COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA PUBLIC UTILITY COMMISSION
COMMONWEALTH KEYSTONE BUILDING
400 NORTH STREET
HARRISBURG, PENNSYLVANIA 17120

July 31, 2026

Cybersecurity Advisory:
Potential Exploitation of Water/Wastewater Utility Operational Technology (OT) Systems

To All Jurisdictional Water/Wastewater Utilities:

Due to the recent cyberattacks on water/wastewater utilities in the state of Minnesota, the Pennsylvania Public Utility Commission (PUC) wants to make you aware of the potential threat to your OT systems. This advisory is anchored on the technical guidance and Tactics, Techniques, and Procedures (TTPs) detailed in CISA Advisory AA26-097A – ***Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure***.

This alert is issued following active cyber intrusions targeting more than 30 community water and wastewater systems across Minnesota between July 26 and July 27, 2026. As documented by Tenable Research, malicious cyber actors successfully utilized the TTPs outlined in the referenced CISA advisory to compromise OT assets.

According to local news reports and disclosures from state authorities at Minnesota IT Services (MNIT), these hacks specifically targeted equipment connected via cellular communications at water towers and lift stations, causing operating controls to malfunction. Public utility disclosures from impacted municipalities—including Braham, Plymouth, South St. Paul, and Maple Plain—confirm that the town of Braham experienced a total operating control shutdown. This forced its well and water treatment plant offline, necessitating an emergency pivot to water tower reserves. While drinking water safety was maintained through rapid manual intervention by local operators, these news accounts highlight a widespread vulnerability in publicly accessible critical infrastructure controls.

The TTPs deployed in these intrusions specifically target vulnerabilities, exposed ports, and default configurations in major industrial hardware. Utilities using the following brands must conduct immediate asset inventories:

- Siemens Programmable Logic Controllers (PLCs) and modules.
- Schneider Electric industrial automation and control devices.
- Rockwell Automation / Allen-Bradley control systems.

CISA Technical Recommendations & Mitigation Summary

To secure industrial control systems and defend against the specific methods deployed in these recent breaches, CISA recommends that all utilities immediately implement the following defenses:

- **Isolate OT from the Internet:** Remove all PLCs, Human Machine Interfaces (HMIs), and supervisory controls from public-facing networks.
- **Secure Cellular Modems:** Audit and restrict internet-connected cellular communications at remote sites (e.g., water towers, lift stations) by establishing tight access-control lists (ACLs).
- **Enforce Multi-Factor Authentication (MFA):** Require robust MFA for all remote access connections into the utility network, without exception.
- **Change Default Credentials:** Force an immediate update of all factory-default usernames and passwords on PLCs, switches, and edge routers.
- **Audit Project Files:** Frequently verify the integrity of PLC logic and project files to ensure unauthorized modifications or code injections have not occurred.

For detailed Indicators of Compromise (IOCs), technical network maps, and step-by-step device hardening instructions, utilities should access the complete advisory at CISA Advisory AA26-097A.

How to Report a Suspected Breach

If a utility identifies unauthorized access, unusual PLC restarts, or unexpected cellular traffic, they must report the incident immediately to both state and federal entities. The FBI regional offices are in Pittsburgh and Philadelphia. The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000. You can contact CISA 24/7 at Report@cisa.gov or call (888) 282-0870.

Pennsylvania utilities can also report incidents to the Pennsylvania Criminal Intelligence Center (PaCIC). PaCIC is the primary All-Hazards Fusion Center for the Commonwealth of Pennsylvania. PaCIC coordinates the intake, processing and dissemination of intelligence and analysis concerning all threats and hazards to the Commonwealth. You can contact PaCIC at tips@pa.gov or call 1-888-292-1919.

Cyber incidents identified in the Commission's cyber incident reporting regulations (52 Pa. Code §§ 57.11 (electric), 59.11 (gas), 61.11 (steam heating) and 65.2 (water)) need to be reported to the PUC's Lead Emergency Agency Representative (AREP). The PUC's Lead AREP can be reached at 717-941-0003.

If you have any questions regarding this advisory, please contact Michael Holko, Director of the Office of Cybersecurity Compliance and Oversight, at 717-425-5327 or via email at miholko@pa.gov.

Sincerely,

Matthew Homsher
Secretary