SPECIAL ADVISORY: WATER-SECTOR PLC ATTACKS IN AT LEAST SEVEN STATES — WASHINGTON ACTIONS

Date: 2026-07-30
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Audience: Washington critical infrastructure — cities, counties, tribal nations, water and sewer districts, PUDs, emergency management, and the agencies that support them
Supersedes in part: Stillwater URGENT Special Advisory, July 29 2026 (cycle 26-10)

CONTENTS

WHAT CHANGED IN THE LAST 24 HOURS

We sent you an advisory yesterday on the Minnesota water incidents. Three things have changed since, and two of them change what you should do this week.

First, the activity is not confined to Minnesota. The FBI and EPA issued a Public Service Announcement today stating that "since 27 July 2026, Water and Wastewater Sector (WWS) utility companies in at least seven states have reported incidents to the FBI, and some of that activity degraded water operations" [1]. The states are not named, so we cannot tell you whether Washington is among them. Treat that uncertainty as a reason to look rather than a reason to wait.

Second, real-world consequences have escalated. Yesterday we told you no boil-water advisory had been reported. That is no longer true of the campaign as a whole. CISA now reports this activity "has resulted in boil water notices and sustained manual operations" [2], and the FBI reports operational effects including "loss of pressure and flooding" [1].

Third, the technique has changed character. Yesterday's picture was quiet: modified control logic, disabled alarms, falsified operator displays, all built to look normal from the control room [3]. Today's documents describe something blunt. Attackers are changing PLC IP addresses and setting passwords, locking operators out of their own controllers [1][2].

Neither federal document attributes this activity to anyone. Both say "malicious cyber actors" [1][2]. We treat the preliminary attribution reporting carefully below.

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Find every Rockwell/Allen-Bradley **MicroLogix 1100 and 1400** in your estate and determine whether any is reachable from the internet	Named specifically in today's FBI/EPA PSA, and a different, older line than the models in the July 22 advisory [1]
2	Get exposed PLCs off the internet today, and put remote access behind a gateway or VPN	The explicit top recommendation in both federal documents [1][2]
3	Confirm you hold a **known-good offline backup of every PLC image**	Attackers are setting passwords to lock operators out. Without a clean image you may not be able to recover your own controller [2]
4	Ask your integrator, in writing, which other Washington customers share your network design	The FBI states third-party network similarities "may provide MCA the opportunity to multiply successes… across customers" [1]
5	Inventory every cellular modem, including any a vendor installed	CISA warns targeting includes modems "that may not be documented or included in routine attack surface scans" [2]

Priority	Action	Why Now
6	Hunt for PLC password changes, unexplained IP changes, and lost HMI visibility without a work order	These are the new behaviours. No new indicator lists were published, so behaviour is the detection [1][2]
7	Re-test manual operation of every critical process, and confirm after-hours staffing	The FBI names manual-operation capability as one of four factors determining how badly a victim is hurt [1]
8	Brief your operators today, and your council or commission this week	Operators are your first detection layer, and the funding decisions sit above them [1][2]

WASHINGTON-SPECIFIC FINDINGS

Three things Washington readers should know that are not in the national reporting.

Check the date on any cyber guidance you are relying on

Standing cybersecurity guidance pages, whether on a state site, an association site, or your own intranet, were mostly written before this month. Several in circulation still describe utility cyber risk as a general concern with no corroborated threat to public safety, which was a reasonable characterization when it was written and does not survive contact with today's federal documents. A federal alert now describes boil water notices and sustained manual operations, and a federal PSA describes loss of pressure and flooding [1][2].

Two practical consequences. If anyone in your organization is relying on an undated guidance page as reassurance, replace that reference with the two federal documents cited here. And if a briefing you give this week draws on standing internal material, check it against those documents before you deliver it, because reassuring language written last year will read as negligence in hindsight if it turns out to be wrong.

Verify the channels you actually belong to

Public reporting is not where the useful detail will appear first. WaterISAC, MS-ISAC, the Washington State Fusion Center, and WA Emergency Management Division all carry member-restricted material that can precede public guidance by days during an active campaign, and we cannot see any of it from outside.

If you hold membership in any of those, check it directly today rather than relying on this document. If you do not, this is the week to establish it; the cost is modest relative to what the channel provides while a campaign is live. Several other states have relayed the federal guidance formally to their regulated water systems this week, so if your state or membership channel has issued something, an operator in your organization may already have it sitting unread.

