TESTIMONY OF

MATT ODERMANN, PAST-PRESIDENT, NORTH DAKOTA RURAL WATER SYSTEMS ASSOCIATION

ON BEHALF OF THE

NATIONAL RURAL WATER ASSOCIATION

BEFORE THE U.S. SENATE COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

HEARING ON IDENTIFYING AND ADDRESSING CYBERSECURITY CHALLENGES TO PROTECT AMERICA'S WATER INFRASTRUCTURE

FEBRUARY 4TH, 2026

Good Morning, Chairman Capito, Ranking Member Whitehouse, Senator Cramer, and Members of the Committee. Thank you for the opportunity to testify on this important issue.

My name is Matt Odermann, and I hail from the great state of North Dakota. I serve as Past President of the North Dakota Rural Water Systems Association, which includes over 282 member systems, representing more than 97% of the state's population. I am especially proud of my service as a board member for more than a decade with All Seasons Rural Water Users District, a small rural water system serving the north-central region of North Dakota.

I am here on behalf of the National Rural Water Association (NRWA), the country's largest water utility association with over 31,000 utility members dedicated to drinking water quality, environmental protection, and protection of public health. NRWA provides training, financial management support, emergency response, disaster relief, environmental compliance, energy audits, governance, and on-site technical assistance to water and wastewater utilities to enhance the public health and safety of citizens in small and rural communities in all 50 states and Puerto Rico. I can attest that this organization truly promotes the water and wastewater professionals that serve small and rural communities across the country and is unmatched in supporting the grassroots advocacy efforts required to help rural America prosper. Additionally, I have represented NRWA for the past two years as a voting member on the Cybersecurity and Infrastructure Security Agency's Water and Wastewater Sector Coordinating Council. In that role, I have participated in a cybersecurity task force focused on developing a practical plan of action to help the water and wastewater sector advance its cybersecurity posture and move forward on key cybersecurity initiatives.

For more than 20 years, I have worked in information technology and cybersecurity-related roles across critical infrastructure sectors, including telecommunications, water, and energy. I hold several industry cybersecurity certifications and have experience spanning both the technical and governance aspects of cybersecurity. I currently serve as a cybersecurity supervisor for an electric generation and transmission cooperative that operates a diverse portfolio of power generation resources and serves a multi-state region. My career has given me extensive experience addressing the challenges of securing

information technology (IT), operational technology (OT), and converged IT/OT environments across multiple critical infrastructure sectors.

Cybersecurity is not just a water and wastewater issue. It is not just a small organization issue, and it is not just a rural issue. Cybersecurity touches every community, every state, and every part of our country. We have seen cyberattacks against water utilities of all sizes, some privately owned and others publicly owned. Every critical infrastructure sector has its own cybersecurity challenges, and within the water and wastewater sector, the needs of systems vary widely depending on size, staffing, and resources. Thankfully, there is growing alignment between the Environmental Protection Agency (EPA) and the water sector on basic cybersecurity safeguards and practices, which is an important and encouraging step.

While the cybersecurity threats and risks facing the water and wastewater sector are real, there are also meaningful positive developments occurring at a rapid pace. Cybersecurity awareness is clearly increasing across the sector, driven by growing engagement between utilities and trusted trade associations such as the National Rural Water Association (NRWA) and the Water Information Sharing and Analysis Center (WaterISAC).

In collaboration with cybersecurity leaders including the SANS Institute, Microsoft, and other partners, NRWA regularly provides cybersecurity-focused training, technical assistance, and conference programming to help utilities better understand and manage cyber risk. NRWA and the SANS Institute have partnered to deliver practical tools and resources specifically designed for small and rural public water systems. As part of this

collaboration, SANS provides NRWA members with a series of cybersecurity training modules that systems can complete to strengthen foundational protections.

NRWA and WaterISAC are also partnering to expand access to threat intelligence and information sharing. Water systems serving 3,300 people or fewer are eligible for a free WaterISAC membership, which provides the water sector's most comprehensive source of cyber and physical threat information. Participating systems receive WaterISAC's biweekly Security Resilience Update, access to monthly threat briefing webinars, and use of an extensive cybersecurity resource center.

