Increased Cyber Threats Targeting Utilities

Due to a recent increase in cybersecurity threats that target utilities, the Cybersecurity & Infrastructure Security Agency (CISA) urges water and wastewater systems to take steps to protect their Internet-connected infrastructure from outside interference.

Programmable logic controllers (PLCs) are especially at risk, with unprotected, remote cellular connected SCADA devices or those reading lift stations being some of the most vulnerable.

> *"These threat actors are targeting water entities of all sizes. Even water organizations with mature cybersecurity processes should validate their external connections."*
>
> **CISA**

Read the full report

SUPPORT FOR SMALL SYSTEMS

NRWA has created the National Rural Water Cybersecurity Center to feature initiatives and resources specifically geared towards small systems. Visit their resource page to learn more about which program is the best fit for your utility's unique situation.

ADDITIONAL RESOURCES

There are multiple ways to report a cyber incident:

1. Contact CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-729-2472
2. Use CISA's online Incident Reporting System
3. Contact your local FBI field office

When preparing a report, record the following details:

- Date, time, and location of the incident
- Type of activity
- Number of people affected
- Type of equipment used for the activity
- Name of the submitting company or organization, and a designated point of contact

LINKS REFERENCED

CISA alert: cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs

National Rural Water Cybersecurity Center: nrwa.org/national-rural-water-cybersecurity-center/

CISA Incident Reporting System: cisa.gov/reporting-cyber-incident

FBI field offices: fbi.gov/contact-us/field-offices