A cyber-caused pressure event looks like an ordinary one

Washington's public drinking-water alert feed routinely carries boil-water notices caused by pressure loss from ordinary sources. As of today it includes, among others, a Grant County system with a boil-water notice issued July 28 recorded as pressure loss, and another Grant County system issued July 22 following a water line leak [7].

Neither of those has any known connection to cyber activity, and we are not suggesting otherwise. We raise them to make a detection point that matters more than any indicator in this document.

The federal mechanism statement is: “Pressure loss in water systems could potentially allow untreated ground water to seep into pipes” [1]. The public notice generated by a cyber-induced pressure loss would be worded the same way as one caused by a leak, would appear in the same feed, and would be indistinguishable to the public, to a reporter, or to a duty officer scanning alerts. Nobody is going to hand you an alert that says “cyber.”

The operational conclusion: whoever reviews public-health and pressure reporting in your organization needs a line to whoever reviews OT telemetry, and that line needs to exist before an event rather than during one. For most Washington jurisdictions those are two different people who have never spoken.

Washington’s structural exposure

Washington regulates drinking water through Group A and Group B system classifications, and the great majority of our systems are small. Small systems are where this campaign lands, for reasons that have nothing to do with the competence of the people running them: one or two operators, an integrator who built the SCADA years ago, a cellular modem at a remote well or tower, and no security staff at all.

Two Washington-specific consequences follow. Our tribal nations operate water systems that serve communities with real distance to the nearest mutual-aid partner, and the recovery clock runs differently when the nearest qualified help is two hours away. And our geography means many systems depend on remote, unstaffed sites reachable only by cellular link, which is precisely the exposure CISA singled out today [2].

WHAT THE TWO NEW FEDERAL DOCUMENTS SAY

Two documents published today. Neither is a numbered Cybersecurity Advisory, which matters if you are searching: CISA’s newest numbered advisory remains AA26-204A from July 23.

The FBI/EPA Public Service Announcement [1]

At least seven states, utilities reporting to the FBI since July 27, with some activity degrading water operations.

The technique: “After remotely accessing internet-facing devices, the actors changed the IP addresses and passwords, resulting in a loss of monitoring and control functionality.” The equipment: Rockwell Automation/ Allen-Bradley MicroLogix 1100 and 1400 series, with the caveat that “while the FBI has only observed this behavior with the referenced Rockwell PLCs, similar considerations should also be made with other branded PLCs.”

The consequences: “Operational effects reported to the FBI have included loss of pressure and flooding.”

The FBI names four factors that determined how badly each victim was hurt: whether the PLC was monitoring or controlling equipment, whether it was an 1100 or a 1400, what function the device supported, and "capability to switch to manual operations." Three were fixed by decisions made years ago. The fourth you can change this week.

The CISA Alert [2]

CISA reports "a significant increase in cyber threat actors targeting programmable logic controllers (PLCs) in the Water and Wastewater Systems (WWS) Sector," and asks owners and integrators to remove exposed PLCs from the internet "as soon as possible."

Two findings matter most. On consequences: "This activity has resulted in boil water notices and sustained manual operations." On who is a target: "These threat actors are targeting water entities of all sizes. Even water organizations with mature cybersecurity processes should validate their external connections, as this targeting activity includes cellular modems installed by operators, vendors, or system integrators that may not be documented or included in routine attack surface scans."

CISA adds a recovery step that is new. Because attackers are setting passwords, you may be locked out of your own controller. CISA advises ensuring "a known clean backup of the PLC image in case they are locked out by a modified password," and points MicroLogix 1400 owners to Rockwell's notice on restoring access when the password is unknown. Find that notice now and put it where on-call staff can reach it.

SHARED THIRD-PARTY ARCHITECTURE ACROSS UTILITIES

From the FBI's threat-landscape section: "across several victims, similarities in network setup provided by third parties may provide MCA the opportunity to multiply successes when vulnerable network and hardware setups exist across customers" [1].

Seven states does not require attackers moving from utility to utility. It is consistent with one reusable weakness in a design pattern that a single integrator or remote-monitoring provider deployed across many customers. Build the same architecture forty times and a weakness in it is a weakness forty times.

For Washington this is the finding with the most leverage, because our small-systems market is served by a modest number of SCADA integrators. If one firm built the controls for thirty systems in a county, that is a regional single point of failure, and the utilities involved cannot see it from where they stand. Counties and the state can.