Additionally, NRWA has partnered with the Center on Cyber and Technology Innovation and Microsoft's Cyber Readiness Institute to launch the "Phased Critical Infrastructure Pilot: Resiliency for Water Utilities." This initiative provides certified cyber coaches, supported training, and practical resources focused on strengthening cybersecurity risk management and improving the ability of utilities to respond to and recover from cyber incidents.

NRWA has also worked with the University of Chicago Harris School of Public Policy's DEF CON Project Franklin, which mobilizes volunteer cybersecurity experts to help protect vulnerable sectors, including water systems. Through this partnership, NRWA has connected water utilities with volunteer experts to provide additional technical support.

Through these efforts, NRWA is helping foster a culture of cybersecurity awareness and practical cyber hygiene that reflects the operational realities of small and rural water systems.

Anecdotally, I see more rural water managers asking thoughtful questions about cybersecurity and moving away from the mindset that "it won't happen to us," toward a recognition that a cyber incident could happen to them and could have serious consequences for their systems and communities.

The vast majority of public water and wastewater treatment systems are communities with populations of 10,000 or less. About 91% of the approximately 50,000 community drinking water systems (typically their local governments) are small and 80% of the country's more than 16,000 wastewater systems serve fewer than 10,000 people.

In West Virginia, 393, or 94%, of the total 418 community water systems serve a population of fewer than 10,000 persons.

In Rhode Island, 75 or 90%, of the total 90 community water systems serve a population of fewer than 10,000 persons.

In North Dakota, 296, or 96%, of the total 306 community water systems serve a population of fewer than 10,000 persons.

Small and rural communities share the same critical public responsibility as any major city: complying with the Safe Drinking Water Act and Clean Water Act, and delivering safe drinking water and reliable sanitation every second of every day. The biggest difference, however, is scale. Small water and wastewater systems operate with limited staff, revenue, and technical capacity, yet we are held to the same federal standards and public expectations as the largest metropolitan utilities in the country.

That reality is of the utmost importance as this Committee considers how to address cybersecurity challenges and protect America's water infrastructure. The

cybersecurity posture of a large metropolitan utility is fundamentally different from that of a small or rural system. Large cities operate highly complex SCADA and cybersecurity architectures, with dedicated IT staff, sophisticated monitoring tools, and the benefit of financial resources that come with their economies of scale. While that complexity presents more potential cyber targets, those systems are also supported by robust technical and financial defenses and they are doing a very good job protecting their infrastructure.

Small systems operate very differently. Our systems and infrastructure are smaller, but our margins are razor thin. Rural water systems do not have in-house cybersecurity teams. We rely on trusted technical assistance and operators who are already overworked. In rural America, cybersecurity is not a question of indifference or neglect- it comes down to capacity.

And yet, the consequences of a successful cyber incident in a small community would extend far beyond that system's service area. A cyber driven contamination event in a rural town would not remain a local story. It would trigger national fear and erode public confidence in drinking water systems everywhere. That is precisely why protecting small systems is just as important to the overall resilience of the nation's water sector.

Small utilities have extremely limited financial resources, and those dollars must be targeted to their most urgent needs such as replacing failing infrastructure, meeting existing regulatory requirements, and keeping water affordable for their customers. Any new federal cybersecurity initiatives that emphasize compliance over capacity risk diverting scarce resources away from those priorities. And unlike larger utilities, small

systems cannot simply raise rates to absorb new federal requirements. In many rural communities, even modest rate increases can force low-income households to choose between water service and other basic necessities. Federal cybersecurity efforts should focus on technical assistance, training, and targeted investments that strengthen system capacity over time, while enhancing security without undermining affordability or reliability. That is how we protect public health, maintain public trust, and build a truly resilient national water sector.

While EPA's initial entry into cybersecurity regulation may have been well-intentioned, I believe their approach created confusion and unintended consequences, especially regarding expectations for small communities. Fortunately, there are industry trade associations like NRWA and federally supported sources such as WaterISAC and CISA that are seen as non-regulatory, operationally focused, and seen as "On your side".

From the perspective of the water and wastewater sector, the Environmental Protection Agency (EPA) is traditionally viewed as a regulator, not as a cybersecurity partner. EPA's historic role has been centered on environmental compliance and public health oversight. When cybersecurity was introduced into state sanitary surveys of water systems, along with varying expectations on how to address those requirements, it created significant confusion and implementation challenges for both state primacy agencies and water utilities.

