SPECIAL ADVISORY: COORDINATED CYBERATTACK ON MINNESOTA WATER UTILITIES

Date: 2026-07-29
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Audience: Critical infrastructure clients — cities, counties, utilities, water districts, and the agencies that support them
Companion to: Stillwater Risk Briefing, July 28 2026 (26-10)

EXECUTIVE SUMMARY

Over roughly 48 hours beginning Sunday July 26, a coordinated cyberattack disrupted operational technology at more than 30 Minnesota community water systems [1]. Four cities have disclosed publicly: Braham, Plymouth, South St. Paul, and Maple Plain [2]. No community lost safe drinking water, and no boil-water advisory or water-quality impact has been reported [1][3]. Minnesota IT Services has activated a statewide cybersecurity response and the Minnesota Department of Health is working directly with the affected systems [1].

The operational profile is what should hold your attention. The attackers went after automation and control, not water chemistry, and the state's assessment of motive is disruption rather than money. Minnesota's chief information security officer, John Israel, put it plainly: "All signs are pointing to disruption, not trying to get a financial gain" [3]. The utilities that recovered fastest did so by falling back to manual operation, which is a capability many districts have quietly allowed to decay.

Four days before the attacks began, a seven-agency federal advisory described this exact class of targeting against internet-exposed programmable logic controllers at water, energy, and local-government victims [4]. We are publishing that advisory's full indicator set below, along with a work plan. No formal attribution has been made for Minnesota, and we are careful about that distinction throughout this document.

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Find every PLC, HMI, and OT gateway reachable from the internet, including anything on a cellular modem, and put it behind a secure gateway	Federal advisory AA26-097A describes opportunistic targeting of exactly these devices; the Minnesota impacts concentrated on cellular-connected water towers and lift stations [4][5]
2	Query 18 months of logs against the 21 federal indicators in the appendix, and watch OT ports 44818, 2222, 102, and 502 plus port 22 on OT-connected modems	CISA's own key action; six indicators run to July 2026, so this is live infrastructure, and the oldest window opens January 2025 [4]
3	Compare running PLC logic against known-good engineering baselines, with specific attention to alarm setpoints, shutdown logic, and reusable code modules	The advisory documents a victim whose malicious project file kept downstream function normal while disabling shutdown and alarm logic [4]
4	Set physical mode switches on Rockwell controllers to RUN, and validate project files before returning any device to run mode	Prevents remote logic modification; the advisory added the pre-RUN validation step on July 22 [4]
5	Confirm you can run every critical process manually, and that the staff who know how are reachable after hours	Braham restored service in under two hours on manual operation; Plymouth ran manually through the incident [3][5]
6	Change default and shared credentials on OT devices and cellular modems, and revoke former-employee access	EPA inspections repeatedly find unchanged defaults, shared single logins, and stale accounts at water systems [6]
7	Ask your SCADA integrator and remote-monitoring vendor, in writing, what they have exposed on your behalf	The advisory specifically warns that service providers may rely on internet connectivity and "may not be fully aware of active threats" [4]
8	Verify your SDWA Section 1433 risk assessment and emergency response plan are current, and that the ERP covers a cyber-induced loss of control	Over 70% of water systems EPA inspected since September 2023 were in violation of these basic requirements [6]

WHAT HAPPENED

The scale is unusual; the individual impacts were contained. More than 30 Minnesota community water systems were affected between July 26 and 27 [1]. The state has not released a full list, and most affected systems remain nonpublic [2]. Of the four cities that disclosed:

- **Braham** (population roughly 1,700 [5]) had its computerized operating controls disabled, which took the well and treatment plant offline. Public works crews restored the plant in under two hours by switching to manual operation [3]. A detail worth dwelling on comes from city administrator Kevin Stahl: "You physically have to be in the plant to change chemical feed rates," and "There was no compromise to any of the flow rates of chemicals or anything like that… they just shut the water off to the well" [2]. A design decision made for ordinary operational reasons put the safety-critical parameter out of the attacker's reach.
- **Plymouth** (population roughly 80,000) disconnected affected cellular-connected equipment at two water towers, along with multiple wastewater lift stations, and continued operating manually [5].
- **South St. Paul** had automated utility controls affected [7]. **Maple Plain** declared a local state of emergency to open up resource coordination and state and federal support [7].

