Written Testimony of Nicole Tisdale

Founder and Principal, Advocacy Blueprints, LLC

Before the

U.S. House Committee on Science, Space, and Technology

Subcommittee on Environment

Research-Driven Resilience: Applying Science to Secure U.S. Water Systems from Cyber Threats

May 21, 2026

2318 Rayburn House Office Building

Table of Contents

I. Introduction

Chairman Franklin, Ranking Member Amo, and Members of the Subcommittee, thank you for the opportunity to testify today. I appear in my individual capacity as Founder and Principal of Advocacy Blueprints, LLC.

I grew up in Nettleton, Mississippi — about 2,000 people, twenty miles south of Tupelo. Tupelo was the first city in America to receive electricity from the Tennessee Valley Authority, in 1934. The lights came on in towns like Nettleton and Tupelo because of what the federal government started in this Congress. No private company prioritized the electricity needs and wired up rural Northeast Mississippi on its own. The federal government decided that rural America was worth investing in — and once it did, the model worked so well it became the blueprint for rural electrification nationwide. Almost a century later, we are asking that same question about cybersecurity.

Every federal cybersecurity decision Congress makes answers one question: *whose security are we actually protecting?* When the answer defaults to the communities with the most resources, the most expertise, and the loudest voices, we leave the rest of the country exposed. That is the part of the country adversaries are now exploiting, one rural water system at a time.

Before I lay out the threat picture, the Subcommittee should know who we are talking about when we talk about "rural water systems." There are roughly 50,000 community water systems across the United States. More than 91 percent of them serve fewer than 10,000 people. More than 81 percent serve fewer than 3,300. That is who keeps the water running in most of America. They do it under the same Safe Drinking Water Act and Clean Water Act obligations as the largest utilities in the country, with a fraction of the economies of scale and almost none of the technical bench. That reality is the starting point for everything else I will say today.

I am not a water engineer or a cybersecurity researcher. I'm a congressional expert. For seventeen years — on the House Homeland Security Committee, at the White House National Security Council, and now in my own practice — I've worked to make Congress more effective at protecting Americans from the threats my colleagues at this table study.

A hearing like this one has to do two things at once. It has to sound the fire alarm — describe the threats, lay out what the research is finding, give the Subcommittee the picture clearly enough that you can act on it. It also has to send the firetruck — translate that picture into the federal programs, authorities, and resources that actually reach the communities under threat. The witnesses sitting with me will help you with the alarm. My job today is to make sure the firetruck gets to the people who need help right now.

II. The Threat Landscape

A. What the Intelligence Community and the White House Have Already Told Us

The Office of the Director of National Intelligence's *2025 Annual Threat Assessment* states plainly that “U.S. water infrastructure has become a more common target” for both domestic and foreign adversaries. That assessment reflects the consensus judgment of the entire Intelligence Community.[1]

The *2026 National Cyber Strategy* identifies water utilities by name among the critical infrastructure sectors that must be hardened — and frames the threat in terms ordinary Americans recognize. The Strategy notes that adversaries and cybercriminals "disrupt critical services like healthcare, banking, food supply, and water treatment."[2]

The Intelligence Community and two consecutive White Houses are aligned on this. The Subcommittee can act on settled ground.

B. Who Is Targeting U.S. Water Systems, and Why

Four categories of actors are reaching into American water systems today. Each has a different objective. Each requires a different federal response. And each has already left a mark on a real American community.

Before walking through them, I want to offer the Subcommittee an analytical judgment from my work at the White House National Security Council, on the House Homeland Security Committee, and consulting with the private sector operators and companies that is essential to understanding this threat: **the chaos and public insecurity these attacks create is not a side effect. It is the strategic objective.**

When a town of 5,500 people in Texas cannot trust its tap water, that fact travels. It travels to other Americans, who lose confidence in their government's ability to protect everyday life. It travels to adversaries' domestic audiences, who see the United States as vulnerable. It travels to allies, who calculate accordingly. State-affiliated actors understand this — and cybercriminals, whether they intend to or not, serve exactly the same destabilizing function. Under-resourced rural utilities are not collateral damage in someone else's cyber war. They are the targets.

