NATIONAL
RURAL WATER
ASSOCIATION
NRWA *America's Largest Utility Membership*

GEORGIA RURAL WATER ASSOCIATION
GRWA

TESTIMONY OF

RICK JEFFARES
PRESIDENT, GEORGIA RURAL WATER ASSOCIATION

BEFORE THE
U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON ENVIRONMENT, MANUFACTURING & CRITICAL MATERIALS

HEARING ON
"ENSURING THE CYBERSECURITY OF AMERICA'S DRINKING WATER SYSTEMS"

JANUARY 31, 2024

Good afternoon, Chairman Carter, Vice Chairman Joyce, Ranking Member Tonko and Members of the Committee. It is an honor to testify before this Committee on this timely and important subject. I am Rick Jeffares; President of the Georgia Rural Water Association and I am here on behalf of the National Rural Water Association (NRWA). NRWA represents over 30,000 water and wastewater utilities serving our small, rural communities across the country. The Georgia Rural Water Association has over 2,100 members representing over 2,400 permitted systems that serve a population of over 10 million throughout the state. Small, rural systems serving less than 10,000 people make up approximately 93 percent of community water systems in Georgia. I currently support the operation and management of over 90 small, rural utilities throughout Georgia. Additionally, I own and operate 4 rural water systems serving 500 residents.

Small and rural communities have the very important public responsibility of complying with all applicable federal Safe Drinking Water Act and Clean Water Act regulations and for supplying the public with safe drinking water and sanitation every second of every day. Over 91% of the approximately 50,000 community water systems serve fewer than 10,000 persons and 81% serve fewer than 3,300 persons. Small and rural communities often have difficulty complying with complicated federal mandates and providing safe/affordable drinking water and sanitation due to limited economies of scale and lack of technical expertise. This difficulty is eased due to ongoing and continuing support offered through rural water training and technical assistance programs.

It's also important to note that small and rural utility systems only operate to serve the public's interests. Small water systems in Georgia are governed by residents of the communities they serve and live in. In Georgia and around the nation, these systems only exist to serve the public and are eager to take all feasible and necessary actions to protect the cybersecurity of our public drinking water supplies. This means that any federal initiative to protect the country's public water supplies should be assistance-based. We need help in the form of technical assistance on how to best implement the newest and most advanced cyber protection actions for our specific water infrastructure as opposed to a regulatory construct. We need help, not enforcement.

I am here today to talk about cybersecurity from a small systems perspective and the steps needed to harden our defenses. To meet these challenges, NRWA is evaluating and participating in several collaboration activities that have the potential to be real solutions for securing the water sector from cyber threats. My testimony includes these voluntary efforts.

My testimony also provides three suggestions as a path forward for consideration as this Committee addresses Cybersecurity protection for America's drinking water systems. The three suggestions are as follows:

1) A path forward must include working with the water sector in a good faith effort to achieve practical safeguards and solutions. With approximately 50,000 community water systems in the country, to adequately address an effort on this scale will require industry participation at all levels, both urban and rural with our federal partners.
2) Any additional or existing technical assistance provided by Congress through EPA to address this issue should be carefully drafted to ensure anticipated outcomes are feasible, including requiring 3rd party non-profits that are selected for funding have qualified and experienced personnel that possess cyber expertise, combined with practical knowledge of water systems operations.
3) Cybersecurity of our water infrastructure must be a shared responsibility. Vendors that have the benefit to receive federal dollars that sell and/or install automated equipment, technology, and software to a utility, should be required to meet standard protocols, established by EPA and other agencies, to better protect water utilities from cyberattacks.

Any federal government policy for water cybersecurity must treat small and large communities very differently while recognizing the fundamental differences in the complexity of the water systems, financial resources, and technical capability. For small towns in Georgia, a $5,000 dollar cost is a significant expenditure. Small and rural communities have a limited workforce including volunteers and part-time employees, who need to implement all safety measures, manage all treatment of the water, read the meters, be on call at night for line breaks, manage the wells, the pumps, the water towers, take all the required U.S. Environmental Protection Agency (EPA) tests including the lead tests, operate the chlorine disinfection and pH adjustment processes which require constant monitoring, submit all the test results to the state, exercise our pumps and valves, sample the water for a variety of water quality parameters every day, complete the federally mandated public water quality report every year, respond to any problems that can occur at any time, and keep the water safe and flowing to every citizens' tap every second of every day, and the list goes on.