Nobody lost safe water. No boil-water advisory or water-quality impact has been reported in any community, and the Department of Health says it knows of no requests for residents to change their water use [1][3].

The response worked. Minnesota IT Services activated a statewide response coordinated with the Department of Health, the Department of Public Safety, the BCA's Minnesota Fusion Center, and the Pollution Control Agency [7]. The FBI is aware and in contact with victims [8].

WHAT IS NOT YET KNOWN

Precision matters more than speed in the first week of an incident like this, so we are explicit about the limits of current knowledge.

- **No attribution has been made.** No federal or state official has attributed these attacks to any actor. MNIT's spokesperson has said the incidents' "timing, methods of access, and targeted infrastructure share characteristics with other coordinated cyber incidents our federal partners have observed involving critical infrastructure," while declining to attribute [8]. That is a deliberately non-committal statement, and it should be read as one. Press and vendor commentary connecting Minnesota to Iranian-affiliated activity is inference, not official finding.
- **The indicators in this advisory are campaign indicators, and nothing incident-specific to Minnesota has been released.** The 21 addresses in the appendix come from federal advisory AA26-097A and are worth hunting. Separately, we swept public vendor and ISAC reporting across eighteen research teams and information-sharing bodies and found no IP addresses, hashes, domains, or signatures tied to the Minnesota incident itself. The investigation is active and technical detail is being deliberately withheld.

Treat any "Minnesota IOC list" circulating in your inbox with suspicion; it is either the federal tables below relabeled, or invented. If you hold WaterISAC or MS-ISAC membership, check those portals directly, because restricted-distribution detail can exist well before anything appears publicly.

- **The entry vector at these utilities has not been disclosed.**

READING THE CLAIMS YOU ARE ABOUT TO SEE

No group had claimed the Minnesota attacks as of publication [12]. When claims do surface, and in a campaign with this much attention they will, treat them as marketing until your own telemetry says otherwise. Three pieces of recent evidence explain why.

A claim against a water utility collapsed under forensics six weeks ago. On June 11 the Handala group claimed a breach of California Water Service, named specific service areas, said it had taken 5 GB, and asserted it could have disrupted the water supply but chose not to [13]. Cal Water's investigation with Mandiant, reported June 24, found no evidence of threat-actor activity in the company's internal information technology or operational technology environments; the access was limited to third-party service-provider accounts [18]. The claim and the reality were substantially different, and the gap ran in the direction of the actor's advantage.

One group breached a fake water plant and announced it as a real one. Forescout ran a decoy water-treatment control system that the hacktivist group TwoNet entered in September 2025 by logging into the operator interface with the credentials admin/admin, moved around in for roughly 27 hours across several sessions including one under an account it created for itself, and then publicly claimed on Telegram as a genuine utility compromise [14]. Two lessons travel together here: public claims are not evidence that a real facility was touched, and the entry method was a default password. (TwoNet is pro-Russian rather than Iranian, so this is a lesson about hacktivist claims generally, not about the actor set in the federal advisory.)

The vendors who track these groups say the same thing in different words. Dragos characterizes the claims as "exaggerated or repeated claims of prior compromises," and Sophos describes "broad and embellished claims, and narrative amplification, rather than delivering materially significant impacts" [15] [16]. These assessments predate the current incident, which is worth noting, but the pattern they describe is long-running.

One actor can look like nine. CISA lists CyberAv3ngers, APT IRAN, Mr. Soul, Soldiers of Solomon, Hydro Kitten, Storm-0784, Bauxite, UNC5691, and the Shahid Kaveh Group as names for a single IRGC-affiliated actor [4]. Coverage that treats those as separate groups makes the threat landscape look more crowded than it is. Similarly, the "Electronic Operations Room" umbrella formed on February 28, and Unit 42 reported some estimates of around 60 individual groups active by March 2 [17]. Treat a headline group count as a measure of how many personas are claiming activity rather than how many are capable of it.