Ask your integrator, remote-monitoring vendor, and any contract operator, in writing:

- Which of your other customers run the same architecture we do?
- Does our design expose any controller, HMI, or modem directly to the internet?
- Do you use shared or reused credentials across customer sites?

- Are you monitoring for this activity across your customer base, and will you tell us if you find it elsewhere?

WHAT WE ARE NOT SAYING

"Confirmed multi-state spread" is stronger than the source. The FBI says utilities in at least seven states "have reported incidents to the FBI." Reported incidents under active investigation are not confirmed compromises, no state list has been published, and the government has not asserted that all seven are one campaign. Reporting volume also rises after a national alert, which is healthy and still inflates counts.

We cannot tell you whether Minnesota is one of the seven. The FBI's window opens 27 July; the Minnesota incidents ran 26–27 July. Anyone saying "seven states plus Minnesota" is adding a state the government did not.

Attribution is preliminary, and it is not the government's. New York Times reporting, relayed by Reuters and others, has three state officials briefed on the investigation saying tradecraft and the absence of a ransom demand led analysts to tentatively conclude Iranian responsibility, explicitly described as preliminary and subject to a final assessment [6]. Against that: neither federal document today names Iran, CyberAv3ngers, the IRGC, or even cross-references AA26-097A. When agencies that attributed freely in April decline to attribute in July, that restraint is itself information.

These may be two related activity sets rather than one. Today's documents describe overt denial on MicroLogix 1100/1400. The July 22 advisory described stealthy logic manipulation on CompactLogix, Micro850, Schneider, and Siemens equipment [3]. One overlap exists: "at least one organization reported modified PLC project files after noticing ladder logic discrepancies across several sites" [1]. Hunt for both.

Nothing incident-specific has been released. No indicators tied to Minnesota or to any of the seven states exist publicly. A "Minnesota IOC list" arriving in your inbox is the federal tables relabelled, or invented.

HUNT PACKAGE

Indicator status

No new government indicators were published today. We read both documents in full to confirm it. Neither contains IP addresses, hashes, or domains [1][2]. The published set remains the 21 addresses from AA26-097A, reproduced below so this document stands alone.

Because there are no new indicators, **the detection value this round is behavioural.**

Network indicators from AA26-097A [3]

CISA's caveat applies: "The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking." Several are hosting-provider addresses carrying legitimate traffic too.

Published July 22 2026

Indicator	Actor association begins	Ends
185.82.73[.]175	September 2025	February 2026
141.11.164[.]153	January 2026	July 2026
175.110.121[.]42	February 2026	March 2026
175.110.121[.]39	February 2026	March 2026
175.110.121[.]41	February 2026	March 2026
175.110.121[.]107	February 2026	February 2026
192.142.54[.]79	May 2026	June 2026
84.200.205[.]165	May 2026	June 2026
185.225.17[.]225	June 2026	July 2026
79.133.46[.]209	July 2026	July 2026
88.80.150[.]199	July 2026	July 2026
88.80.150[.]200	July 2026	July 2026
88.80.150[.]202	July 2026	July 2026

Published April 7 2026

Indicator	Actor association begins	Ends
185.82.73[.]162	January 2025	March 2026
185.82.73[.]164	January 2025	March 2026
185.82.73[.]165	January 2025	March 2026
185.82.73[.]167	January 2025	March 2026

Indicator	Actor association begins	Ends
185.82.73[.]168	January 2025	March 2026
185.82.73[.]170	January 2025	March 2026
185.82.73[.]171	January 2025	March 2026
135.136.1[.]133	March 2026	March 2026

Transcription caution. Some summaries render these as ranges (`88.80.150.199–.202` , `175.110.121.39–.42`). CISA lists neither `88.80.150.201` nor `175.110.121.40` . Use the individual values.

Domain indicators (vendor-sourced)

Trend Micro publishes two CyberAv3ngers command-and-control DNS indicators, which it states are sourced from CISA [4]:

Indicator	Type
tylarion867mino[.]com	C2 DNS
ocferda[.]com	C2 DNS

These do not appear in the AA26-097A indicator tables we read. We include them because they are worth querying, and we label their provenance because you should know it is vendor-relayed. Vet before blocking.

Behavioural detections

The first six rows are new today. The rest carry forward from yesterday and remain valid.

