LOTSIXTEEN

Committee:	Senate Environment & Public Works Committee
Event:	Identifying and Addressing Cybersecurity Challenges to Protect America's Water Infrastructure
Date:	February 4, 2026

Executive Summary: The hearing examined cybersecurity vulnerabilities in the nation's water infrastructure and sought to strike a proper balance between federal regulation and local capabilities across 170,000 diverse water systems. Members from both parties acknowledged the need to strengthen cybersecurity measures and provide effective guidance for the water sector, recognizing that water utilities vary in terms of resources and workforce capabilities, among other variables. They offered various proposals, such as implementing "circuit riders" and utilizing market-based mechanisms like requiring cyber insurance to encourage defensive upgrades, along with expanding the Environmental Protection Agency's (EPA) authority. Meanwhile, witnesses unanimously agreed that insufficient funding and a shortage of cybersecurity experts are significant barriers to achieving cyber resilience in the water sector. They urged Congress to develop practical and effective tools to help utilities enhance their cybersecurity defenses.

Member Toplines:

Chair Shelley Moore Capito (R-WV): Capito emphasized that water utilities are increasingly targeted by foreign adversaries such as Iran, China, and Russia, underscoring the need to balance the adoption of digital control technologies with robust defense mechanisms. She argued that solutions must be tailored to utility size and location rather than a "one-size-fits-all" federal mandate, which she contended would be unworkable for small systems already managing limited resources. Moreover, Capito stressed the importance of empowering local utilities to address challenges through flexible toolkits rather than burdensome regulations.

Ranking Member Sheldon Whitehouse (D-RI): Whitehouse warned that state-sponsored actors are relentlessly attacking American critical infrastructure facilities and that current information-sharing efforts are insufficient to meet this ongoing threat. He criticized the Trump Administration for weakening federal cybersecurity capabilities and cutting research funding, arguing that the water sector needs increased information sharing and additional resources to modernize infrastructure and cyber defenses. Whitehouse highlighted that updating cybersecurity measures is often deferred to maintain service levels, a dynamic that must change to meet new and emerging threats.

Witness Toplines:

Dr. Scott Simonton, Fellow, Marshall University Institute for Cybersecurity: Dr. Simonton highlighted that although small water systems have implemented modern digital monitoring, they do not have the same cybersecurity mandates and staffing levels as larger utilities. He proposed creating a scalable "circuit rider" support framework, similar to the U.S. Department of Agriculture's Technical Assistance Program for rural utilities, that includes targeted assistance for basic cybersecurity practices. He advocated for incentives to encourage small systems to adopt federal security requirements and public-private partnerships.

Matt Odermann, Executive Board Member, North Dakota Rural Water Systems Association: Odermann argued that federal cybersecurity efforts should prioritize assistance over enforcement. He highlighted that framing cybersecurity solely as a compliance obligation instills fear of punitive action among operators. To address this, he recommended funding new mandates focused on foundational controls, such as password management, rather than focusing on complex nation-state threats. Additionally, he suggested using trusted sector partners to help bridge technical and structural gaps in cybersecurity.

Scott Dewhirst, Deputy General Manager, Fairfax Water (on behalf of Association of Metropolitan Water Agencies): Dewhirst stated that voluntary federal guidance is insufficient and called for the establishment of a "Water Risk and Resiliency Organization" modeled after the energy sector's North American Electric Reliability Corporation to develop and oversee cybersecurity standards and guidelines. He emphasized the need for dedicated grant funding to help systems invest in software and personnel, noting that cybersecurity competes with infrastructure upkeep for limited financial resources.

Major Takeaways:

- Chair Capito identified a data gap regarding the number and origin of attacks, arguing that better metrics are essential for developing best practices. She also discussed the difficulty of recruiting young people into the water utility sector and suggested that modernization and cybersecurity could serve as recruitment tools.
- Ranking Member Whitehouse argued that the committee should expand EPA authority to help update digital infrastructure and noted that the $50 billion provided by the *Infrastructure Investment and Jobs Act* (P.L. 117-58), was a good start, but ultimately insufficient.
- Sen. **Lisa Blunt Rochester** (D-DE) discussed the Water Infrastructure Resilience and Sustainability Act (S. 3590), which she introduced with Sen. **John Curtis** (R-UT) to reauthorize EPA grant programs that help water systems address and reduce cybersecurity threats.

- Sen. **Ed Markey** (D-MA) promoted his bill, the Water Intelligence Security and Cyber Threat Protection Act (S. 1118), which would direct the EPA to develop and implement a program that provides utilities with the resources to access and maintain services with the Water Information Sharing and Analysis Center (Water-ISAC).
    - Markey recalled his previous efforts to mandate cybersecurity upgrades for electric utilities, noting that industry lobbying defeated those measures, leaving infrastructure vulnerable to costly, harmful attacks.
- Sen. **Adam Schiff** (D-CA) stated that he is working on legislation to provide the EPA with more tools to address cyber threats and provide resources for fortification without impacting ratepayer costs.
- Capito inquired about the viability of a "circuit rider" cybersecurity program, suggesting that a plug-and-play framework is necessary for small systems that cannot afford dedicated staff.
- Sen. **Kevin Cramer** (R-ND) emphasized the need for collaboration in rural areas while protecting the sovereignty and autonomy of local water systems.
- Sen. **Pete Ricketts** (R-NE) highlighted staffing shortages in rural communities and suggested that cloud-based management platforms could offer security advantages such as built-in protections and geo-location diversity.
- Sen. **Jon Husted** (R-OH) noted during his questioning that rural water systems face daily attempted cyberattacks and that human error remains a primary vulnerability that requires constant training and vigilance.
- Whitehouse proposed requiring "cyber insurance" riders in general liability policies to force the insurance industry to evaluate utility vulnerabilities annually and to drive the adoption of defensive standards.
    - Cramer expressed interest in the insurance proposal, suggesting that a market-based insurance requirement might be a more effective regulatory mechanism than a government agency.
- Ricketts suggested that better documentation of attacks specifically targeting water infrastructure is necessary to differentiate the threat level from that in other sectors, such as healthcare.
- Blunt Rochester highlighted the importance of stackable cybersecurity credentials to help small utility staff build the necessary skills without leaving their systems for extended training.