As you know, our water systems, like every entity in both the private and public sectors, have proven vulnerable to cyber and physical attacks, both from foreign and domestic adversaries. Small and rural systems are not exempt from this threat. Protecting small and rural water systems from cyberattacks has been a top priority for the National Rural Water Association (NRWA). Unfortunately, given the scope and complexity of cyberthreats to critical water infrastructure, the reality is most rural utilities lack the financial resources and in-house expertise to defend themselves. To meet these challenges, NRWA is proactively evaluating and participating in several collaborative exercises that have the potential to be real solutions for the water sector.

When I started my career in 1982, everything was handled by phone. In rural Georgia computers didn't enter the process until the mid-nineties and my generation didn't grow up with the technology available today. We certainly didn't have Supervisory Control and Data Acquisition (SCADA) systems, cell phones, remote access, or cyber security protection software. It was a simpler time in the water industry. Now, when I get a new cell phone, I need my granddaughter to set it up for me. Although cybersecurity is in the news and a reality, the challenges small water systems face goes beyond this threat. Physical security, for example, has the potential to cripple a system and impact customers' health and confidence in their water.

Additionally, our workforce is ageing. The average age of a water operator in Georgia is 58. With so many retirements on the horizon, it is critical to recruit the next generation of water operators. Water and particularly wastewater operations is not a glamorous field. Additionally, because of lean budgets, rural water systems struggle to offer the competitive salaries necessary to recruit and retain good employees. NRWA is addressing this challenge through our successful U.S. Department of Labor registered apprenticeship programs. We anticipate the next generation of water operators will have a higher level of computer and cyber sophistication than I possess but, in the meantime, we all need to continue learning to implement strong cybersecurity plans.

Cybersecurity is not only important to NRWA, but across the entire sector, as new challenges to protect public health are increasing at a rapid rate. NRWA values collaboration and information sharing with our federal partners to address the dynamic nature of the cyber threats facing our critical infrastructure. The water sector has actively participated in multiple briefings provided by the Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Environmental Protection Agency (EPA) that illuminate the evolving threat environment. These briefings help professional organizations, such as NRWA, build awareness among members.

NRWA has supported assessment tools from CISA and EPA, and we work daily to build the partnerships needed to harden our cyber defenses. Success will require responsibility and collaboration.

The federal government and the private sector have sought to address these concerns for years. However, many proposed solutions substantially increase administrative burdens, are cost prohibitive, and may not yield results necessary to protect small and rural communities. New regulations could exacerbate these unintended consequences. Many small and disadvantaged communities are limited in their financial and staff capacity necessary to address the current regulatory environment without direct third-party professional assistance. Compliance with emerging contaminants like PFAS and the new Lead and Copper Rule is extremely expensive and the funding available to comply with these regulations may not cover the anticipated costs. Many of these smaller rural utilities that serve very low-income customers operate on a very thin margin and have no options except to pass on increased costs to the residents they serve. We simply can't just increase water rates to cover the cost of new federal regulations. The potential impact to our low-income residents could force vulnerable, low-income customers to make difficult decisions, like choosing which living essentials they can go without such as healthy food, safe housing, or medical care.

Additional unfunded regulations not only burden the water systems, but the state primacy employees that are charged with enforcement. The Rural Water constituency works closely and collaboratively with these public health professions, but much like small water utilities, these agencies may lack the resources and expertise to add cybersecurity enforcement to their workload. They also lack the time and technical expertise to assess every water system in their jurisdiction to determine if all the complex requirements of a potential cybersecurity regulation are being met.

The technical and financial challenges small and rural systems will face must be at the center of any federal action on cybersecurity for water systems. Presently, cybersecurity is not high on the list of potential threats to Georgia's small and rural communities due to population size, limited use of the SCADA systems, and lack of connectivity to the internet. The greatest threat is likely the physical disruption of the water supply. However, our most significant issue, from my perspective, is the lack of personnel to operate and maintain the public water supply, fulfill the mandatory compliance testing and reporting, and respond to the typical small-scale emergencies in a water distribution system such as line breaks and leaks. The reality is that small towns have limited financial resources, which must be targeted to meet our greatest needs.

Technical Assistance (TA) will be a critical component to the success of any federal cybersecurity action. However, technical assistance (TA) funding alone will not secure the water sector from cyber threats. I can't emphasize this point enough, if it is the desire and intent of this committee to provide EPA additional resources to assist small communities to address cyber vulnerabilities- how the agency structures the assistance through their guidance combined with experience and ability of the awardees that receive the funding, will directly determine the outcome of any intended results.