What to do with this. Decide now, in writing, who verifies a public claim that names your utility, what telemetry they check, and who is authorized to say anything publicly. Verify against your own logs and control-system state before you confirm or deny anything. A ransom-note-style post naming your city, arriving at 6 p.m. on a Friday, should trigger a defined process rather than an improvised press response.

THE FEDERAL ADVISORY PUBLISHED FOUR DAYS EARLIER

On July 22, seven agencies (FBI, CISA, NSA, EPA, the Department of Energy, Cyber National Mission Force, and Treasury) updated joint advisory AA26-097A on Iranian-affiliated actors targeting internet-connected PLCs [4]. The advisory names three sectors: "Government Services and Facilities (to include local municipalities), Water and Wastewater Systems (WWS), and Energy" [4]. Whether or not Minnesota is connected to this campaign, the advisory is the best available description of how a small utility's control system gets taken over, and it was published before the attacks began.

The single most important thing to understand about it: there is nothing to patch. The advisory says so directly. It "is not highlighting a new vulnerability in the identified products, but instead discusses opportunistic targeting" [4]. The devices being compromised are working as designed and are simply reachable from the internet, often with default credentials. Remediation is configuration and architecture, and no vendor has issued or can issue a firmware fix that changes that. A patch-centric security program will not touch this risk.

What the actors do once they are in. The advisory documents actors downloading and modifying controller project files, altering what operators see on HMI and SCADA displays, and exfiltrating project files using the vendors' own engineering software run from leased hosting infrastructure [4]. Two findings deserve specific attention from anyone running a treatment plant:

- At one victim, a malicious project file "retained ladder logic for downstream function but added logic that overrode specific instruction sets responsible for maintaining safe operating parameters" [4]. Describing the campaign more broadly, the advisory states that the actors' changes "disabled critical shutdown and alarm logic, allowing systems to enter unsafe conditions without notifying operators of the anomalies" [4]. A control system in that state looks normal from the control room.
- The actors deployed Dropbear SSH on victim modems for persistent remote access over port 22 [4].

Affected equipment named in the advisory: Rockwell Automation CompactLogix and Micro850, Schneider Electric BMX P34 and Modicon M340, Siemens S7-1200, "and potentially other manufactured PLCs" [4]. Vendor scope expanded on July 22; the earlier version was Rockwell-focused.

The cellular-modem pattern. Censys found in April that 5,219 internet-exposed hosts globally identified themselves as Rockwell or Allen-Bradley devices, 3,891 of them in the United States, and that 62.4% of the global total sat on Verizon and AT&T mobile networks, which is the signature of field equipment reaching the internet through cellular modems [9]. That figure is a point-in-time snapshot from April 7 and is now roughly

sixteen weeks old. We flag the convergence carefully: the federal advisory describes persistence on cellular modems, the exposure data shows cellular field gear is where the exposure concentrates, and Minnesota's disclosed impacts landed on cellular-connected water towers and lift stations. That is a strong argument for where to hunt first. It is not evidence that the campaigns are the same.

WHY THIS LANDS HARDEST ON SMALL UTILITIES

The structural problem is well documented and has nothing to do with any individual utility's competence.

EPA reports that over 70% of water systems it inspected since September 2023 were in violation of basic Safe Drinking Water Act Section 1433 requirements, which are the risk assessments and emergency response plans mandated by the 2018 America's Water Infrastructure Act [6]. The violations EPA cites are unglamorous: unchanged default passwords, shared single logins, and access that was never revoked when employees left [6]. Note the scoping on that statistic, because it is often misquoted: it describes 70% of the systems EPA inspected, not 70% of all water systems in the country.