- **The People's Republic of China — Volt Typhoon.** This is the most sophisticated and persistent threat. The PRC's strategy is not to disrupt today; it is to *pre-position* — to quietly gain access to U.S. critical infrastructure now so they have leverage during a future crisis, particularly any conflict in the Indo-Pacific. U.S. agencies have confirmed Volt Typhoon as a nation-state actor pre-positioning for disruptive or destructive attacks in the event of a crisis.[3] In **Littleton, Massachusetts** (fewer than 10,500 residents), Volt Typhoon compromised the local water facility and remained undetected for at least nine months, potentially accessing systems tied to water treatment plants, wells, an electrical substation, operational technology, and network security devices.[4] This is what pre-positioning looks like. The PRC was not trying to break Littleton's water. They were establishing the option to break it later.
- **Russia — Sandworm.** Russian operations are more aggressive and overt, mirroring tactics Russian intelligence services have used against Ukraine. Sandworm, linked by Mandiant to Russian state actors, does not pre-position quietly. It disrupts visibly.[5] In **Muleshoe, Texas** (fewer than 5,500 residents), in January 2024, Russian-linked actors caused water tank overflows. Similar incidents were reported in two nearby towns at the same time.[6] This is what disruption looks like, and the message it sent — to Muleshoe's neighbors, to other small American cities, and to anyone watching from abroad — was the entire point.
- **Iran-linked actors — CyberAv3ngers.** Iranian operations blend state-backed actors with proxy hacktivists and frequently target systems tied to public health and safety, often as retaliation for geopolitical events far from the affected community.[7] In **Aliquippa, Pennsylvania** (fewer than 9,500 residents), in November 2023, Iranian-linked hackers compromised the Municipal Water Authority by exploiting a specific brand of programmable logic controller used at the plant. The intrusion triggered an alarm and shut the affected system off.[8] A town in western Pennsylvania became a proxy target in a geopolitical dispute thousands of miles away — because of the equipment in its water plant.
- **Cybercriminals.** Ransomware crews — many of them tolerated, sheltered, or quietly enabled by adversary states — make money by holding American infrastructure, like water, energy, healthcare, and businesses, hostage. Rural water utilities are particularly attractive targets because they are under-resourced by design. They cannot afford the security tools that make ransomware attacks difficult, and they cannot sustain prolonged outages, which makes them more likely to pay.[9] In **Arkansas City, Kansas** (fewer than 12,000 residents), in September 2024, a cybersecurity incident forced the utility to switch to manual controls.[10] No nation-state attribution. The chaos still served the same purpose. And six weeks before this hearing, ransomware hit the water treatment plant in **Minot, North Dakota** (approximately 47,000 residents). The water itself was not compromised, but staff had to operate

manually for several hours. The FBI is investigating.[11] This is the most recent incident in a pattern that is accelerating.

C. Why This Is Not Just a Small-Town Problem

When a small rural water system fails, the consequences do not stay local.

- **Military readiness.** More than 400 military installations across the United States rely on civilian water systems — many of them rural — for potable water, firefighting, and waste treatment.[12] In 2017, Hurricane Irma damaged a bridge in Cape Canaveral, Florida — a town of fewer than 10,000 — that carried the sole water main to Patrick Air Force Base. Had the bridge collapsed, the base would have been without water indefinitely.[13] What a hurricane can do by accident, an adversary can do on purpose. Compromising one rural utility can take a military mission offline.
- **The digital economy.** More than 4,000 U.S. data centers depend on local water for cooling, with the highest concentrations in the rural Mid-Atlantic, Southeast, and Midwest.[14] A water attack is a data center attack is a national digital-economy attack.
- **The food supply.** Rural water serves food processing facilities, livestock operations, and irrigation. An attack on a small-town utility ripples into the food supply nationally, affecting prices, availability, and confidence well beyond the affected community.
- **Public health and civil defense.** When water fails, firefighting, emergency medical services, hospitals, and basic sanitation all degrade. Unlike larger urban systems with redundancy, most rural systems operate single points of failure: one treatment plant, one operator, one set of controls. A 2024 EPA survey, documented in the EPA Office of Inspector General's November 2024 management implication report, found that 97 drinking water systems serving 26 million Americans had critical or high-risk cybersecurity vulnerabilities.[15]

Rural water systems are not small targets. They are small *systems* with large national consequences when they fail. Our adversaries already understand this.

III. Why the Threat Lands Hardest on Small Systems

The threat is real. The architecture is not catching it. To understand why, the Subcommittee needs three things: a clear lens for thinking about who is exposed, an honest look at the workforce reality inside rural utilities, and a candid account of how current federal programs are failing the communities they were designed to help.

A. The Cyber Poverty Line

In 2013, the cybersecurity expert Wendy Nather introduced a concept called the *Cyber Poverty Line*.[16] The idea is simple, and it is one of the most useful tools we have for talking about who is — and is not — actually being protected by federal cyber policy.

The same way an economic poverty line tells policymakers who cannot afford basic needs, the Cyber Poverty Line tells us who cannot afford basic cybersecurity protections. Four resource gaps define it: insufficient funding for security tools, a lack of in-house cybersecurity expertise, outdated technology that cannot support modern defenses, and limited influence to attract outside help from federal agencies, private vendors, or nonprofits.

In rural communities, all four gaps are sharper. Cybersecurity tools cost three to five times more per person in small communities than in large ones, because rural systems cannot achieve the volume that drives down per-unit pricing.[17] Rural cybersecurity roles take roughly 70 percent longer to fill than other IT positions.[18] Cybersecurity professionals, almost without exception, do not relocate to small towns. The harsh reality is that the talent has to be built from within, or it does not exist.