Watch for	Why it matters	Source
A password set or changed on a PLC that previously had none	The core new technique. On many small-utility controllers no password was ever configured, so any password is anomalous	[1][2]
A PLC IP address changing without a work order	The other half of the technique, used to disconnect the device from its own SCADA	[1][2]
An HMI or SCADA server losing communication with a field asset that is physically fine	“Loss of view” is the documented first symptom. Crews finding healthy equipment the control room cannot see is the signature	[1]

Watch for	Why it matters	Source
An operator unable to authenticate to a controller they have always reached	Lockout is the intended effect. Treat as a security event, not a broken password	[2]
A cellular modem discovered that is not in your asset inventory	Named as the blind spot; installed by operators, vendors, or integrators and often undocumented	[2]
Ladder logic not matching your engineering baseline across multiple sites at once	How one victim found it. A single site looks like an error; several sites is a campaign	[1]
Inbound internet connections to OT ports 44818, 102, 502, 2222	The advisory's named ports for actor communication with PLCs	[3][4]
SSH on port 22 to or from cellular modems and OT field gear	Dropbear SSH deployed on victim modems for persistence	[3]
Control-system protocol functions that change operating mode or modify programs	Called out in the advisory's monitoring guidance	[3]
Project-file downloads or uploads outside a change window	Project-file modification and exfiltration are core campaign activity	[3]
PLC mode-switch changes, especially to program or remote	Precondition for remote logic modification	[3]
Mismatch between HMI-displayed values and physical or field readings	Display manipulation is documented actor behaviour	[3]
Pressure or flow anomalies reported through public-health or customer-complaint channels	The Washington-specific point above: this is how a cyber event is likely to surface first here	[1][7]

MITRE ATT&CK techniques cited in AA26-097A [3]

Tactic	Technique	ID
Initial Access	Internet Accessible Device	T0883
Command and Control	Commonly Used Port	T0885
Command and Control	Remote Access Tools	T1219

Tactic	Technique	ID
Exfiltration	Exfiltration Over C2 Channel	T1041
Impact	Data Manipulation	T1565

End-of-life equipment

The FBI/EPA PSA devotes a full recommendation block to end-of-life planning, which signals where the exposure sits [1]. The MicroLogix 1100 is widely reported to be past end of life, with the 1400 still in production, but we have not verified either against Rockwell's own lifecycle documentation and will not assert a date we have not confirmed. Check your model numbers against Rockwell's Product Lifecycle Status page. The action does not depend on the date: an unsupported controller reachable from the internet is the highest-priority item in your estate.

RECOMMENDED MITIGATIONS BY WASHINGTON ORGANIZATION SCALE

Federal guidance is identical for everyone. Capacity to act on it is not. Each tier is written to be achievable by an organization of that size.

Tribal organizations

You may be running a water system with one or two operators, an integrator based hours away, and no security staff, serving a community for which the nearest mutual-aid partner is a long drive. That combination means the recovery clock matters more for you than for anyone else on this list, and it is the reason the offline PLC backup sits so high.

1. **Call your integrator today** and ask: "Is any of our control equipment reachable from the internet?" Get the answer in writing. If yes, ask them to remove it this week and confirm when done.
2. **Get a copy of every PLC program onto a USB drive and put it in the safe.** If an attacker sets a password you do not know, this file is the difference between a day of downtime and waiting for a replacement controller to ship. Do this before anything else on this list if you do only one thing.
3. **Walk your sites and photograph every modem, radio, and control panel.** A phone-photo inventory in a shared folder beats no inventory, and it is how you find the modem nobody documented.
4. **Change every default and shared password** on controllers, HMIs, and modems. Store the new ones physically at the plant in a sealed envelope in the safe.
5. **Write the manual-operation procedure on one laminated page** and hang it in the plant. Confirm two people can execute it and both are reachable after hours.

6. **Use your sovereign channels.** Tribal nations have direct federal relationships that do not run through the state. CISA's Tribal liaison, your CISA Region 10 office, and EPA's Cybersecurity Technical Assistance Program all engage tribal systems directly, and the assistance is at no cost.
7. **Ask about PISCES.** The Public Infrastructure Security Cyber Education System provides no-cost network monitoring to Washington public entities, including tribal governments, and is built for exactly the organization that cannot staff a SOC.

