

How District Defense Group Uncovered and Closed a Live Path Into a Texas Water District's Control Systems

A real-world look at how an air-gapped environment was found exposed to the public internet — and what was done about it.

One independent advisor. Three security domains. **One remediation strategy.**

SECTOR
 **Municipal Water & Wastewater**

LOCATION
 **Texas**

SCOPE
 **2 Water Plants + 1 WWTP**

ENGAGEMENT PARTNERS
 **Specialized OT partners**



 This case study has been anonymized. All identifying details about the client district, its personnel, and its facilities have been removed or generalized.

02 THE DISCOVERY

WHAT THE DISTRICT BELIEVED

Water Plant 1 and Water Plant 2 control systems operated on an isolated network with no obvious path from the public internet.

WHAT DDG FOUND

Both water plants were actually connected to the internet through modems no one was managing. There was no industrial firewall protecting the control systems, and remote-access software was left running and reachable around the clock.

They thought the control systems were isolated. They weren't.

HOW DDG APPROACHED THE ENGAGEMENT

1 ASSESS Evaluate physical, operational, and cyber posture.	2 IDENTIFY Expose vulnerabilities and hidden dependencies.	3 PRIORITIZE Separate immediate risk from longer-term work.	4 REMEDiate Coordinate an actionable remediation program.	5 MONITOR Establish ongoing visibility and accountability.
---	--	---	---	--

WHO DID WHAT

DISTRICT DEFENSE GROUP — Lead Advisor & Project Manager

- Physical & Operational Security
- Public Safety Intelligence
- Risk Prioritization
- Remediation Management
- Board-Level Reporting & Accountability

SPECIALIZED OT PARTNERS — Technical Resources

- Industrial Control Systems (ICS) Engineering
- OT / SCADA Cybersecurity
- Network Analysis & Technical Remediation

DDG coordinated the specialist resources required for the ICS/cyber engineering work and translated the findings into a remediation plan the Board could act on.

03 WHAT WE FOUND & WHAT WE DID

Both water plants maintained internet-accessible remote connections to their control environments — with no industrial firewall or continuous monitoring in place.

CYBER & NETWORK NO INDUSTRIAL FIREWALL - Unattended remote access - No intrusion detection - No network traffic monitoring	PHYSICAL SECURITY ACCESS CONTROL & PERIMETER GAPS - Generic / shared master codes - Structural perimeter barrier gaps - Unsecured ingress points	OPERATIONAL READINESS FRAGMENTED RESPONSE - Alert fatigue - Siloed response protocols - No unified escalation path
--	--	--

14

WORKSTATION VULNERABILITIES IDENTIFIED

2 High • 11 Medium • 1 Low

CONNECTING FINDINGS TO IMPACT

INTERNET EXPOSURE No industrial firewall protecting the control environment.	→	INDUSTRIAL FIREWALL PROTECTION Purpose-built industrial firewalls designed and lab-tested for deployment at the water plants as part of the remediation plan.
UNCONTROLLED REMOTE ACCESS Unattended remote-access applications created persistent external connectivity.	→	SECURE, MONITORED REMOTE ACCESS Remediation plan transitions remote access to secured, logged, and monitored VPN connectivity.
NO CYBER VISIBILITY No continuous intrusion detection or network monitoring.	→	24x7 MONITORING & ESCALATION Remediation plan establishes continuous managed monitoring, alert analysis, and defined escalation.
PHYSICAL + OPERATIONAL GAPS Shared credentials, physical vulnerabilities, and siloed response protocols.	→	ACCOUNTABLE ACCESS & UNIFIED RESPONSE Remediation plan strengthens access controls and unifies escalation across physical security, operations, and cyber monitoring.

Network architecture was also documented to support cybersecurity governance and recognized industry frameworks.

04 THE RESULT

3

FACILITIES ASSESSED
2 Water Plants + 1 WWTP

14

WORKSTATION VULNERABILITIES IDENTIFIED
2 High · 11 Medium · 1 Low
Remediation plan developed

24×7

CYBER MONITORING
Established through the remediation program

4

MAJOR EXPOSURE AREAS
Addressed by a coordinated remediation plan

The assessment identified previously unknown internet exposure and additional physical, cyber, and operational vulnerabilities across the District's control environment. DDG developed a remediation plan addressing each exposure category and coordinated the specialized resources — including purpose-built firewalls, secured remote access, and continuous monitoring — required to carry it out. The District now has a documented path toward stronger monitoring, more accountable physical access, and unified incident response.

Security doesn't stop at the fence line.

ABOUT DISTRICT DEFENSE GROUP

District Defense Group is an independent security advisory firm serving Texas municipal utility and special districts. DDG assesses risk across physical security, operations, public safety, and cybersecurity, then coordinates the specialized resources required to remediate identified vulnerabilities. The result is one accountable security partner from assessment through implementation and ongoing oversight.

DO YOU KNOW WHAT'S CONNECTED TO YOUR DISTRICT'S CONTROL SYSTEMS?

If your district isn't certain what's really connected to the internet, that uncertainty is the risk.

SCHEDULE A CONFIDENTIAL INFRASTRUCTURE SECURITY ASSESSMENT



info@districtdefensegroup.com • (713) 305-2672 • Texas DPS License #B31016401