The framing this Subcommittee should take from the Cyber Poverty Line is that rural communities are not behind on cyber; they are underserved by infrastructure and public policy. That distinction matters because it determines what kind of federal response is appropriate. If you assume rural communities are behind, you build programs that ask them to catch up. If you understand they are underserved, you build programs that meet them where they are.

B. The Workforce Problem Is the Security Problem

The single most important point this Subcommittee can understand about rural water cybersecurity is that the workforce problem and the security problem are the same problem.

In most rural water systems, the operator who runs the treatment plant also drives the truck, reads the meters, and answers the phone. There is no IT department. There is no cybersecurity team. There is one person — sometimes with a part-time helper — running a system that serves the entire community. Asking that operator to become a cybersecurity expert on top of everything else is not realistic, and any federal program that assumes otherwise will fail in the field.

That is not a future problem. It is a present one, and it is about to get worse. Fifty-seven percent of rural water operators plan to retire within ten years; nearly one-third within five.[19] This is the largest knowledge drain the sector has ever faced — and it is happening at exactly the moment when adversaries have decided that rural water is a target worth attacking.

The National Rural Water Association calls the workforce crisis a *Five-Front Battle*: insufficient pay, an aging workforce, a shrinking talent pool, regulatory burdens, and financial strain.[20] These pressures are not independent — they compound. They produce exactly the conditions adversaries exploit: small staffs, deferred upgrades, unpatched systems, and no slack in the day for anyone to think about cybersecurity.

For this Subcommittee's R&D jurisdiction specifically, the workforce reality has one urgent implication: research and tools developed without rural operator input fail in the field. A toolkit that assumes high-speed broadband, dedicated IT staff, and 24/7 monitoring will not protect a system run by one person and a part-time helper. The lab-to-operator gap is the security gap. Federal R&D investment that does not close this gap produces innovations no one in rural America can deploy.

The good news is that part of the federal toolkit for this already exists. NIST, the same federal standards body the Subcommittee works with on environmental measurement, also maintains the NICE Workforce Framework for Cybersecurity. It gives utilities a common federal vocabulary for describing the security work that needs to get done at a water plant, even when that work is shared across one operator, a part-time helper, and a contracted vendor.[21] For a small rural utility, that vocabulary is useful in three concrete ways: it helps describe what a utility needs when applying for federal funding, it gives the utility clear language to hold its vendors accountable, and it gives federal agencies a shared way to measure whether their assistance is reaching the field. The NICE Workforce Framework exists. What rural utilities need is the federal support to actually use it.

C. Three Structural Ways Federal Programs Are Failing Rural Water

Three current federal programs illustrate the design problem. I raise them not to criticize the people running them. The civil servants at EPA, USDA, CISA, and DHS who work on water security are doing serious and amazing work — often with limited authority, fragmented funding, and competing demands on their time. They are not the problem. The problem is that the *program designs* — the rules, the application processes, the funding mechanisms Congress wrote into law — exclude the very communities those programs were meant to help. That is something only Congress can fix.

1. The State and Local Cybersecurity Grant Program (SLCGP) is landmark legislation that excludes by design.

   I helped build SLCGP at the White House, and I am telling this Subcommittee candidly that it falls short for rural water. Water competes against transportation, health, education, and other state priorities for the same funding. The match-first, reimburse-later funding model assumes cash flow rural utilities do not have. The competitive application process favors communities with professional grant writers and dedicated cybersecurity staff — exactly the resources rural towns lack.[22]

2. EPA has the regulatory authority but no cyber R&D-to-deployment pipeline.

   The Clean Water Act and Safe Drinking Water Act create compliance burdens without corresponding cybersecurity assistance. EPA's State Revolving Funds operate as state-administered loans, not grants — with terms running up to 40 years. That structure may make sense for replacing pipes. It does not match the urgency of a cyber threat that is active right now.[23]

3. The federal government has a proven cyber leadership model in the Department of Energy — and is not replicating it for water.

   DOE's Office of Cybersecurity, Energy Security, and Emergency Response receives roughly $200 million annually for sector-specific cyber coordination, with dedicated research, technical assistance, and emergency response capabilities for the energy sector.[24] Water cybersecurity investment, by contrast, is fragmented across EPA, USDA, CISA, and FEMA — with no agency owning the mission. The energy-water nexus makes this incoherent on its face: thermoelectric cooling accounts for roughly 38 percent of U.S. freshwater withdrawals.[25] You cannot protect the energy grid without protecting the water that cools it.

These three failures share a single root cause. Each program was designed for an environment that does not exist in rural America — an environment with dedicated staff, cash on-hand, and the administrative capacity to navigate federal complexity. The fix is not more money for the same program designs. The fix is program designs that reflect rural reality from the start. That is what the framework in the next section provides.