Small cities and districts

Everything above, plus:

1. **Put a gateway or jump host in front of all OT remote access**, with multifactor authentication at the gateway. This works even though the PLC cannot do MFA, which is the point.
2. **Enable logging on cellular modems** and route those logs somewhere a person reviews weekly.
3. **Query 18 months of firewall and modem logs** against the indicators and behavioural table above. If you have no logs going back that far, that finding is itself worth reporting to your council.
4. **Set physical mode switches to RUN** on controllers that have them, and validate project files before any mode change.
5. **Join WaterISAC and MS-ISAC**, and register with the Washington State Fusion Center. Member channels carry technical detail before it is public, and during an active campaign that lead time is the product.
6. **Tell your council this week**, in three sentences, what you found when you asked your integrator question one. A council that hears it now will fund it; a council that hears it during an incident will ask why they did not know.

Medium cities

Everything above, plus:

1. **Run a real OT asset inventory** with owner, location, model, firmware, lifecycle status, and network path for every controller, HMI, and modem. Reconcile it against what your integrator believes is deployed; the gap between the two lists is where incidents live.
2. **Segment OT from IT** with enforced policy rather than documented intention, and test the enforcement.
3. **Baseline every PLC program** and implement automated integrity checking with alerting on drift.
4. **Bring OT telemetry into your SIEM**: PLC authentication events, configuration changes, modem connections.
5. **Connect your public-works and public-health reporting to your security function.** This is the Washington-specific action from the pressure-notice finding above, and at your scale it is a meeting and a shared inbox rather than a project.

6. **Exercise a cyber-induced loss of control** with operations, IT, public works, and communications in the room. Include the decision about issuing a precautionary boil-water notice, because that decision is demonstrably on the table now.
7. **Put security requirements into integrator and vendor contracts**, including notification when the vendor finds this activity at another customer.

Large cities and metro utilities

Everything above, plus:

1. **Treat the shared-integrator pattern as a formal third-party risk finding.** Enumerate every vendor with remote access to your OT, map what each can reach, and require attestation about their other customers' architectures.
2. **Hunt proactively across the full estate** rather than sampling, specifically for the multi-site logic-discrepancy pattern the FBI describes.
3. **Instrument the physical layer as a detection source.** Pressure, flow, and level telemetry that disagrees with SCADA is a cyber indicator, and at your scale that correlation can be automatic.
4. **Run a purple-team exercise against the actual technique**: change a PLC IP and set a password in a test cell, and measure detection and recovery time. Recovery time is the number your executives need.
5. **Pre-position recovery capability**: clean PLC images under configuration management, spare controllers on the shelf for critical assets, a tested restore procedure.
6. **Lead regional mutual aid.** You have OT recovery capability the small systems around you do not. Formalizing that now is cheaper than improvising it during a regional event, and it is the single most useful thing a large Washington utility can do for the rest of the state this month.

Counties and statewide agencies

Your leverage is different. You can make the small systems in your jurisdiction safer faster than they can make themselves safer.

1. **Enumerate the systems in your jurisdiction and identify the smallest ones.** That is where this campaign lands, and many will not know today's documents exist.
2. **Push a one-page version of the tribal/small-system actions** through channels those operators already read, then follow up by phone with the ones who do not respond.
3. **Map integrator concentration in your region.** If one firm built the SCADA for thirty systems in your county, that is a regional single point of failure and you are the only party positioned to see it. This is the highest-value action on this list.
4. **Offer shared services** small systems cannot staff alone: a jump host, log collection, scanning, or a retained OT responder on standby. PISCES already provides part of this in Washington at no cost, and your role may be simply getting systems enrolled.

5. **Add cyber-induced loss of control to your CEMP** as a distinct scenario with its own public-messaging annex. It behaves differently from a main break: water may be safe while control is degraded, and the communication is harder.
6. **Rehearse the emergency-declaration decision** with elected officials before they make it under pressure. A Minnesota city made that call this week.
7. **Publish one referral path** covering the state drinking-water program, WA EMD, and the State Fusion Center, so a small utility that finds something knows exactly who to call, once. Ambiguity about who to call costs hours during an incident, and the utilities least able to absorb that delay are the ones most likely to be affected.
8. **Relay the federal guidance formally to the systems in your jurisdiction.** Several states have done this through their drinking-water programs this week. An official relay through the channel operators already read reaches people who will never see a CISA alert on their own.

