

The State of The District



DATE ISSUED August 4, 2026	PREPARED BY District Defense Group	DISTRIBUTION District Counsel & Consultants
-------------------------------	---------------------------------------	--

THE CURRENT CLIMATE

- Since late July 2026, water and wastewater utilities across at least seven states, including Minnesota, Michigan, South Dakota, and Georgia, have reported coordinated cyberattacks targeting Internet-connected programmable logic controllers (PLCs), the industrial devices that operate pumps, valves, and treatment equipment.
- In Minnesota alone, more than 30 community water systems were affected; several took systems offline or declared temporary emergencies. A related incident was reported at a South Dakota wastewater lift station.
- Federal investigators, including the FBI, EPA, and CISA, are examining a suspected link to Iran-affiliated hackers, though the U.S. government has not issued an official attribution as of this writing.
- Security researchers report roughly 10,000 similar industrial controllers are currently exposed to the Internet nationwide, meaning the configuration exploited in these attacks is common, not exceptional.

WHY THIS MATTERS FOR SPECIAL DISTRICTS

Many special districts, particularly MUDs and other water, wastewater, and utility districts, operate the same class of Internet-connected PLCs, SCADA systems, and remote monitoring equipment now being targeted, frequently installed by third-party vendors with limited district visibility into configuration or remote-access exposure.

Incidents that begin in operational technology can escalate into IT and administrative systems holding sensitive personal information, such as employee, resident, or customer records. When they do, the Texas Identity Theft Enforcement and Protection Act (Tex. Bus. & Com. Code § 521.053) requires notification to affected individuals, and to the Texas Attorney General when 250 or more Texas residents are affected, generally within 60 days of discovery. District counsel are well positioned to help clients assess this exposure before an incident sets that timeline in motion.

A Resource From District Defense Group

District Defense Group is an independent, vendor-neutral public safety and security advisory firm working with special districts across Texas. This bulletin is offered as a resource for district counsel and the consultants supporting their clients. Districts working with DDG, or attorneys who would like an independent overview of a client's operational technology exposure, are welcome to reach out to arrange a confidential briefing.

Sources: GovTech, "Water Utilities in Seven States Report Cybersecurity Incidents," July 31, 2026; SecurityWeek, "Dozens of Minnesota Water Utilities Targeted in Coordinated OT Attacks" and "US Water Cyberattacks Extend Beyond Minnesota to at Least 6 Other States," August 2026; NBC News, MPR News, and The Hacker News reporting, July–August 2026; FBI/EPA Public Service Announcement PSA260730; CISA Advisory AA26-097A; Tex. Bus. & Com. Code § 521.053. This bulletin is provided for general informational purposes and does not constitute legal advice.