IV. A Framework for Federal Action

I want to offer the Subcommittee a policy framework I developed at Advocacy Blueprints, LLC to address exactly this design problem. It is called the *Inclusive Cyber Policy Framework*, and it gives federal policymakers a design lens for cybersecurity programs — a set of seven principles for evaluating whether a program will actually reach the communities it is meant to protect, or whether it will exclude them by design.[26] Six of those principles map directly to the questions before this Subcommittee.

Principle 1 — Equal Access to Secure Digital Technologies.

Rural water systems should have access to the same protections urban systems do. That means affordable tools, built for the operational realities of small utilities, and federal infrastructure investment that does not stop at the metropolitan edge. It also means broadband. The threat picture is accelerating: AI is making it cheaper and faster for adversaries to identify vulnerabilities, automate intrusions, and exploit weaknesses at scale. Defenders need the same speed to keep up. But many rural utilities still do not have the broadband connectivity to run modern cybersecurity tools, receive timely threat alerts, or push security patches.

The federal response has to deliver on two fronts at once. In communities that still lack reliable broadband, the federal government has to close that gap before any cyber tool will work. And in the

communities that do have connectivity, federal R&D has to produce practical, AI-enabled cybersecurity tools designed for utilities run by one operator and a part-time helper. Access is the precondition for everything else this framework asks the federal government to do.

Principle 3 — Proportionate Protection from Cyber Threats.

Federal resources should scale to risk and need, not to the administrative capacity of the applicant. When a grant program rewards the communities best at writing grants, it inverts the protection it was meant to provide. Small systems are supporting our global supply chains, military installations, food processing facilities, and data centers. Federal protection has to follow the risk, not the resumes of the people applying for it. A funding mechanism that systematically excludes the highest-risk utilities is not a funding mechanism. It is a sorting mechanism.

Principle 4 — Equitable Representation in Cybersecurity Decision-Making.

The people most affected by cyber policy decisions are too often the furthest from the table when those decisions are made. Rural operators belong in the room when federal R&D priorities are set. So do the students and early career professionals who will become the next generation of cyber policy leaders — particularly those from rural and historically underrepresented communities and academic institutions. Through the Cyber Policy Leadership Institute, a program I co-founded, we have spent the last two years building exactly that pipeline, bringing students from rural community colleges and Minority-Serving Institutions into cyber policy careers. The talent exists. The pipeline is what has been missing.[27]

Principle 5 — Balanced Cybersecurity Benefits and Risks.

Federal cyber policy should not shift burdens onto already-stretched small utilities. Compliance mandates without corresponding assistance, and reimbursement-first funding models, do exactly that. They look like accountability on paper. In practice, they push security risk *onto* the communities least equipped to absorb it.

Principle 6 — People-Centered Cybersecurity Research.

This is the principle most directly relevant to this Subcommittee's R&D jurisdiction. Federal cybersecurity research should center the *impacts* of cyberattacks on communities — service and administrative days lost, public health outcomes, downstream agricultural and military effects — not just the techniques adversaries use. Research that measures only adversary behavior tells us what the threat looks like. Research that measures community impact tells us whether the federal response is actually working.

Principle 7 — Breaking Down Policy Silos for Holistic Solutions.

Water cybersecurity sits across EPA, USDA, CISA, DOE, DOD, and DHS. None of those agencies owns the mission. That is a coordination problem, and it is also a deployment problem because every gap between agencies is a gap an adversary can exploit.

This framework is what tells you whether a federal program will actually reach a town like Nettleton or whether it will be one more well-intentioned policy that looks good on paper and does not work in the field. The recommendations in the next section apply it directly.

V. Recommendations for Congress

I offer eight recommendations — four within the direct jurisdiction of this Subcommittee, and four that this Subcommittee can champion across other committees of jurisdiction.

Within the Science, Space, and Technology Committee's Jurisdiction

Recommendation 1. Adopt the Inclusive Cyber Policy Framework — particularly Principle 6, People-Centered Research — as a federal design principle for water-sector cybersecurity R&D.

The Ask: Direct EPA, the National Science Foundation, and the National Institute of Standards and Technology to measure the community-level impact of cyber incidents on water systems — not just adversary techniques. That measurement should include both operational and administrative impacts: service days lost and water quality degradation on the operational side, and on the administrative side, billing system disruptions, customer data breaches, ransomware payments diverted from infrastructure investment, and the cost of recovery and reporting. Cyberattacks reach utilities through both doors. Federal research should be measuring both.

The Problem It Solves: Federal cyber R&D today is overwhelmingly adversary-focused. It tells us what threats look like. It does not tell us whether the federal response is actually reaching the communities under threat. Without community-level impact data, covering both how an attack disrupts operations and how it disrupts administration, Congress cannot evaluate whether its investments are working.

Why It Works: This is a directional change, not a new spending program. It can be implemented through committee report language, agency guidance, and existing R&D authorizations and appropriations. It costs almost nothing and changes everything about how the federal government measures success.

