achieving Efficiency Through State and Local Preparedness" (E.O. 14239). The Order enables state and local governments to better understand, plan for, and address the needs of their citizens by reducing the complexity of federal preparedness and response policies.

This approach prioritizes risk informed decision making, empowering state and local governments to take greater responsibility for preparedness, while further underscoring that all critical infrastructure organizations play a role in supporting national security. This joint Information Sharing Bulletin (ISB) supports this effort by providing awareness on priority security and resilience topics impacting the water and wastewater sector.

The Order requires the National Security Advisor to publish a National Resilience Strategy (within 90 days) that articulates the priorities, means, and ways to advance the resilience of the nation. The Order requires a review of all infrastructure, continuity, and preparedness policies to modernize and simplify federal approaches, aligning them with the National Resilience Strategy. This includes:

- Reviewing and recommending revisions to national critical infrastructure policy (within 180 days), including moving from an "all-hazards" approach to a risk-informed approach, prioritizing resilience and action over mere information sharing. This will include a review of National Security Memorandum 22 or April 30, 2024 (Critical Infrastructure Security and Resilience) which among other things identified the 16 sectors and respective Sector Risk Management Agencies.

- Reviewing and revising national continuity policy (within 180) to modernize its framework, streamline operations, and right-size the federal footprint for sustained readiness.
- Evaluating national preparedness policies (within 240 days) to reformulate the process and metrics for federal responsibility.

The Order also creates a National Risk Register (withing 240 days) to identify, describe, and measure risks to our national infrastructure, related systems, and their users to guide smarter spending and planning. In addition, the Secretary of Homeland Security is required (within 1 year) to propose changes to the various functions that organize national preparedness and continuity.

Ultimately, the new Order emphasizes common-sense investments by states and localities to enhance security, safeguard taxpayers, and protect American lives. Together, these initiatives aim to build resilience against evolving threats while ensuring public health and safety.

2024 Cyber Incidents Impacting the Water Sector: Threat Actors and TTPs

In 2024, the water and wastewater sector experienced an increasing number of cyber incidents that exposed critical vulnerabilities in its operational technology and information technology systems. These attacks were carried out by nation-state actors and cyber-criminal groups, targeting vital infrastructure with the potential to disrupt essential services and erode the public's trust in the safety of the water supply.

Amid the overall uptick in attacks against the water and wastewater utilities, there were several high-profile cyber-attacks, in 2024, targeting the water sector that underscored critical vulnerabilities at the intersection of IT and OT systems.

- One of the most prominent incidents was the attack in October on American Water, the largest U.S. water utility serving over 14 million people, which disrupted its billing systems and customer service platform for a week, though water operations remained unaffected.

- Earlier in January, a Russian-linked hacktivist group targeted a water utility in Muleshoe, Texas, exploiting SCADA system vulnerabilities to cause a tank to overflow for 30 - 45 minutes. Similar cyber incidents were reported in nearby towns, highlighting the risks posed by weak or default credentials in remote access software.

The primary threat actors targeting the sector included pro-Russian hacktivist groups such as the "People's Cyber Army," Iranian-backed organizations like "CyberAv3ngers," and Chinese state-sponsored groups, such as "Volt Typhoon," as well as various cyber criminal networks.

The tactics, techniques, and procedures (TTPs) employed during these attacks ranged from exploiting default or weak credentials on SCADA systems and programmable logic controllers (PLCs) to deploying ransomware, phishing campaigns targeting employees through social engineering, and exploiting unsecured remote access points to gain unauthorized access to OT environments. Additionally, poor IT/OT network segmentation facilitated lateral movement between networks, further exacerbating vulnerabilities.

The increasing frequency and sophistication of cyber-attacks targeting the water sector demand immediate action to safeguard public health and ensure uninterrupted services.