FROM THE PANEL VIEW: BRIEFING YOUR OPERATORS

The people most likely to catch this first are operators, not analysts. **The leading indicators of this attack are physical, not cyber.** Loss of view, loss of control, pressure anomalies, flooding, and equipment that does not answer are all things an operator or field crew notices hours before a security tool does, and in a small Washington system there may be no security tool at all.

What to say to operators

Keep it to five points. Longer will not survive a shift change.

1. **“There is a national campaign right now against the controllers that run our plant. You are the detection system.”** Operators who understand they are the sensor behave differently from operators told to be careful.
2. **“If the screen and the world disagree, believe the world.”** A gauge, a sight glass, a physical reading, or your own eyes outrank the HMI. Attackers in this campaign have both frozen and falsified displays.
3. **“If you get locked out of a controller, that is a security event, not a broken password.”** Do not keep retrying, and do not let anyone reset it before it is reported. Attackers are deliberately setting passwords.
4. **“Tell someone even when you are not sure, and you will never be second-guessed for it.”** Say it out loud, mean it, and have supervisors demonstrate it. The failure mode in these incidents is a person who noticed something at 2 a.m. and decided it was probably nothing.
5. **“Know how to run your process by hand, today.”** Walk it, do not just read it. The FBI named manual-operation capability as one of four factors determining how badly a utility is hurt, and it is the only one you can change this week.

What operators should watch for

Symptom	What it may mean
A screen that has not updated in a while, or values that look too steady	Loss of view, or a display frozen or falsified upstream
Cannot log in to a controller you have always reached	Password set by an unauthorized party
SCADA cannot see a site, but the crew finds the equipment running fine	The controller's IP address may have been changed
Pressure or flow that does not match what the screen reports	The most consequential mismatch here, and the one connected to public health
A pump, valve, or blower that does not respond to a command	Loss of function, the more serious half of the FBI's finding
An alarm that should have fired and did not	Alarm and shutdown logic has been disabled in this campaign family
A tone, vibration, or smell that is wrong even though the panel is green	Trust it. This sense has caught more OT incidents than any product

What to tell your council, commission, or tribal council

Non-technical decision-makers need three sentences, not a threat briefing.

- The equipment that runs our water system is being attacked nationwide, in at least seven states, and the federal government asked utilities today to disconnect this equipment from the internet.
- The realistic worst case is losing remote visibility and control, running the plant by hand, and possibly issuing a precautionary boil-water notice. That has already happened somewhere in this campaign.
- What we need is a decision on funding for [the specific gap you have], and thirty minutes to walk through what we would do if it happened here.

Two things to say clearly, because both are true and both are usually misunderstood. The utilities hit in Minnesota did not fail; Braham was back in under two hours on manual operation [5]. And the margin between "disruption" and "emergency" at a small utility is a couple of trained people and a written procedure, which is a budget question rather than a competence question.

For emergency managers specifically

Your event will not arrive labelled as cyber. It will arrive as a pressure complaint, a boil-water notice, a flooded lift station, or a public works crew that cannot reach a site. Three things to do now:

- **Add a cyber cause to the decision tree you already have for water events.** You do not need a new plan; you need one branch in the existing one, and a rule for when to bring in your IT or security contact.
- **Know who to call before you need to.** Confirm your path to DOH Office of Drinking Water, WA EMD, the State Fusion Center, your CISA regional office, and the FBI Seattle field office, and confirm it is a person rather than a general line.
- **Pre-draft the public message for "water is safe, control is degraded."** It is a genuinely hard message and it is much harder to write at 9 p.m. with a reporter waiting. Water quality unaffected while the utility operates manually is the most likely public-facing shape of this event.

CROSS-SECTOR RISK IN WASHINGTON

Water is the sector under attack. The exposure is not water's alone.

Hospitals. A hospital cannot operate long without water. Sterile processing, dialysis, cooling for imaging equipment, and sanitation all depend on it, and a boil-water notice triggers clinical workarounds well before any supply is lost. Confirm you know which utility serves you, that utility's notification path, and how long you can run on stored water. Most facilities have that number on paper and have never tested it. Rural Washington hospitals served by a single small water system carry this risk most acutely, and they are often served by exactly the systems least able to defend themselves.

Schools. A boil-water notice usually closes a school or forces bottled-water operations, because food service and handwashing requirements cannot otherwise be met. Districts should know their utility's notification path and hold a closure decision rule that does not have to be invented on a Monday morning. With the school year approaching, this is worth resolving in August rather than September.