Recommendation 2. Direct and fund federal water cybersecurity R&D to be informed by CIRCIA incident data.

The Ask: Direct EPA, NSF, and NIST to use anonymized water-sector incident data collected under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) as a research input for setting federal R&D priorities.

The Problem It Solves: When I helped pass CIRCIA at the White House, the law was designed to capture what is actually happening to American infrastructure — not what we think might happen.[28] The data is being collected. It is not yet shaping R&D. That gap means federal research is driven by threat intelligence about adversary tradecraft, but not by the real incident record of the utilities under attack.

Why It Works: The data exists. The legal authority exists. The implementation gap is directional, and this Subcommittee can close it through report language.

Recommendation 3. Direct and fund EPA environmental R&D programs to develop AI-enabled cybersecurity tools designed for single-operator rural utilities.

The Ask: Prioritize R&D funding for tools that translate cyber alerts into operator-actionable steps; tools that do not assume dedicated IT staff; tools that work on rural broadband.

The Problem It Solves: Rural water utilities cannot hire their way out of the cybersecurity workforce shortage. There are not enough cybersecurity professionals in the country to staff every small utility, and even if there were, they would not relocate to towns of 2,000 people. The only realistic path is to give the operators who already run these systems tools that augment their capacity — so they do not have to become cybersecurity experts to keep their systems safe.

Why It Works: This is exactly the kind of applied R&D this Subcommittee's jurisdiction was designed to drive. It directs federal research toward the deployment environment that actually exists, rather than idealized environments that small utilities cannot match.

Recommendation 4. Establish and fund a Rural Water and Wastewater Cybersecurity Circuit Rider Program.

The Ask: Authorize $25 million annually over the next five fiscal years to establish a cyber-specific circuit rider program, modeled on USDA's 50-year-proven Rural Water Circuit Rider program.[29]

The Problem It Solves: Rural water utilities face sophisticated nation-state cyber threats with no in-house cybersecurity expertise. Generic federal training programs assume a level of personnel and infrastructure most rural systems do not have. What works in rural America is embedded, trusted, on-site technical assistance from experts who understand rural operational realities. The Circuit Rider model has delivered exactly that for water operations for half a century. Cybersecurity is the gap.

Why It Works: The model is proven. The trusted relationships already exist. The Subcommittee should consider carefully where to place the cyber-specific program — USDA has the relationships and the delivery infrastructure; EPA has the sector authority and falls within this Committee's jurisdiction. A coordinated approach across both agencies, designed deliberately rather than as a turf accommodation, is the right structure.

Recommendations the Subcommittee Can Champion Across Other Committees

Recommendation 5. Elevate cyber policy leadership at Sector Risk Management Agencies to a Senate-confirmed, Assistant Secretary-level position.

The Ask: Direct non-national-security agencies that serve as Sector Risk Management Agencies — particularly EPA and USDA — to establish a Senate-confirmed cyber policy lead at the Assistant Secretary level.

The Problem It Solves: Today, the people making cybersecurity budget and policy decisions at EPA, USDA, and similar agencies are career civil servants. They are skilled and committed; however, they do not have political appointee authority, and they are not at a rank that allows them to make policy decisions in cross-agency conversations with CISA, ODNI, and the NSC. As cyber threats to water, agriculture, and other non-traditional national security sectors grow, the Sector Risk Management Agencies need a cyber policy lead with the standing to be in those rooms.

Why It Works: This is a structural fix that aligns the cyber policy chain of command with how cyber threats actually cross agency boundaries. It does not require new spending. It requires Congress to recognize that water, agriculture, and similar sectors are now national security infrastructure — and to staff the federal response accordingly. *(Jurisdiction of the authorization committees for each affected agency.)*

Recommendation 6. Reform the State and Local Cybersecurity Grant Program to fix exclusion-by-design.

The Ask: Reauthorize SLCGP before the current extension expires, with three changes: a 10 percent dedicated allocation for rural water and wastewater systems; elimination of the "match-first, reimburse-later" requirement for systems serving fewer than 10,000 people; and simplified application procedures that do not require professional grant-writing capacity.[30]

The Problem It Solves: SLCGP currently excludes the communities most exposed to cyber risk. Water competes against transportation, health, and education for the same pot. Cash-strapped utilities cannot front project costs. Competitive applications favor towns with grant writers. Each of those design choices was made for understandable reasons. Together, they exclude rural America.

Why It Works: These are surgical fixes to an existing program. They do not require a new authorization or a new agency. They require Congress to look honestly at what SLCGP is producing in the field and adjust accordingly. *(House Homeland Security Committee jurisdiction.)*

Recommendation 7. Direct ODNI to produce an Annual Water Threat Assessment.

