Opening Statement of Chairman Brian Babin

Environment Subcommittee Hearing
Research-Driven Resilience: Applying Science to Secure U.S. Water Systems from Cyber Threats
Thursday, May 21, 2026

Good afternoon. Thank you to our Subcommittee Chairman, Mr. Franklin, for presiding over this important hearing, and thank you to our witnesses for sharing their insights with us today.

Many associate cybersecurity with financial networks or the electric grid, yet the infrastructure that provides safe drinking water and manages wastewater is equally vital to households and industries nationwide.

Recent cyberattacks on water utilities in my home state of Texas highlight the growing threat facing critical infrastructure across the country.

In January 2024, the water system in Muleshoe, Texas, was reportedly hacked, leading to thousands of gallons of water spilling into the streets after attackers manipulated the city's control systems.

Authorities indicated that the suspected perpetrators even released footage demonstrating how they accessed and reset the controls. Incidents like this are a stark reminder that water and wastewater systems, especially those serving small and medium-sized communities, are increasingly vulnerable to cyber threats that can disrupt essential public services and jeopardize public safety.

What concerns me is not just that these systems are being targeted, but how unevenly prepared they are to respond. Across the country, there are more than 50,000 community water systems, many of them serving small populations with limited technical staff.

Often, these facilities lack the funding to implement cybersecurity measures. Many rely on decades-old industrial control systems designed when cyberwarfare was more science fiction than a real-world threat. Others depend on third-party contractors for maintenance and software updates, creating additional points of entry for attackers.

The reality is that defending this infrastructure has become extraordinarily complex. It is no longer a challenge that human operators alone can manage.

As water systems undergo rapid digital modernization, the boundaries between information technology and operational technology have blurred. Today, an attack can begin with something as simple as a phishing email, which then moves across unsecured computer systems into the controls that manage pumps, valves, and chemical treatment processes. In some cases, attackers

do not even need to directly seize control to cause disruption. Simply by targeting monitoring systems, bad actors can force operators to pause services.

For years, conventional wisdom suggested that keeping critical systems isolated from the internet, a security technique known as "air-gapping," was the best defense against cyber threats. But that approach alone is no longer sufficient or practical.

Modern water systems depend on connectivity for cost-effective remote management, and even so-called "isolated" networks have proven vulnerable to determined and increasingly sophisticated adversaries.

We need to examine how innovation can help close these gaps. Advances in automation, artificial intelligence, and anomaly detection could offer new tools for identifying threats earlier.

But adopting these technologies could also have the unintended consequence of introducing new risks if they are not implemented securely from the start. Research will be critical to ensuring cybersecurity is incorporated into the design of new technologies intended to address existing vulnerabilities and improve system efficiency.

This hearing is an opportunity to move beyond identifying problems and toward meaningful solutions that recognize the complexities of our water systems, the constraints they face, and the evolving nature of the threat landscape.

I look forward to today's discussion, and I yield back the balance of my time.