Power. Thermal generation needs cooling water; water and wastewater treatment need power. The dependency runs both directions, and the same PLC exposure pattern exists in generation and distribution. Washington's PUDs frequently operate both electric and water utilities, which concentrates the exposure in one organization and one integrator relationship. That is worth a specific look if it describes you.

Chemical and industrial processes. Any facility whose safety case depends on cooling water, fire water, or process water should re-examine what happens if municipal supply becomes unreliable rather than absent. Intermittent and unreliable is harder to design for than a clean outage, and it is the failure mode this campaign produces. Facilities with Risk Management Program obligations should confirm their hazard analysis contemplates degraded utility service rather than only total loss.

Wastewater specifically. Wastewater receives less attention than drinking water and carries a more immediate environmental consequence. Flooding is one of the two operational effects the FBI names [1], and in Washington a lift-station failure becomes a surface-water discharge with Ecology reporting obligations quickly.

Ports, food processing, and agriculture. Washington's ports, food and beverage processors, and irrigation districts all run the same class of controller, often on cellular links at unstaffed sites. MicroLogix controllers are not water-specific, and the FBI's note that similar considerations apply to other branded PLCs widens this further [1]. If you own any internet-reachable PLC, today's documents apply to you regardless of sector.

WHAT WE WILL BE WATCHING

- **A named state list**, or a numbered joint advisory merging this activity with AA26-097A. Either would settle whether this is one campaign.
- **Formal attribution.** Today's federal silence is deliberate; a change from it would be meaningful.
- **The first incident-specific indicators.** None exist yet.
- **A named integrator or vendor** at the centre of the shared-architecture pattern. This is the development most likely to change who needs to act urgently.
- **Any Washington-specific guidance** issued through state or ISAC member channels.
- **Any boil-water notice with a confirmed cyber cause**, which would be the first unambiguous public-health consequence of this campaign.

We will send a further advisory if any of these lands.

REFERENCES

[1] FBI and EPA, Public Service Announcement, "Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions" (2026-07-30) — https://www.fbi.gov/news/press-releases/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet--facing-programmable-logic-controllers-causing-operational-disruptions

[2] CISA Alert, "CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs" (2026-07-30), with EPA and FBI contributions — https://www.cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs

[3] Joint Cybersecurity Advisory AA26-097A, "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure" (published 2026-04-07, last revised 2026-07-22) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

[4] Trend Micro, “Federal Agencies Warn of Ongoing PLC Exploitation Against Critical U.S. Infrastructure” (2026-07-23) — https://www.trendmicro.com/en_us/research/26/g/plc-exploitation.html

[5] Stillwater Group, URGENT Crit Infra Special Advisory, “Coordinated Cyberattack on Minnesota Water Utilities” (2026-07-29), and sources therein

[6] New York Times reporting on preliminary attribution (2026-07-30), relayed by Reuters/Al Jazeera and Valley News Live — https://www.aljazeera.com/news/2026/7/30/us-authorities-probe-cyberattack-on-water-systems-in-minnesota

[7] Washington State Department of Health, “Drinking Water Active Alerts” (retrieved 2026-07-30) — https://doh.wa.gov/community-and-environment/drinking-water/active-alerts. Cited only for the routine, non-cyber pressure-loss and line-leak boil-water notices discussed above.

[8] US EPA, Enforcement Alert, “Drinking Water Systems to Address Cybersecurity Vulnerabilities” (2024-05) — https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities

Additional Resources

- CISA Cyber Hygiene Services, no cost — https://www.cisa.gov/cyber-hygiene-services
- CISA Region 10 (Washington) and CISA Tribal engagement
- EPA Cybersecurity Technical Assistance Program for the Water Sector
- PISCES — no-cost network monitoring for Washington public entities
- Washington State Fusion Center
- Washington Emergency Management Division
- WA DOH Office of Drinking Water
- FBI Seattle Field Office; IC3 at https://www.ic3.gov
- Rockwell Automation PSIRT — PSIRT@rockwellautomation.com
- WaterISAC — https://www.waterisac.org
- Top 20 Secure PLC Coding Practices — https://plc-security.com

YOUR STILLWATER CONTACT

Kevin Rolnick, Sales & Partnerships Executive kevin@stillwater.io · www.stillwater.io · +1-425-818-1745

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net