Opening Statement of Chairman Scott Franklin

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

Good afternoon, and thank you to our witnesses for joining us today. The purpose of this hearing is to examine how environmental research and development protects our nation's water systems from cyber threats. These threats come from foreign adversaries, malicious actors, and ransomware gangs seeking to exploit vulnerabilities in critical infrastructure.

Just last month, the Environmental Protection Agency, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and National Security Agency issued a joint advisory warning the water sector about an urgent cybersecurity threat linked to Iran-affiliated actors.

My home state of Florida has already seen the consequences of cyber issues in our water system. In 2021, a cyber-lapse in Oldsmar, Florida, lead to a situation where sodium hydroxide levels in the water supply were digitally increased for a brief period from normal treatment amounts to deadly levels before quickly being reverted.

During my time in Congress, I've been a strong advocate for increased funding for local water districts. Through the FY26 Appropriations process, I helped secure $13 million in Community Project Funding Requests to support critical water and wastewater improvements across Florida's 18th District, including meaningful upgrades in Auburndale, Bartow, and Lakeland. In FY27, I am supporting Polk County with several new projects, as well as other water infrastructure upgrades across Hendry and Highlands counties.

These projects are essential, but they only scratch the surface of the need. Fewer than 20 percent of Florida utilities currently meet the Department of Homeland Security's standards for ransomware preparedness. And aging infrastructure only compounds the challenge. That is why I'm continuing to advocate for additional funding in FY27.

The far-reaching implications of a successful cyberattack that disrupts water treatment and distribution systems cannot be overstated. Access to clean and safe water is foundational to economic growth, as well as public health and safety. A cyberattack on water systems could lead to widespread ramifications across the chemicals, manufacturing, and energy sectors, all of which depend upon access to water. It could also severely impact emergency response operations, hospitals, firefighters, and food production.

The water sector is vulnerable because many utilities, especially small and rural systems, rely on ratepayers to fund upgrades. Oftentimes, they lack the resources to invest in cybersecurity and

modernization. As infrastructure ages and technology becomes more interconnected, limited funding leaves these systems increasingly exposed to cyber threats.

At the same time, water systems are rapidly digitizing. Many are adopting AI management tools, smart sensors, remote controls, and cloud-based platforms. Most importantly, utilities are increasingly dependent on supervisory control and data acquisition systems, which are some of the highest risk targets for cyberattacks.

These technologies can greatly improve efficiency, especially for small and rural systems, but they also increase potential attack pathways and make incidents harder to detect.

That is why we must continue supporting research and development that produces affordable, cyber-resilient technologies for the water sector. Security cannot be treated as an afterthought. It must be built into these systems from the start, through approaches like the Cybersecurity and Infrastructure Security Agency's 'Secure by Design' framework.

We have a responsibility to ensure utilities of all sizes can access technology that is resilient, secure, and practical to deploy. Strengthening the research ecosystem and investing in innovation will defend our critical infrastructure.

I am hopeful today's hearing will help identify the research and development priorities needed to strengthen and protect our water infrastructure from cyber threats.

I look forward to today's testimony and discussion. Thank you.