In response to the heightened threat, CISA, EPA, FBI, and WaterISAC have jointly issued these recommendations to mitigate the risk of an attack:

1. Enforce user access controls and multi-factor authentication for all critical systems
2. Conduct cybersecurity risk assessments focused on reducing public internet exposure
3. Inventory ICS assets to identify and manage vulnerabilities
4. Change default passwords immediately
5. Strengthen network segmentation between IT and OT environments
6. Implement regular cybersecurity assessments and awareness training
7. Develop and exercise incident response and recovery plans 💧

Additional Reading:

CISA - Nation-State Cyber Actors

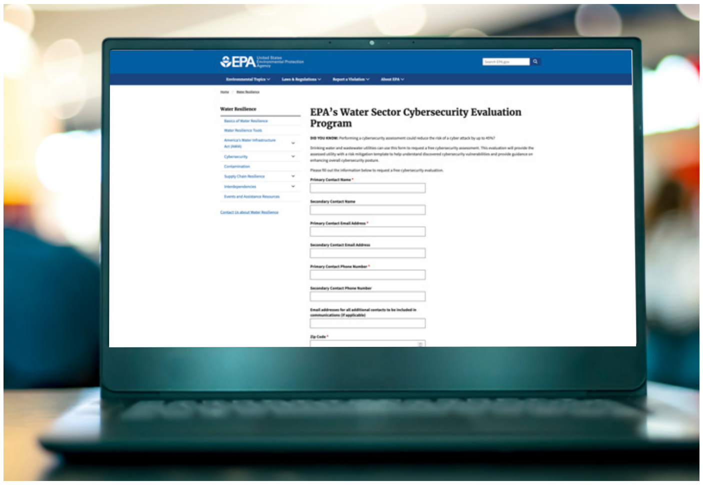
Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

CISA warns of continuing attacks on water systems after Kansas town reports incident

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

EPA's Free Cyber Evaluation Services

The EPA conducts a free cybersecurity assessment for Water/Wastewater Systems (W/WSs) to identify gaps or vulnerabilities in information technology (IT) and operational technology (OT) using the EPA Cybersecurity Checklist. A W/WS must register to receive a cybersecurity assessment. Once registered, an EPA contractor will contact the W/WS to gather basic information, provide guidance on how to prepare and schedule an assessment.



EPA's Water Sector Cybersecurity Evaluation Program

DID YOU KNOW: Performing a cybersecurity assessment could reduce the risk of a cyber attack by up to 45%?

Drinking water and wastewater utilities can use this form to request a free cybersecurity assessment. This evaluation will provide the assessed utility with a risk mitigation template to help understand discovered cybersecurity vulnerabilities and provide guidance on enhancing overall cybersecurity posture.

Please fill out the information below to request a free cybersecurity evaluation.

Primary Contact Name *

Secondary Contact Name

Primary Contact Email Address *

Secondary Contact Email Address

Primary Contact Phone Number *

Secondary Contact Phone Number

Email addresses for all additional contacts to be included in communications (if applicable)

Zip Code *

During the assessment, the EPA contractor will ask the W/WS each of the questions in the Cybersecurity Checklist. The contractor will generate a report that identifies cybersecurity gaps and/or vulnerabilities in the W/WS's IT/OT based on response to the Cybersecurity Checklist. In addition, a template for a Risk Mitigation Plan will be generated, which the W/WS can use to plan and document actions to address cybersecurity gaps. 💧

To register your W/WS, please visit: *https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program*

CISA's Free Cyber Vulnerability Scanning Services Available to Water and Wastewater Utilities

Water and wastewater utilities can greatly reduce the risk of experiencing cyber attacks by externally scanning their networks for vulnerabilities caused by publicly facing devices. Towards that effort, the Cybersecurity and Infrastructure Security Agency (CISA) can help your utility identify and address vulnerabilities with a no cost vulnerability scanning service subscription.

CISA's vulnerability scanning program continuously assesses the health of internet-accessible assets by checking for known vulnerabilities, weak configurations—or configuration errors—and suboptimal security practices at participating organizations. Immediate practical benefits for utilities enrolling in this service include:

- Identifying internet-accessible assets
- Identifying vulnerabilities in your utility's assets connected to the internet, including Known Exploited Vulnerabilities and internet-exposed services commonly used for initial access by threat actors and some ransomware gangs
- Weekly reports on scanning status and recommendations for mitigating identified vulnerabilities
- Significant reduction in identified vulnerabilities in the first few months of scanning for newly enrolled water utilities
- Ongoing detection and reporting with continuous scanning for new vulnerabilities

CISA, EPA, WaterISAC, the Water Sector Coordinating Council (WSCC), and the Association of State Drinking Water Administrators (ASDWA) encourage water and wastewater utilities to enroll in this free service to help network defenders reduce exposure to cyber threats by taking a proactive approach to mitigating potential attack vectors. 💧

Read more about the free vulnerability scanning program at CISA **or** *watch a related video here*.