Separately, an EPA Office of Inspector General passive assessment of 1,062 drinking water systems serving more than 193 million people found 97 systems, serving roughly 26.6 million people, with critical or high-risk cybersecurity vulnerabilities, plus another 211 systems serving more than 82.7 million people rated medium or low [10]. The OIG also noted that EPA lacks its own cyber incident reporting system for the water sector [10].

With more than 148,000 public water systems in the United States [11], most of them small, the arithmetic is unforgiving. Braham's mayor pointed to limited staff, aging technology, and inadequate resources [12], and Maple Plain's emergency declaration exists precisely to reach for capability the city does not hold on its own [7].

This is the part cities, counties, and districts should take to their governing bodies: the affected utilities did not fail. Braham was back in under two hours. What the incident demonstrates is that the margin between "disruption" and "emergency" at a small utility is a couple of trained people and a manual procedure.

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Inventory internet-reachable OT.** Every PLC, HMI, engineering workstation, and gateway, and specifically every cellular modem serving a remote site: towers, lift stations, wells, booster stations, SCADA radios. Field sites installed by an integrator years ago are the ones that will surprise you. If any controller in your estate is internet-reachable, treat yourself as in scope regardless of vendor [4].

2. **Remove the exposure.** Put devices behind a secure gateway or jump host so the OT system is never directly exposed, and mediate, monitor, and control all access [4]. Where a device must stay remotely reachable, restrict it to known source addresses and require multifactor authentication at the gateway, which works even when the PLC itself cannot do MFA [4].
3. **Hunt your logs against the indicators in the appendix**, going back eighteen months, since the earliest actor-association window opens in January 2025. Look for traffic on ports 44818, 2222, 102, and 502, and on port 22 to OT-connected modems, especially from foreign hosting providers [4].
4. **Verify control logic against engineering baselines.** Use vendor integrity-checking tools and visually compare running programs to known-good logic. Check reusable code modules (Add-On Instructions on Rockwell equipment) for anomalous modification, and confirm alarm setpoints and shutdown logic specifically, because disabling those is documented behavior [4].
5. **Set physical mode switches to RUN** on controllers that have them, return them to RUN immediately after any authorized download, and validate project files before switching, since the mode change locks in whatever was last downloaded [4].
6. **Fix credentials and access.** Change default and shared passwords on PLCs, HMIs, and cellular modems; revoke departed-employee access; disable unused services such as Telnet, FTP, RDP, VNC, and device web interfaces [4].
7. **Brief your operators.** Manipulated displays are documented behavior in this campaign. Operators should know to escalate any mismatch between what the screen says and what physical indications, field readings, or gauges show, and they should never be made to feel foolish for raising one [4].
8. **Confirm manual fallback works.** Walk through running each critical process by hand, verify the procedures are current and physically accessible when the network is down, and confirm the people who know how are reachable at 2 a.m. This is what contained the Minnesota incidents.
9. **Validate your backups before you would need them.** Keep offline copies of PLC logic and configuration, and verify a backup does not contain malicious logic before restoring it [4].

Strategic Actions (This Month)

1. **Put safety-critical setpoints out of remote reach.** Braham's chemical feed required physical presence and was never touched. Decide deliberately which parameters should be changeable only at the panel, and engineer that constraint rather than relying on policy.
2. **Re-architect cellular OT connectivity.** Replace consumer-grade cellular modems with industrial gateways, and move toward the isolated architectures the advisory now recommends: private APN, 5G PNI-NPN, cellular SD-WAN, zero-trust network access, or site-to-site VPN [4]. Enable and review modem logs.
3. **Bring your service providers into scope in writing.** Ask your SCADA integrator, remote-monitoring vendor, and any contract operator what they have connected on your behalf, through what path, and who else can reach it. The advisory explicitly warns that providers may not be aware of active threats against the connectivity they depend on [4].

