GLOBAL DATA SYSTEMS

Cameron Parish Waterworks District 10

Committed to Providing Clean, Safe Water for our Entire Community

PROTECTING OUR WATER SYSTEMS: A VITAL PRIORITY

The security of our nation's water systems has never been more critical, especially for communities in Louisiana. Recent warnings from the Biden administration underscore the urgent need for heightened vigilance against cyber threats targeting water infrastructure.

Cyber attackers affiliated with governments such as Iran and China are actively targeting water and wastewater systems across the United States, posing a significant risk to our communities' safety and well-being.

Call Us:
(888) 435-7986

Email:
info@getgds.com

Visit:
www.getgds.com

Schedule a Consultation Today!

In a joint letter addressed to state governors, Environmental Protection Agency Administrator Michael Regan and National Security Advisor Jake Sullivan emphasized the alarming trend of disabling cyberattacks on essential water infrastructure.

Water and wastewater systems can represent an "attractive target" for cyberattacks because of their essential nature and frequent lack of "resources and technical capacity to adopt rigorous cybersecurity practices," said Michael Regan, the administrator of the Environmental Protection Agency (EPA), and White House national security adviser Jake Sullivan. These attacks, which have been attributed to groups linked to the Iranian Government Islamic Revolutionary Guard Corps and the Chinese state-sponsored group Volt Typhoon, have the potential to disrupt the vital lifeline of clean and safe drinking water in Louisiana and beyond, imposing substantial costs and endangering public health.

Our water systems, including those in Southwest Louisiana like the Cameron Parish Waterworks District 10, are vulnerable to various factors, including weak controls, insufficient funding, and staffing shortages. Despite their critical importance, many water facilities need more resources and technical capabilities to defend effectively against sophisticated cyber threats.

We must proactively safeguard our water systems from cyber threats in Louisiana. Basic cybersecurity precautions, such as resetting default passwords and updating software to address known vulnerabilities, can significantly mitigate risks and prevent disruptive cyber incidents.

Global Data Systems, a leading cybersecurity firm renowned for safeguarding critical infrastructure, launched a transformative partnership with Cameron Parish Waterworks District 10.

Find us on LinkedIn!

Through a comprehensive vCISO (Virtual Chief Information Security Officer) engagement, Global Data Systems brought its wealth of experience to fortify the security posture of the water district, ensuring the protection of vital resources and infrastructure. Recognizing the ever-evolving landscape of cyber threats, Global Data Systems' tailored approach addressed the unique challenges Cameron Parish Waterworks District 10 faced, empowering them with proactive strategies to mitigate risks and enhance resilience.

Global Data Systems explained the ongoing notifications by CISA and other state and federal agencies regarding consistent and current attacks on the wastewater and water sectors by nation-state bad actors. Through deep conversations with Cameron Parish Waterworks District 10 managers and board members, Global Data Systems provided reporting and guidance through a cyber security gap analysis and a path forward to obtain the needed hardware, software, and documentation to strengthen their cyber security posture.

With the efforts of Global Data Systems cybersecurity team, Cameron Parish Waterworks District 10 has been provided with a solid cybersecurity solution that will protect them against these ongoing and prevalent cybersecurity threats.

As of 2025, the threat landscape for critical infrastructure, particularly water and wastewater systems, continues to evolve rapidly. Recent developments include:

- Nation-state actors are increasingly leveraging AI to automate reconnaissance and identify vulnerabilities.
- The CISA 2025 Water Sector Resilience Initiative promotes stronger endpoint protection and network segmentation.

- Threats now target SCADA systems via compromised remote access tools, which are often overlooked.
- EPA audits, reinstated in late 2024, are enforcing compliance with updated cybersecurity standards for public utilities.
- Attacks such as Volt Typhoon have grown more sophisticated, blending long-term stealth tactics with data exfiltration efforts.

As part of our commitment to enhancing water system security in Louisiana and beyond, we invite state officials to join us in a collaborative effort to assess and address cybersecurity vulnerabilities within their jurisdictions. Together, we can ensure that all water systems comprehensively evaluate their current cybersecurity practices, implement robust security measures, and develop contingency plans to prepare for and respond to potential cyber incidents.

The safety and resilience of our water systems in Louisiana are paramount. By working together and prioritizing cybersecurity, we can fortify our defenses, protect our communities, and safeguard the integrity of our nation's critical infrastructure.

Join us in our mission to secure our water systems in Louisiana for generations to come.

Find us on LinkedIn!