



Written by [Veronika Kyrylenko](#) on September 1, 2026

Trump Admin Cyber Push Reaches Texas Water Systems, With Plans to Expand Nationwide

The Trump administration has launched a new cybersecurity initiative ostensibly aimed at protecting Texas water systems from foreign hackers.

The state and federal officials present the pilot program called Project Watershed 250 as a defensive effort. But it also advances a much broader shift: bringing locally operated critical infrastructure into an increasingly integrated network of federal, state, and private control.

If the pilot succeeds, the administration plans to roll out the model nationwide. The move carries particular consequences for Texas, where water has long been a critical issue and the rapid expansion of data centers is adding further strain. That raises grave concerns over federalization and the concentration of power over systems essential to everyday life.



RoschetzkyIstockPhoto/iStock/Getty Images Plus
Mansfield Dam at Lake Travis in Texas

Project Watershed 250

Governor Greg Abbott and White House National Cyber Director Sean Cairncross [launched Project Watershed 250](#) in San Antonio on Monday. Abbott argued,

Project Watershed 250 will connect water utility providers with cyber defense resources at no cost by leveraging the experience of private sector businesses with the expertise of the Texas Cyber Command. Our communities and water systems will be better secured from the onslaught of cyber-attacks.

“Many rural providers lack the resources they need to defend themselves,” his office added.

[Nextgov reported](#) that the six-month pilot will bring together the Office of the National Cyber Director, Texas Cyber Command, the Environmental Protection Agency (EPA), the Cybersecurity and Infrastructure Security Agency (CISA), and private technology companies.

The latter include Microsoft, Palo Alto Networks, Dragos, Reflection AI, Parsons, Fortinet, Cloudflare, and others. Participating utilities will receive cybersecurity and artificial-intelligence tools at no cost.

The administration plans to use Texas as a model for expansion across the country.

The immediate rationale is clear.

Minnesota [reported](#) in late July that more than 30 community water systems had been hit in what



Written by [Veronika Kyrylenko](#) on September 1, 2026

officials described as a “coordinated cyberattack.” Utilities in at least seven other states also [reported](#) cyber incidents to the FBI. Hackers targeted equipment used to remotely monitor and control water operations. They also changed IP addresses and passwords, causing operators to lose monitoring and control capabilities. Reported effects included pressure losses and flooding, while some affected systems had to rely on manual operations.

The Government Accountability Office (GAO) [warned](#) in May that Internet connectivity increasingly allows remote access to operational technology controlling “valves, pumps, and other physical devices.”

Watershed 250 is supposed to close those vulnerabilities.

A Bigger Federal Role

Yet the program also continues a years-long effort by Washington to expand its role in the cybersecurity of infrastructure traditionally operated by municipalities, regional authorities, states, and private companies.

The EPA [attempted in 2023](#) to require states to examine cybersecurity during periodic inspections of public water systems. Missouri, Arkansas, and Iowa challenged the move, and the U.S. Court of Appeals for the Eighth Circuit [stayed its implementation](#). The EPA withdrew the policy several months later, explicitly citing the litigation.

The underlying federal effort continued.

In 2024, the GAO [recommended](#) that the EPA evaluate whether its existing legal authority was sufficient to address cybersecurity risks and seek additional authority if necessary. The EPA later identified several critical gaps and limitations in its authority under federal drinking-water and clean-water laws to address them.

Watershed 250 takes a different approach. Rather than beginning with a federal mandate, Washington is offering expertise, technology, monitoring, and private-sector capabilities through voluntary participation and at no cost.

And Watershed is not occurring in isolation.

On August 12, Trump signed a [presidential memorandum](#) creating a federal program that allows vetted private companies to conduct cyber surveillance and cyber operations against designated foreign criminal organizations.

Those companies operate, according to the memorandum, “under the control and oversight of the Federal Government.”