4. **Refresh your SDWA Section 1433 documents with cyber in them.** Update the risk and resilience assessment and emergency response plan so the ERP covers loss of control-system integrity, not only physical events, and exercise it.
5. **Exercise the scenario with elected officials in the room.** Maple Plain's emergency declaration was a resource decision made under pressure. Council members, county boards, and district commissioners should rehearse that decision before they face it, including public communication when water is safe but control is degraded.
6. **Join and use the sector channels.** WaterISAC, MS-ISAC, and your state fusion center carry member-only technical detail that does not appear in public reporting. If you are not a member, the cost is modest relative to what the channel provides during an active campaign.

APPENDIX: FEDERAL INDICATORS OF COMPROMISE (AA26-097A)

Use these to query historical logs. CISA's own disclaimer applies and we reproduce it deliberately: "The FBI observed the threat actors using the IP addresses listed below in the specified time frames. This data is being provided for customers to query against logs for indications of historical targeting by the Iranian-affiliated APT actors. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking" [4]. Several of these are hosting-provider addresses that may serve legitimate traffic, so vet before you blackhole anything.

Read the scope carefully. These 21 addresses are published federal indicators for the AA26-097A campaign, and they are the reason this appendix exists. They are not drawn from the Minnesota incident, and no indicators specific to Minnesota have been released by any source.

New indicators, 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

Indicator	Actor association begins	Ends
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

Historical indicators, 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
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

A caution on transcription. At least one published summary of these indicators renders them as ranges (`88.80.150.199–.202` and `175.110.121.39–.42`). CISA lists neither `88.80.150.201` nor `175.110.121.40` . If you ingest a range, you will block two addresses the government did not attribute. Use the individual values above.

Machine-readable bundles. CISA publishes the July 2026 indicators as STIX XML (29 KB) and STIX JSON (30 KB), and the April set as STIX XML (36 KB) and STIX JSON (12 KB), for direct import into SIEM, IDS, and firewall platforms [4].

Behavioral detection, since indicator lists will not be enough

Infrastructure changes faster than advisories publish, and nothing incident-specific to Minnesota has been released. Pair the addresses above with behaviour:

Watch for	Why
Any inbound connection from the internet to OT ports 44818 (EtherNet/IP), 102 (S7comm), 502 (Modbus), 2222	The advisory's named ports for actor communication with PLCs [4]
SSH on port 22 to or from cellular modems and OT-connected field gear	Dropbear SSH deployed on victim modems for persistence [4]
Control-system protocol functions that change operating mode or modify programs	Explicitly called out in the advisory's monitoring guidance [4]
Project-file downloads or uploads outside a change window	Project-file modification and exfiltration are the campaign's core activity [4]
PLC mode-switch changes, especially to program or remote	Precondition for remote logic modification [4]
Any configuration change on an asset-management system without a work order	The advisory recommends monitoring these to establish expected parameter settings [4]
Mismatch between HMI-displayed values and field or physical readings	Display manipulation is documented actor behavior [4]

MITRE ATT&CK techniques cited in the advisory

Tactic	Technique	ID
Initial Access	Internet Accessible Device	T0883
Command and Control	Commonly Used Port	T0885
Command and Control	Remote Access Tools	T1219
Exfiltration	Exfiltration Over C2 Channel	T1041
Impact	Data Manipulation	T1565

Vendor contacts for suspected compromise

Vendor	PSIRT contact	Hardening guidance
Rockwell Automation	PSIRT@rockwellautomation.com	Security Advisory SD1771
Schneider Electric	cpcert@se.com	Cybersecurity User Guide for Modicon Controller Platform
Siemens	productcert@siemens.com	Security Bulletin 104599

If you believe you were targeted, the advisory directs you to contact the authoring agencies and your PLC manufacturer [4]. CISA also offers Cyber Hygiene Services, including external scanning, at no cost [4].