Many utilities perceived this as being asked to self-report cybersecurity weaknesses to a regulatory body. That raised concerns such as: Could this information become a violation? Could it be used in enforcement actions? Even when EPA's intent may not have

been punitive, the reality is that the regulatory power dynamic shapes how these actions are received. Long-term trust and effective progress are built on collaboration and technical partnership, not on civil penalties and enforcement-driven relationships.

Federal cybersecurity oversight and regulation are not feasible or affordable without adequate funding, training resources, and dependable technical assistance. What water utilities and state primacy agencies heard when the sanitary surveys were going to include a cybersecurity component was that cybersecurity is now part of compliance. Achieving a cybersecure water and/or wastewater utility takes a trained workforce, sustained and prioritized investment, and trusted, effective technical assistance.

It's also important to note that there is a cultural gap between water operations professionals and cybersecurity professionals. Operators are trained to focus on water quality, pressure, pumps, chemistry, and keeping systems running 24/7. Cybersecurity professionals focus on risk, vulnerabilities, and controls. Those worlds don't always speak the same language. When cybersecurity guidance is delivered in purely technical or compliance-driven terms, it can feel disconnected from day-to-day utility operations.

What works better is when cybersecurity is framed as operational resilience - protecting pumps, treatment processes, SCADA systems, and the ability to deliver safe drinking water and manage wastewater. When cybersecurity is explained in terms of keeping water flowing and protecting public health, operators understand it. That translation layer is critical, and NRWA plays a vital role in bridging that gap.

Based on my experience in water, energy, and telecommunications, I would offer a few key principles.

1. Lead with assistance, not enforcement.

If cybersecurity is perceived primarily as a compliance requirement enforced by a regulator like the Environmental Protection Agency (EPA), utilities will naturally be cautious and defensive. If it is presented as risk reduction support, with trusted partners and clear technical help, adoption will be much stronger.

2. Fund any mandate.

Cybersecurity improvements require hardware, software, technical assistance, training, and staff time. For small systems, even a few thousand dollars can be a barrier. Grants, low-interest loans, and set-asides specifically for cybersecurity in water infrastructure programs are essential. You cannot build resilience without resourcing it.

3. Focus on foundational controls.

Most water systems are not struggling with advanced nation-state threats first. They are struggling with phishing, weak passwords, outdated systems, and lack of backups. Federal efforts should prioritize practical, achievable baseline controls rather than complex frameworks that overwhelm small utilities.

4. Use trusted intermediaries.

Organizations like NRWA, WaterISAC, and state rural water associations have decades of established trust with utilities. When cybersecurity guidance and programs flow through these channels, they are more likely to be understood, accepted, and implemented.

5. Recognize diversity in the sector.

A small rural system serving 800 people with two employees cannot be treated the same as

a large metropolitan utility with a full IT department. A one-size-fits-all approach will fail. Flexibility and scalability must be built into any federal cyber action.

The bottom line is that NRWA strongly supports additional federal investment in cybersecurity. With these resources, NRWA would expand support to help utilities certify and complete their EPA required Risk and Resilience Assessments, increase no cost security evaluations and follow up implementation support, expand cyber training in every state, improve information sharing and threat briefings in partnership with our federal and sector partners, and develop peer-to-peer support networks that systems can use long after initial training. These enhancements will translate federal dollars into practical, scalable support that small utilities can rely on to reduce cyber risk and increase resilience.

Water and wastewater utilities understand their responsibility. They are deeply committed to protecting public health and the environment. Cybersecurity is now clearly part of that responsibility, but it must be approached in a way that reflects the realities on the ground.

With the right balance of partnership, funding, practical guidance, and respect for the operational mission of utilities, we can meaningfully improve cybersecurity across America's water infrastructure — not through fear, but through collaboration and resilience.

Our goal should be to help water and wastewater systems build layers of resilience; steadily, practically, and with the right support, so that when challenges come, communities remain protected and essential services continue without interruption.

On behalf of the 31,000 small and rural systems NRWA represents, thank you, Madam Chairman and Members of the Committee for the honor to testify. We appreciate your leadership and all the opportunities this Committee has provided rural America to participate in the federal water and environmental legislation and policy crafting process. I look forward to your questions.