The U.S. Intelligence Community's 2025 Annual Threat Assessment Highlights the Growing Cyber Threat to the Water Sector and the Enduring Threat of Violent Extremists

The Office of the Director of National Intelligence (ODNI) recently released its 2025 Annual Threat Assessment of the U.S. Intelligence Community, highlighting the growing cyber threat to water and wastewater utilities, as well as the heightened threat environment from violent extremists.

The assessment notes that state actors like Russia, China, Iran, and North Korea, as well as non-state actors, pose immediate threats to U.S. national interests and critical infrastructure. **For the first time, the report states that "U.S. water infrastructure has become a more common target**. In October 2024, criminal actors conducted cyber-attacks against both large and small water utilities in the United States, possibly inspired by attacks against water infrastructure by Russian hacktivists and Iranian cyber actors in 2023 that had little effect but drew substantial publicity." The assessment—based on data collected from November 2023 to April 2024, which was highlighted in a U.S. government graphic—reveals the expanding cyber activity targeting key infrastructure sectors that could ultimately impact U.S. national security.

Moreover, terrorist and transnational criminal organizations pose direct threats to the homeland. Among foreign terrorist organizations, the report assesses the Islamic State's "most aggressive branches, including ISIS-Khorasan (ISIS-K), and its entrepreneurial plotters will continue to seek to attack the West, including the United States, via online outreach and propaganda aimed at directing, enabling, or inspiring attacks, and could exploit vulnerable travel routes."

In addition, Russia, China, Iran and North Korea—individually and collectively—are challenging U.S. interests in the world, seeking to challenge U.S. dominance and sow fear in our local communities. Critically, this growing alignment heightens geopolitical tensions and increases the chances of these nations coordinating their actions during a crisis or war.

These findings emphasize the escalating threat landscape facing U.S. critical infrastructure and the imperative for organizations to implement robust physical and cybersecurity strategies to protect essential services. ***Read the full threat assessment here***. 💧

DHS Office of Intelligence & Analysis Threat Briefings

The DHS Office of Intelligence & Analysis (I&A) is a member of the U.S. Intelligence Community (IC) and routinely supports the Water and Wastewater Systems Sector in its intelligence mission. I&A is the only IC element statutorily charged with delivering intelligence to our State, Local, Tribal and Territorial (SLTT) and private sector partners at the lowest possible classification level.

Concurrently, I&A works with those partners to develop unique intelligence insight that informs DHS Intelligence Enterprise and IC partners. Within I&A, the Cyber Intelligence Center (CIC) serves I&A's analytic and research arm for finished all-source analysis of cyber threats to critical infrastructure, including the Water and Wastewater Systems Sector.

CIC hosts an UNCLASSIFIED//FOR OFFICIAL USE ONLY Bi-Weekly Cyber Threat Intelligence Teleconference which highlights current and emerging issues in the cyber threat landscape and serves as a conduit to other DHS and federal government cyber threat intelligence resources. Recommended participants for these calls include private and public sector cyber security and/or intelligence professionals who in the course of their work support cyber/information or critical infrastructure security. **If you are interested in participating this call or in CIC's mission, contact cyber@hq.dhs.gov.** 💧

Protecting Water Infrastructure: Understanding Federal Legal Consequences

Recent years have seen a disturbing rise in attacks and security breaches targeting water utilities across the United States. In March 2024, the Cybersecurity and Infrastructure Security Agency (CISA) reported the Water and Wastewater Sector is continuously targeted by a variety of threat actors, including opportunists, hacktivists, nation-state actors, financially motivated actors, and insider threats. State and federal intelligence agencies have documented multiple sophisticated attempts to compromise water treatment facilities, ranging from cyberattacks that target control systems to physical intrusion attempts at critical water infrastructure sites.