REFERENCES

[1] Minnesota IT Services, “Statewide cybersecurity response to support affected communities and protect critical infrastructure” (2026-07-28) — https://mn.gov/mnit/media/blog/?id=38-761869

[2] MinnPost, “Cyberattacks highlight risks to Minnesota drinking water from aging IT systems” (2026-07) — https://www.minnpost.com/drinking-water/2026/07/cyberattacks-highlight-risks-to-minnesota-drinking-water-from-aging-it-systems/

[3] CBS Minnesota, “Cyberattack, malware caused Braham water plant outage” (2026-07-28) — https://www.cbsnews.com/minnesota/news/cyberattack-malware-braham-water-plant-outage/

[4] Joint Cybersecurity Advisory AA26-097A, “Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure,” FBI, CISA, NSA, EPA, DOE, CNMF, Treasury (published 2026-04-07, updated 2026-07-22) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a (PDF: https://www.ic3.gov/CSA/2026/260722.pdf)

[5] StateScoop, “Coordinated cyberattack disrupts water utilities in 30 Minnesota communities” (2026-07-28) — https://statescoop.com/coordinated-cyberattack-disrupts-water-utilities-in-30-minnesota-communities/

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

[7] Valley News Live, “Cyberattack hits more than 30 Minnesota community water systems” (2026-07-28) — https://www.valleynewslive.com/2026/07/28/cyberattack-hits-more-than-30-minnesota-community-water-systems/

[8] Reuters (AJ Vicens), “Minnesota IT officials disclose coordinated cyberattack at more than 30 local water systems” (2026-07-28) — https://kfgo.com/2026/07/28/minnesota-it-officials-disclose-coordinated-cyberattack-at-more-than-30-local-water-systems/

[9] Censys, “Iranian-Affiliated APT Targeting of Rockwell/Allen-Bradley PLCs” (2026-04-08, data snapshot 2026-04-07) — https://censys.com/blog/iranian-affiliated-apt-targeting-rockwell-allen-bradley-plcs/

[10] EPA Office of Inspector General, “Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems,” Report 25-N-0004T (2024-11-13) — https://www.epa.gov/sites/default/files/oig/documents/Full%20Report%2025-N-0004_Errata.pdf

[11] US Environmental Protection Agency, “Information about Public Water Systems” (page updated 2026-03-16) — https://www.epa.gov/dwreginfo/information-about-public-water-systems

[12] Cybersecurity Dive, “Authorities investigating a coordinated cyberattack against Minnesota water systems” (2026-07-28) — https://www.cybersecuritydive.com/news/authorities-investigating-a-coordinated-cyberattack-against-minnesota-water/826427/

[13] Nozomi Networks, “Handala’s Water Play: What the Breach Was, What It Wasn’t” (2026-06-18), with Cal Water and Mandiant findings reported 2026-06-25 — https://www.nozominetworks.com/blog/handalas-water-play-what-the-breach-was-what-it-wasnt-and-what-utilities-should-be-doing-anyway

[14] Forescout Vedere Labs, “Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS” (honeypot intrusion September 2025) — https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/

[15] Dragos Intelligence assessment of Iranian-nexus hacktivist claims, quoted in Information Security Media Group, “Iranian Cyberthreats Test US Infrastructure Defenses” — https://www.bankinfosecurity.com/iranian-cyberthreats-test-us-infrastructure-defenses-a-31299

[16] Sophos, “Hacktivist campaigns increase as United States, Iran, and Israel conflict intensifies” — https://www.sophos.com/en-us/blog/hacktivist-campaigns-increase-as-united-states-iran-and-israel-conflict-intensifies

[17] Palo Alto Networks Unit 42, “Threat Brief: Escalation of Cyber Risk Related to Iran” (Electronic Operations Room formed 2026-02-28; some estimates of 60 individual groups active as of 2026-03-02) — https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

[18] SJV Water, reporting Cal Water and Mandiant findings on the Handala claim (2026-06-24) — https://sjvwater.org/

Additional Resources

- CISA Cross-Sector Cybersecurity Performance Goals — https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- CISA Cyber Hygiene Services (no cost) — https://www.cisa.gov/cyber-hygiene-services

- WaterISAC — https://www.waterisac.org
- Joint guidance, Secure Connectivity Principles for OT — referenced in AA26-097A
- 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