The Ask: Direct the Office of the Director of National Intelligence to produce an annual, water-specific threat assessment — with rural-system-specific analysis and identification of which rural utilities directly support the Defense Industrial Base.[31]

The Problem It Solves: The 2025 Annual Threat Assessment acknowledges water as a growing target but lacks the sector-specific depth needed to drive resource allocation and early warning. Most rural utilities that support military missions do not know they support military missions — which means they are not accessing the DOD-tier cyber resources they would qualify for under Defense Industrial Base membership.

Why It Works: This builds on existing intelligence community infrastructure. It does not require new collection authorities. It requires a directed analytical focus on a sector that has been underrepresented in IC reporting relative to its national security importance. *(House Intelligence Committee jurisdiction.)*

Recommendation 8. Establish a Coordinated Federal Rural Water and Wastewater Security Strategy.

The Ask: Require EPA, USDA, CISA, DOE, DOD, and ODNI to coordinate a single federal rural water security strategy, modeled on the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

The Problem It Solves: Currently, responsibility for rural water cybersecurity is fragmented across at least six federal agencies, none of which owns the mission. The result is duplicated reporting requirements for utilities, inconsistent technical assistance, and gaps that adversaries exploit. DOE solved this exact problem for the energy sector with CESER, which receives roughly $200 million annually and provides comprehensive sector-specific cyber leadership. Water has no equivalent.

Why It Works: The model exists and is operating successfully at DOE. The energy-water nexus — thermoelectric cooling accounts for roughly 38 percent of U.S. freshwater withdrawals — makes the disparity strategically incoherent.[32] *(House Committees on Energy & Commerce, Homeland Security, and Agriculture.)*

I recognize this is a substantial slate of recommendations. Each deliberate recommendation is grounded in a federal program model with a demonstrated track record in another sector or another context. They require Congress to extend what is already working to the rural communities current federal programs do not yet reach.

VI. Conclusion

A bipartisan through-line runs from the 2023 National Cybersecurity Strategy[33] to the 2025 Annual Threat Assessment to the 2026 National Cyber Strategy: America's national security depends on all water systems and the federal government must help to defend them. That consistency, across two administrations and both parties, is a sign of bipartisan stability all Americans need to know still exists.

Closing where I started: There are thousands of small water facilities across every state represented in this room. The federal government decided almost a century ago that rural communities were worth investing in and protecting. We are better as a country because of that decision. We should do it again and protect rural water.

Thank you for your time and focus on this important issue.

VII. Endnotes

1. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, March 2025), 8, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

2. The White House, *President Trump's Cyber Strategy for America* (Washington, DC: The White House, March 2026), 3, 5, https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

3. National Rural Water Association and Nicole Tisdale, *Rural Water's Ripple Effect: National Security, Cyber Threats, and the Future of Water* (Duncan, OK: NRWA, November 24, 2025), https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2026/03/nrwa-policy-paper-rural-water-s-ripple-effect-national-security-cyber-threats-and-the-future-of-water-final-2026.ZbfXJ2BywJ.pdf. The author served NRWA as a national security and cybersecurity policy consultant.

4. NRWA and Tisdale, *Rural Water's Ripple Effect*, 3.

5. NRWA and Tisdale, *Rural Water's Ripple Effect*, 3.

6. NRWA and Tisdale, *Rural Water's Ripple Effect*, 3–4.

7. NRWA and Tisdale, *Rural Water's Ripple Effect*, 3.

8. NRWA and Tisdale, *Rural Water's Ripple Effect*, 3.

9. NRWA and Tisdale, *Rural Water's Ripple Effect*, 3.

10. NRWA and Tisdale, *Rural Water's Ripple Effect*, 4.

11. Kyona Rivera, "FBI releases statement on ransomware attack of Minot's water treatment plant," KFYR-TV, April 3, 2026, https://www.kfyrtv.com.

12. NRWA and Tisdale, *Rural Water's Ripple Effect*, 4–5.

13. NRWA and Tisdale, *Rural Water's Ripple Effect*, 4.

14. NRWA and Tisdale, *Rural Water's Ripple Effect*, 6.

15. U.S. Environmental Protection Agency, Office of Inspector General, *Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems*, Report No. 25-N-0004 (Washington, DC: EPA OIG, November 13, 2024), https://www.epaoig.gov/sites/default/files/reports/2024-11/full_report_-_25-n-0004t_1.pdf. Cited in NRWA and Tisdale, *Rural Water's Ripple Effect*, 3.

16. Wendy Nather originated the concept of the "Cyber Poverty Line" in 2013. The term is publicly cited in Nicole Tisdale, "Small Towns, Big Targets: Rethinking Cybersecurity Policy for Rural Communities," *Aspen Digital*, 2025, https://www.aspendigital.org/blog/cyber-poverty-line/. The blog was developed in partnership with craig newmark philanthropies' Cyber Civil Defense Network.

