Three questions every water utility should be able to answer this week

Federal investigators will spend weeks on attribution. The people who run treatment and distribution systems have a more immediate problem — and it is one they can act on now.

InflexionPoint News brief 5 minute read

Federal agencies are investigating a coordinated cyberattack that affected municipal water systems across multiple states this week, including more than 30 systems in Minnesota. Investigators are examining whether the activity originated with Iran-affiliated actors, though attribution has not been confirmed and may not be for weeks.

The attribution question will dominate the news cycle. For the people who actually run treatment and distribution systems, it is the least useful part of the story.

What matters more is the target. This activity reached operational technology — the PLCs, HMIs, and SCADA systems that move water — not just the business network. And it follows a pattern that has been building for years, not a single geopolitical moment.

THE RECOGNIZABLE PROFILE

- Flat network — SCADA VLAN one bad rule from the business network
- Cellular modems at remote sites, unaudited since commissioning
- Integrator and OEM access still live from a 2019 project
- Firmware that cannot be patched without a planned outage
- One or two people who understand the whole system — both near retirement

Not just one headline. A pattern.

In November 2023, attackers took an internet-connected pressure controller offline at the Municipal Water Authority of Aliquippa, Pennsylvania. The device shipped with a publicly published default password. The utility had a manual backup and kept pumping.

In January 2024, plants in four small Texas cities — Hale Center, Muleshoe, Lockney, and Abernathy — were hit in a coordinated set of intrusions. Video posted by the purported attackers showed them inside SCADA systems, adjusting settings remotely. In Muleshoe, a water tank overflowed for roughly 30 minutes. The common thread was the vendor software the communities used for remote access.

Two more followed: Tipton, Indiana in April 2024 and Arkansas City, Kansas in September 2024. Both caught the activity and moved to manual control.

Four events, four states, same class of target. In nearly every case the entry point was the same — a control device or remote-access path reachable from the public internet, protected by a credential the vendor shipped and nobody changed. The exposure is structural, and it is not unique to Minnesota.

Why water utilities are structurally exposed

Most community water systems were not designed to be defended. They were designed to run reliably for thirty years with a small crew.

That produces a recognizable profile: a flat network where the SCADA VLAN and the business network are one bad rule apart. Remote lift stations and booster stations reached over cellular modems that nobody has audited since commissioning. Integrator and OEM remote access still active from a project that closed in 2019. Controllers running firmware that cannot be patched without a planned outage nobody wants to schedule. And one or two people who understand the whole system, both of whom are near retirement.

None of that is negligence. It is the accumulated result of doing more with less for a long time.

THE THREE QUESTIONS

Answer these with evidence, not assumption

Before evaluating any tool, service, or grant application, a utility should be able to answer all three.

01

Can you produce a current inventory of every device on your OT network — including remote sites — and identify which of them are reachable from outside your perimeter?

02

Do you know every active remote access path into your control system, who owns each one, and whether any of them still use default or shared credentials?

03

If a controller's logic were modified at 2:00 a.m. on a Sunday, how long would it take you to know?

> Utilities that cannot answer all three do not have a technology problem yet. They have a visibility problem, and visibility is what an assessment is for.

Start with CISA. It costs nothing.

Before spending a dollar with anyone, enroll in CISA's Cyber Hygiene Services. It is free, it is endorsed by EPA, the Water Sector Coordinating Council, and the Association of State Drinking Water Administrators, and there is no defensible reason for a community water system not to be subscribed.

What you get is real. CISA runs continuous automated scanning against your internet-facing assets, flags Known Exploited Vulnerabilities and the exposed services that ransomware operators typically use for initial access, and sends recurring reports with mitigation recommendations.

FREE, FEDERAL

CISA Cyber Hygiene Services

Continuous external scanning of internet-facing assets, with recurring reports and mitigation recommendations. No cost to enroll.

STANDARD

IEC 62443

The international standard for industrial automation and control system security — the frame a defensible OT assessment is written against.

Where the free scan stops

Understanding the boundaries of the service matters as much as enrolling in it, because two limitations are easy to miss.

LIMITATION ONE

It is external only. By design, CISA's scanning is a non-intrusive review of internet-accessible systems. It does not reach inside your private network and it cannot change anything. That means it sees nothing about the segmentation between your business network and your SCADA VLAN. Nothing about default credentials on a controller that is not internet-facing. Nothing about the vendor VPN account that has been live since commissioning. Nothing about a cellular-connected RTU at a remote lift station that may not appear in your declared IP ranges at all. The findings that would have mattered most in several recent water sector incidents sit in exactly that blind spot.

LIMITATION TWO

It produces findings, not fixes. This is the more consequential limit. A weekly report identifying an exposed service is useful only to the extent that someone with OT-specific judgment closes it — during a maintenance window, without tripping a process, on equipment that cannot simply be rebooted. CISA is not staffed to do that work, and does not claim to be. For a utility running on two or three people who already own everything from pump maintenance to compliance reporting, the gap between "we received a report" and "we remediated it" is where risk actually lives.

Scanning tells you where the unlocked doors are. It does not lock them.

From findings to fixed

The work that closes the loop is not glamorous and it is not a product purchase. Whether findings come from a CISA scan or a full IEC 62443-aligned assessment, remediation on a water or wastewater system generally means:

01	Removing or properly brokering internet-exposed assets that never should have been reachable
02	Replacing default, shared, and legacy credentials across controllers, HMIs, and engineering workstations
03	Inventorying and consolidating undocumented remote-access paths, and assigning an owner to each one that survives
04	Bringing cellular connectivity at remote and unmanned sites under managed, monitored control
05	Establishing real segmentation between IT, OT, and safety systems — not a VLAN tag and a hope
06	Correcting firewall rule sets that accumulated over years of project work
07	Standing up detection and response, so that question three has an answer measured in minutes

Each of those has to be sequenced around plant operations, budget reality, and staffing that is already fully committed. That sequencing is the actual deliverable.

InflexionPoint works with water and wastewater utilities on the part that comes after the findings. We conduct vendor-neutral OT cybersecurity risk assessments aligned to IEC 62443 — and we remediate what gets identified, whether the source is our assessment or a CISA scan you are already receiving.

We are not reselling a security product, and we do not hand you a report and leave. As an Operating Partner, we stay in the environment: monitoring, hardening, and adapting as the threat picture and your infrastructure both change.

Call us today to schedule a quick evaluation of your network along with a custom report for next steps to secure your infrastructure.

Request an assessment →