NRWA feels strongly that properly structured TA for cybersecurity would meet Congress's intent of impacting water security enhancements in the Safe Drinking Water Act Funding Priorities. Under EPA's current programs, TA is awarded to many new providers and dollars are being capped in numerous categories, creating barriers to provide uninterrupted, critical services on a national level. Many of these providers lack any experience working with small, rural water systems.

For over 45 years, the National Rural Water Association and our 50 state affiliates have been providing small, rural, tribal, and disadvantaged communities with local, on-site technical assistance and training. This is not a new concept. The Infrastructure Investment and Jobs Act of 2021 (IIJA) included multiple technical assistance provisions and set asides to provide assistance directly to communities that lack the financial, managerial, and technical capacity to access newfound federal resources. Rural Water, through trusted relationships and exceptional technical expertise, has established itself as the premier resource and partner for small, rural, disadvantaged, and tribal communities to comply with the numerous federal Environmental Protection Agency (EPA) regulations, avoid EPA fines, access water infrastructure funding, and safely operate drinking water and wastewater systems.

Our constituency exists to improve drinking water and sanitation in rural and small communities and on-site technical assistance initiatives are the most effective environmental protection efforts for drinking water and wastewater, ground water, source water, and compliance with the Clean and Safe Drinking Water Acts. Many small systems face unique challenges in providing reliable drinking water and wastewater services that meet federal and state regulations, including a lack of financial resources, aging infrastructure, and high staff turnover. The onsite technical assistance we provide helps small and rural communities build the technical, managerial and financial capacity necessary to effectively operate drinking water and wastewater systems to comply with regulations, improve operations and management practices, promote system sustainability predominantly through funding access, and better protect public health and the environment. We believe this assistance is most effective when it comes from a trusted individual who is willing to travel directly to the community, has technical expertise to remedy the specific issue with existing treatment and infrastructure, and can be available on-site at any time. Even when considering the technological advances we deploy today, having staff work directly at a physical location, in our experience, is required to provide the adequate level of services necessary to address this issue. The NRWA and its State Associations are comprised of expert field staff that have previous experience operating rural systems. Because we understand the challenges, nuances, and the impact each decision will have on the water system, we are well equipped to lead this effort.

Lastly, any solution must include shared responsibility between the federal government, water systems, consultants and the manufacturers of SCADA and software that impacts cybersecurity. Small systems pay for SCADA systems and are too often installed with a simple password that would not meet minimum security requirements and comes with operating manuals that are complex and difficult to digest and understand. Vendors benefiting from these federal funds must ensure adequate training is available and provide a substantial level of assistance during onboarding.

NRWA prides itself on being a solutions-based organization. We don’t just complain about a problem or make excuses, we are forward thinking, innovative and look to meet our challenges head on. I would now like to discuss a few things our association is doing that are easy to implement and will prepare our members to be more cybersecurity minded, technically efficient and prepared to keep our systems secure and our water safe.

Voluntary Actions by NRWA to Address Cybersecurity

Partnering With Federal Agencies

NRWA has taken several steps to collaborate with our federal partners. We have invited experts in this field to speak at our conferences and provide opportunities for our staff and members to interface with EPA and CISA partners at our annual training events. As an example, at our annual WaterPro Conference this past September, CISA and EPA lead cybersecurity workshops which highlighted their tools and solutions for our members to see. Additionally, a roundtable discussion was held with senior staff from CISA and EPA's Office of Water around cybersecurity. At our annual In-Service training last June, both agencies provided training to our Circuit Riders, providing not only awareness but solutions these professionals can use when visiting water systems with cybersecurity vulnerabilities across the country.

NRWA has endorsed and actively participated in the rollout of EPA's Water Cybersecurity Assessment Tool Kit (WCAT). This kit helps water systems self-assess their cybersecurity practices. State Primacy Agencies and TA Providers can also use this tool when conducting a cybersecurity assessment at water systems. The tool utilizes EPA's Cybersecurity Checklist, which contains the basic cybersecurity controls needed to build a strong, resilient cybersecurity program. In most cases, basic controls and knowledge will assist a system in reducing vulnerabilities. With accompanying Cybersecurity Checklist Fact Sheets, for each of the 33 questions on the WCAT, utilities can learn additional details on each cybersecurity control including why it's important, recommendations and implementation tips. NRWA participated in two tool kit training events designed for our Circuit Riders. Our Circuit Riders work directly with small systems throughout the country and this self-assessment can be very valuable in determining vulnerabilities and improvements that can easily be made.