17. Tisdale, "Small Towns, Big Targets."

18. Tisdale, "Small Towns, Big Targets."

19. NRWA and Tisdale, *Rural Water's Ripple Effect*, 7.

20. NRWA and Tisdale, *Rural Water's Ripple Effect*, 7–11.

21. National Institute of Standards and Technology, "NICE Framework: Current Versions," National Institute of Standards and Technology (accessed May 18, 2026). https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions

22. NRWA and Tisdale, *Rural Water's Ripple Effect*, 13–14, 22.

23. NRWA and Tisdale, *Rural Water's Ripple Effect*, 14.

24. NRWA and Tisdale, *Rural Water's Ripple Effect*, 16.

25. NRWA and Tisdale, *Rural Water's Ripple Effect*, 16. CRS R43199 cited therein.

26. Advocacy Blueprints, LLC, *Inclusive Cyber Policy Framework* (Washington, DC: Advocacy Blueprints, LLC, 2025), https://advocacyblueprints.com/rural-cyber-workforce. Developed with support from Microsoft's Academic Engagement initiative.

27. The Cyber Policy Leadership Institute (CPLI) was developed and funded by CrowdStrike, in partnership with Advocacy Blueprints, LLC and POPVOX Foundation. See *Cyber Policy Leadership Institute: Inaugural Cohort (Spring 2024) Final Report* and *Cyber Policy Leadership Institute: Spring 2025 Cohort Final Report* (Washington, DC: Advocacy Blueprints, LLC, 2024 and 2025).

28. Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 49 (2022).

29. NRWA and Tisdale, *Rural Water's Ripple Effect*, 21–22.

30. NRWA and Tisdale, *Rural Water's Ripple Effect*, 22.

31. NRWA and Tisdale, *Rural Water's Ripple Effect*, 20.

32. NRWA and Tisdale, *Rural Water's Ripple Effect*, 16.

33. The White House, *National Cybersecurity Strategy* (Washington, DC: The White House, March 2023), https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Appendix:
Congressional District Rural Water Connection Points

Context

The cybersecurity of America's water systems is often discussed in national terms. It is also a local story. Each Member of this Subcommittee represents communities where rural and small water and wastewater utilities are already partnering with state Rural Water Associations on workforce, infrastructure, and resilience. The information below is intended to make those connections concrete — not to characterize any Member's record, but to point to the work already underway in their districts that bears on the questions before this Subcommittee.

Full Committee Leadership

Chairman Brian Babin (Texas-36) — Southeast Texas

> Texas has one of the largest concentrations of small and rural community water systems in the country, with thousands of utilities serving communities of fewer than 10,000 people. These systems anchor the data centers, military installations, energy infrastructure, and agricultural economy that drive Texas and the nation. The cybersecurity research needs of small Texas systems — from operational technology vulnerabilities to threat intelligence sharing — are central to building the data foundation federal water sector R&D requires.

Ranking Member Zoe Lofgren (California-18) — *Silicon Valley and surrounding agricultural communities*

> California's Central Valley anchors the national agricultural water conversation, and California more broadly illustrates how agricultural, municipal, and technology economies share water infrastructure. The cybersecurity of small agricultural and rural water systems is inseparable from national food security and from the resilience of the technology corridors that depend on the same water sources. Federal coordination across EPA, USDA, CISA, and DOE will be essential to align research, technical assistance, and workforce investments at the scale California's water systems require.

Subcommittee Leadership

Chairman Scott Franklin (Florida-18) — *Central and south-central Florida*

> The Florida Rural Water Association has provided asset management, financial sustainability planning, GIS mapping, and energy audit services to communities across FL-18, including Arcadia, Bartow, Bowling Green, Clewiston, Davenport, Dundee, Eagle Lake, Fort Meade, Frostproof, Hardee County, Lake Alfred, Lake Hamilton, Lake Placid, Mulberry, Spring Lake Improvement District, and Sunrise Utility. The Sun N Lakes Improvement District in the Sebring area recently joined the FRWA Registered Apprenticeship Program, with its first apprentice on path to a licensed journeyman operator credential serving south-central Florida's sensitive environment and growing population.

Ranking Member Gabe Amo (Rhode Island-01) — *Providence and coastal Rhode Island*

The Rhode Island Rural Water Association works with approximately 37 drinking water and wastewater utilities within RI-01, providing accredited training and continuing education for operators across both the rural and urban portions of the district. RIRWA is advancing apprenticeship in partnership with the towns of Cumberland and Lincoln, and has prioritized lead service line resolution work with the Bristol County Water Authority (serving Bristol, Barrington, and Warren) and the Portsmouth Water and Fire District. Statewide, 75 of Rhode Island's 90 community water systems serve fewer than 10,000 people, meaning the workforce and cybersecurity challenges facing small systems are deeply present in Rhode Island's First District.