EPA Criminal Investigation Division: Protecting Water Critical Infrastructure

The Environmental Protection Agency's Criminal Investigation Division (EPA CID) protects the environment and human health through the investigation and prosecution of criminal conduct and is focused on defending water infrastructure. EPA CID agents are the primary federal experts in investigating serious environmental crimes. The Safe Drinking Water Act specifically criminalizes Tampering with a Public Water System, a federal charge that carries significant legal consequences for those who intentionally threaten water infrastructure with the intent to cause harm. Through independent investigations and joint task force memberships across the country, EPA CID works closely with your local law enforcement and federal partners including the FBI, EPA OIG, and DHS, to use this powerful legal tool to investigate and prosecute individuals who attempt to compromise public water systems.

Federal Protections and Penalties

Under federal law, intentional interference with public water systems is a grave criminal offense. The Safe Drinking Water Act provides substantial criminal penalties, including possibly 20 years in federal prison and fines exceeding $250,000. In addition to criminal penalties, civil penalties of up to $1,000,000 for tampering and up to $100,000 for attempts or threats may apply.

- Water utility tampering may involve:
- Computer network intrusions
- Unauthorized access to water treatment facilities
- Intentional contamination of water supplies
- Sabotaging water treatment equipment
- Disrupting water distribution systems
- Introducing harmful substances into water infrastructure

Reporting Criminal Activities

If you observe any suspicious behavior or potential security threats, please consider:

- Contacting local law enforcement immediately
- Notifying Federal Partners
    - Local FBI Field Office or 1-800-CALL-FBI
    - Cybersecurity and Infrastructure Security Agency, 888- 282-0870
    - Environmental Protection Agency, WICRD-outreach@epa.gov

Protecting our water infrastructure is a shared responsibility. Any deliberate attempt to compromise these critical systems will be met with the full force of federal law.

Remember: Protecting Water = Protecting Lives 💧

Insider Threat Corner – Unintentional Negligence

An unintentional insider threat is a risk posed by employees, third-party vendors, or contractors who compromise security, cause damage to infrastructure or loss of information through negligence, errors, or lack of awareness without malicious intent. Water infrastructure is critical for the functioning of society. Any disruptions may have severe consequences on public health and safety in a short period of time.

Causes:

- **Negligence:** Being careless or taking short-cuts
- **Lack of awareness:** Insufficient knowledge of procedures and protocols
- **Errors:** Mistakes in following procedures and using systems

Example:

- Clicking on a phishing email
- Attaching a wrong document to an email
- Sending an email to the wrong person
- Taking short-cuts in everyday tasks
- Not having appropriate security configuration for IT equipment
- Ignoring security updates and patches
- Using default passwords
- Misplacing or losing devices
- Unintentionally altering chemical levels

Consequences of unintentional insider threat actions:

- Disruption in water supply
- Threats to public safety e.g. un- or under-treated contaminated drinking water made publicly available
- Public required to take safety precautions (boiling water)
- Financial losses

- Data/infrastructure/facility breaches
- Compromised company or customer sensitive or financial information

Two past cases of unintentional insider threat incidents impacting the water and wastewater sector include:

- A small combined utility experienced a spike in chlorine levels after an **employee error**, which led to additional operational disruptions. The utility said an inexperienced employee had mistakenly turned off a chlorine level monitor during a routine procedure but failed to turn it back on, resulting in chlorine levels three times higher than normal pumped into the utility's water system for 12 hours. The utility spent several weeks recovering from the incident.

- In an incident reported to WaterISAC, a utility employee negligently left the main gate open to facilitate access for construction workers who were working at the water treatment plant. This resulted in criminals gaining unauthorized access to the plant by easily driving their vehicle into the facility via the main gate. The criminals were tracked on a security camera stealing the utility's scrap metal.

Read more about insider threats at CISA here.

Useful Links and Contact Information

For feedback, comments or questions related to the content in this bulletin, please email Water-NSISB@epa.gov

WaterISAC

Website | www.waterisac.org/

Membership Information | www.waterisac.org/membership

Incident Reporting Form | www.waterisac.org/report-incident

24 Hour Line | 866-H2O-ISAC

EPA

Office of National Security | www.epa.gov/national-security

Drinking Water and Wastewater Resilience Website | www.epa.gov/waterresilience

Cybersecurity for the Water Sector | www.epa.gov/waterresilience/epa-cybersecurity-water-sector

Water Sector Coordinating Council

- American Water Works Association
- Association of Metropolitan Water Agencies
- National Association of Clean Water Agencies
- National Association of Water Companies
- National Rural Water Association
- Water Environment Federation
- WaterISAC
- Water Research Foundation