Two weeks later, Trump [declared a national emergency](#) involving the bulk-power system. The order gives federal officials authority, under certain circumstances, to require foreign-manufactured or operated equipment to be identified, monitored, isolated, disconnected, replaced, or removed.

Together, these policies point toward a growing federal security architecture surrounding systems once largely controlled closer to home.

Meanwhile, Texas Needs More Water

The concern becomes more significant because water itself is becoming more contested.

Texas has long struggled with drought, aging infrastructure, and regional supply shortages. Mandatory rationing already exists.



Written by [Veronika Kyrylenko](#) on September 1, 2026

Under the [Texas Commission on Environmental Quality](#)'s most severe M3 drought category, outdoor water use can be prohibited and "all consumption may also be limited to each customer in specific ways."

Water suppliers are also required to maintain drought contingency plans. That includes procedures for enforcing mandatory restrictions.

At the same time, a rapidly expanding industry is adding new pressure.

The [Texas Tribune](#) reported last September that Texas had more than 400 data centers operating or under development. About 70 additional facilities had been planned. The report linked part of the buildout to the [\\$500-billion Stargate Project](#) launched by the Trump administration in early 2025.

The Houston Advanced Research Center (HARC) estimated that existing data centers would consume approximately 25 billion gallons of Texas water in 2025. And it gets worse:

By 2030, this demand could increase up to 2.7% of the total annual water use in Texas. That's the equivalent water consumption of 1.3 million [average U.S. households](#).

That statewide percentage can obscure far greater local effects. For instance, the impact is worse when developers build massive facilities in smaller communities or water-stressed regions.

What If the Threat Becomes the Pretext?

Project planners say the goal is to prevent hostile actors from attacking critical infrastructure. Yet at least some of that threat may itself be blowback from Washington's never-ending wars and foreign interventions.

Attribution in cyber warfare is also often complex, delayed, and initially uncertain. Even in the Minnesota attacks, federal investigators initially said Iranian responsibility had not been definitively established.

That uncertainty creates an obvious potential for abuse.

Such concerns are not abstract. Federal law enforcement has faced criticism over operations in which informants helped develop plots, including cases described as the FBI "[hatching and financing](#)" terrorist plots.

A future administration, national-security state, law-enforcement apparatus, or allied corporate interests could exaggerate a threat, misattribute an attack, or, in the most extreme scenario, manufacture an incident to justify powers that would otherwise encounter political resistance.

The important question is not whether current officials intend to do that.

It is whether the emerging architecture would make such abuse possible, if not appealing.

From Protection to Control

Cybersecurity access is not abstract.

Modern water networks rely on remote monitoring systems, programmable logic controllers, supervisory control, and data acquisition (SCADA) networks, pumps, valves, and other operational technology.

Parsons, one of the companies participating in Project Watershed 250, specifically [cited](#) its expertise in



Written by [Veronika Kyrylenko](#) on September 1, 2026

these systems.

Utilities also increasingly possess the ability to monitor consumption remotely. The EPA [says](#) advanced metering infrastructure can provide frequent, and in some cases real-time, information about customer water use.

What Watershed 250 potentially adds is another layer: a more integrated cybersecurity architecture connecting local utilities with Texas Cyber Command, federal agencies, and private companies.

Texas Cyber Command itself already has broad defensive authorities. House Bill 150, passed in June 2025, [authorizes](#) real-time cybersecurity monitoring, firewall management, intrusion detection, threat hunting, and coordinated operations to “isolate, contain, and mitigate” cyber incidents affecting participating systems.

Currently, those capabilities may protect water infrastructure.

But if shortages worsen, or another emergency is declared, the same combination of real-time monitoring, centralized cyber access, customer-level consumption data, and remotely controlled infrastructure could make rationing easier to monitor, coordinate, and potentially enforce.

That is why the larger issue is not simply whether hackers can reach America’s water systems.

It is who ultimately gains the ability to see, monitor, and influence the systems on which access to water depends, and how much of that power Americans are willing to centralize in Washington in the name of keeping them safe.



Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.