Subcommittee Members

Rep. Nick Begich (Alaska (At-Large)) — *Statewide, including remote bush communities*

Alaska's water systems include some of the most geographically isolated utilities in the country. Many bush community systems operate without consistent broadband or cellular connectivity, which makes the cybersecurity research and resilience conversation fundamentally different than in the Lower 48. It also underscores why federal research and development must be designed with rural and remote operating conditions in mind from the start. Coast Guard installations and other federal mission sites in Alaska also depend on local water access, illustrating how rural systems anchor national presence even in the most remote parts of the country.

Rep. Suzanne Bonamici (Oregon-01) — *Northwest Oregon, coastal and suburban Portland*

Oregon-01 includes coastal rural communities outside the Portland metropolitan area whose small water and wastewater systems face the same workforce and cybersecurity gaps documented in rural systems nationally. The Pacific Northwest is also a major concentration of data center infrastructure and federal facilities whose continuity depends on the reliability of upstream small systems — a pattern that links coastal Oregon's small utilities to the resilience of the broader regional economy.

Rep. Jeff Hurd (Colorado-03) — *Western and southern Colorado*

The Colorado Rural Water Association works extensively across CO-03 to include many small and remote areas and indigenous tribes. Recent projects include an energy efficiency assessment for Avondale receiving a USDA award on May 20, 2026; an energy efficiency award for Manzanola; a successful financing package for the Ute Mountain Ute Tribe in Towaoc combining USDA Rural Development and EPA funding; and operator certification work with the Center Sanitation District, whose wastewater supervisor was named Operator of the Year at the 2024 state conference. CRWA also hosts an annual conference in Durango. These projects illustrate the federal-state-tribal coordination model that water sector cybersecurity will require to reach the smallest and most remote systems.

Rep. Deborah Ross (NC-02) — *Raleigh and the Research Triangle*

Raleigh Water has graduated two registered apprentices through the North Carolina Rural Water Association's program, even though NC-02 is among the state's most urban districts. This reflects a pattern observed by NCRWA and other state affiliates: workforce development that begins in small and rural communities builds the pipeline that fills shortages in larger systems and major cities. The cybersecurity of small upstream systems is also functionally inseparable

from the public health and economic vitality of growing metropolitan areas like the Research Triangle.

Rep. David Rouzer (NC-07) — *Coastal and southeastern North Carolina*

North Carolina Rural Water Association serves more than 100 water systems across NC-07, spanning Bladen, Brunswick, Columbus, Cumberland, New Hanover, Pender, Robeson, and Sampson Counties. NCRWA Circuit Riders have completed over a dozen local water supply plans and Consumer Confidence Reports in NC-07 this year alone, and the Town of Goldsboro graduated one of NCRWA's seventeen registered apprentices. The North Carolina Department of Environmental Quality has credited Circuit Riders with helping more than 65 percent of the state's 500-plus water systems meet their 2025 planning deadline — a model of the trusted, traveling technical assistance the testimony recommends extending to cybersecurity.

Rep. Matt Van Epps (TN-07) — *Middle Tennessee, rural and outer Nashville suburbs*

Tennessee is served by the Tennessee Association of Utility Districts, one of the oldest and highest-capacity state water associations in the nation. TN-07 reflects a pattern visible across the South: a large rural population whose small water systems are physically and economically interconnected with fast-growing metropolitan infrastructure — data centers, manufacturing corridors, and military installations across Middle Tennessee. The cybersecurity of small utilities in TN-07 is inseparable from the resilience of the regional economy they support.

Themes Across Districts

Workforce is local everywhere.

The National Rural Water Association's Apprenticeship Program (funded by USDA) is producing licensed operators in districts represented at this hearing. These are the people who will run, monitor, and defend water systems for the next generation, in communities of every size.

The Circuit Rider model is already working and is the correct model.

The same trusted, traveling technical assistance model that state Rural Water Associations deploy today to help small systems with planning, energy efficiency, lead service lines, and operator certification is the model the testimony recommends extending to cybersecurity. Members see this work in their districts already. The Cyber Circuit Rider pilots have worked, but they need to be authorized and appropriated in order to sustain and scale.

Urban and suburban districts are not exempt.

Small water systems sit upstream of the data centers, military installations, hospitals, and economic corridors that anchor every Member's district. A successful cyberattack on a small utility does not stay small — it cascades into the public health and economic continuity of the larger communities those systems support.

Federal research must be designed for the operating environments that need it most.

From Alaska's bush communities to Colorado's tribal lands to Rhode Island's small coastal towns, the conditions under which rural and small systems actually operate must shape federal R&D from the start.

Sources. District-specific information in this appendix is drawn from communications with the National Rural Water Association and its state affiliates — the Alaska Rural Water Association, Colorado Rural Water Association, Florida Rural Water Association, North Carolina Rural Water Association, Oregon Association of Water Utilities, Rhode Island Rural Water Association, and Tennessee Association of Utility Districts — during the preparation of this testimony, May 2026, and is cited with NRWA's permission.