NRWA has also promoted EPA's Cybersecurity Technical Assistance Program for the Water Sector. Primacy agencies, TA Providers, and utilities can submit cybersecurity questions and receive one-on-one assistance remotely from a cybersecurity subject-matter expert. These experts are contractors who keep these conversations confidential and do not share them with EPA.

The Water Sector Coordinating Council and NRWA have encouraged water systems to use CISA's no-cost vulnerability scanning service. CISA's vulnerability scanning can help utilities identify and address cybersecurity weaknesses that an attacker could use to impact the system. These are just a few of the initiatives NRWA has helped our federal partners deploy, and we stand ready to endorse good ideas and services into the future.

Cyber Readiness Institute Pilot Program

In partnership with the Center on Cyber and Technology Innovation and Microsoft, the Cyber Readiness Institute (CRI) has launched a pilot initiative, called the "Phased Critical Infrastructure Pilot: Resiliency for Water Utilities." This program is providing coach-supported training and resources focused on improving cybersecurity risk management and the ability to respond and recover from a cybersecurity incident. The pilot is for water and wastewater utilities serving between 500 and 10,000 customers.

The program is based on CRI's Cyber Readiness Program which is designed to be clear and accessible for organizations regardless of size and technical expertise. The program focuses on human behavior, helping a designated Cyber Leader develop and implement cyber readiness policies throughout the organization. The program only requires about an hour per week for six weeks and very minimal technical expertise. Participants proceed at their own pace, with the help of a coach to work through implementing organization-wide training and policies for strong passwords, multi-factor authentication, patch management, anti-phishing, business continuity, and other core cyber readiness topics.

At the conclusion of the training, each student completes a playbook. The playbook is comprised of a template for Cyber Leaders to document their core four policies, a software update management tool, a prioritization worksheet, incident response plan template, and a training attestation sheet for the Cyber Leader and head of the organization to sign. The playbook also has training email templates for each of the core four policies, additional training materials, and helpful links. Once the playbook is complete, the coach presents the participant with a certificate.

Although this pilot is in its early stages, there is already promising feedback coming from the participants. At the conclusion of the pilot, NRWA will work with CRI to review the results to determine if any sector specific additions or changes should be made. This program has the potential to be a small system standard and a low-cost solution to ensure all systems are accountable for cybersecurity.

Water ISAC Membership

The U.S. water and wastewater sector's leading national associations and research foundations established the Water Information Sharing and Analysis Center (WaterISAC) in 2002, in coordination with the U.S. Environmental Protection Agency. WaterISAC is the only all-threats security information source for the water and wastewater sector. In addition to security updates and information, the WaterISAC provides training and opportunities for the water sector to collaborate and find solutions to our most complicated cybersecurity challenges.

Since its inception, the WaterISAC has been cost prohibitive for many small and rural systems. Managing small budgets, prioritizing requirements while trying to maintain affordable rates for system customers has kept membership out of reach. However, today I am proud to tell you about a partnership we are finalizing. The WaterISAC has agreed to partner with NRWA and provide NRWA's member systems serving less than 3,300 people a full membership for one flat fee. NRWA is paying that fee for the benefit of these small communities out of non-federal funds. This is a game changer for our small and rural systems and a testament to the successes we can achieve when the sector operates together. I want to thank the Association of Metropolitan Water Agencies (AMWA) and the WaterISAC for their generosity and partnership, I am excited to see the positive results to come.

Working to implement our federal partners programs, the Cyber Readiness Institute Pilot Program and the WaterISAC membership agreement are just a few examples of what NRWA is doing to address our cybersecurity vulnerabilities. Unlike many of the large systems around the country, our systems require a scalable, affordable, and easy to operate solution. We cannot take a one size fits all approach to cybersecurity, and we will continue to be forward thinking, deliberate and ready to ensure each of our systems are secure.

In summary, NRWA is an active participant in the cybersecurity space. We are not sitting on the sidelines or waiting for something to happen. We are doing the work. Although technology and cybersecurity are concepts many of us did not grow up with, rural water operators understand that times change and that we have a responsibility for providing safe, clean, and affordable drinking water and wastewater services. We ask EPA not to overregulate but listen to our concerns and ideas. We stand ready to continue providing cutting edge and industry leading TA as we work to implement cybersecurity solutions. Lastly, we are looking at several solutions that can be tailored to the needs of small and rural systems. Although there are many challenges, NRWA is prepared and will continue to work tirelessly towards improving the quality of life for rural America. Thank you for the opportunity to participate today and I stand ready to take any questions that you may have at this time.