

KONIAG PUBLIC WORKS OT CYBER RESILIENCE PACKAGE

Protect the systems that keep
your community running



30+ Systems

Water and wastewater utilities across Minnesota were hit in a recent coordinated attack.

Iran-Affiliated Actors

Federal advisories tie the activity to state-linked groups targeting internet-connected PLCs nationwide.

Manual Operations

Automated controls went offline at multiple facilities. Operators fell back to running plants by hand.

Public works organizations need cybersecurity designed for operational technology — not simply another IT assessment.

Water and wastewater infrastructure is an active cyber target. A recent coordinated attack hit operational technology at more than 30 water and wastewater systems across Minnesota — and federal advisories tie the pattern to state-linked actors probing internet-connected PLCs across U.S. critical infrastructure nationwide.

A Practical Path to OT Resilience

The Koniag Public Works OT Cyber Resilience Package helps organizations identify critical exposure, reduce immediate risks, and maintain essential services during a cyber incident.

01 Rapid OT/ICS Assessment

- Inventory critical PLCs, HMIs, SCADA systems, remote connections, and vendor access
- Evaluate internet exposure, network segmentation, credentials, logging, and backups
- Identify evidence of known attack activity
- Prioritize risks based on safety, compliance, and service continuity

02 Immediate Risk Reduction

- Protect internet-exposed operational technology
- Secure remote access with gateways, multifactor authentication, and monitoring
- Harden PLC, HMI, SCADA, firewall, and communications configurations
- Validate offline backups of controller logic and critical configurations

03 Response Readiness

- Establish focused monitoring for suspicious access and configuration changes
- Connect cyber-response procedures with plant operating procedures
- Define responsibilities across operations, IT, leadership, vendors, and emergency management
- Exercise a scenario involving the loss of automated controls

Prioritized Roadmap

Leadership receives clear findings, recommended actions, and an implementation roadmap organized around immediate, near-term, and strategic improvements.

Why Koniag?

Koniag combines two capabilities rarely found in one provider. Together, these teams understand how public works systems operate, and how to secure them without unnecessary disruption.



Builds and upgrades water and wastewater facilities. Automation, controls, PLC and HMI systems, engineering, commissioning, maintenance, and optimization.



Specialized OT/ICS capabilities spanning assessment, system hardening, secure architecture, threat detection, incident response, and recovery planning.

Built for Public Works

Water & Wastewater Utilities

Municipal, County & Tribal

Resource-Constrained Teams

Rural & Remote Facilities

Legacy & Mixed-Generation Controls

Secure the System. Prepare the Team. Protect the Community.

A cyber incident should not become a public-service crisis. Koniag can help reduce exposure and build the resilience needed to keep essential services running.



Scan to Start Your Rapid
OT/ICS Assessment

Schedule an OT Resilience Consultation With Koniag

Email: info@koniagcyber.com

Website: koniagcyber.com

Phone: (907) 261-4001