

RURAL WATER'S *RIPPLE* EFFECT

*National Security, Cyber Threats,
and the Future of Water*

Nicole Tisdale



NATIONAL
RURAL WATER
ASSOCIATION

America's Largest Utility Membership

2026

Table of Contents

Introduction	2
Threat Landscape	2
Threat Impact	4
Military Base Dependency	4
Global Technology and AI impacts	6
Broader Public Health and Civil Defense Implications	7
The Workforce Crisis	7
The Five Front Battle	8
The Compensation Crisis: More Than Just Low Pay	8
The Aging Workforce: A Ticking Clock for National Security	9
The Shrinking Talent Pool: When Supply Cannot Meet Demand	9
The Skills and Security Gap: What the Numbers Reveal	10
Regulatory Burdens and Financial Strains: When Compliance Diverts Resources from Security	11
Federal Policy Gaps	12
Current Federal Authorities: Strong Foundation, Implementation Gaps	13
State and Local Cybersecurity Grant Program (SLCGP): Landmark Legislation with Rural Challenges	13
Environmental Protection Agency (EPA) Water Infrastructure Authorities: Regulatory Framework Without Cybersecurity Integration	14
United States Department of Agriculture (USDA) Rural Development Authorities: Proven Technical Assistance Model, Cybersecurity Gap	15
Cybersecurity and Infrastructure Security Agency (CISA) Critical Infrastructure Authorities: National Coordination Without Rural Engagement	16
Federal Investment Patterns: Massive Energy Investment, Fragmented Water Support	16
Department of Energy (DOE) Cybersecurity Leadership Model	16
Fragmented Water Cybersecurity Investment	17
Workforce-Cybersecurity Intersection: Compounding Vulnerabilities	17
The Five-Front Battle Creates Cyber Vulnerabilities	17
Rural Systems Need External Cybersecurity Support but Face Multiple Barriers	18
Policy Recommendations	19
A Strategy Built on Proven Success	19
Threat Intelligence Recommendations	20
1. Annual Water Threat Assessment	20
Technical Assistance Recommendations	21
2. Rural Water and Wastewater Cybersecurity Circuit Rider Program	21
3. Rural Water Cybersecurity Set-Aside in State and Local Cybersecurity Grant Program	22
4. Water Industry Workforce Support through Apprenticeship	22
Strategic Coordination Recommendations	23
5. Coordinated Federal Rural Water and Wastewater Security Strategy	23
Conclusion	24

Introduction

America's rural water systems face an unprecedented crisis, extending far beyond individual communities, which threatens our national security, economic resilience, and public health. As sophisticated cyber adversaries at home and abroad intensify their attacks on U.S. water infrastructure, the rural water workforce—the first and last line of defense for millions of Americans—is underfunded, under resourced, and preparing for mass retirement.

This analysis, based on comprehensive survey data from over 10,000 rural water professionals, reveals the stark reality of what we call "the five-front battle." Rural water systems are simultaneously fighting insufficient compensation, an aging workforce, a shrinking talent pool, crushing regulatory burdens, and severe financial constraints. These interconnected pressures create exactly the vulnerabilities that both state-sponsored adversaries and cybercriminals seek to exploit.

The numbers tell a compelling story: 57 percent of rural water workers plan to retire within the next decade, with nearly one-third exiting the field in the next five years alone.¹ These retirements will create an unprecedented knowledge drain from systems that serve millions of Americans and support critical infrastructure such as military bases, data centers, hospitals, schools, emergency services, and food production facilities.

The future of rural water systems is not merely a workforce challenge—it's a national security vulnerability hiding in plain sight. The same systems that keep America's communities operational are fighting for survival just as cyber threats reach unprecedented levels. The convergence of these crises demands immediate federal action based on data-driven solutions and proven models of success.

This paper provides: comprehensive analysis of rural-specific workforce challenges, documentation of cybersecurity threats targeting water infrastructure, assessment of current federal policy gaps, and actionable recommendations for targeted federal investment. Each recommendation leverages existing authorities, builds on successful programs, and meets rural water systems where they are—not where policymakers wish they were.

The window for effective action is narrowing rapidly. We have the data, the stakeholders, and the models needed to address this crisis. What we need now is the federal commitment to act with the urgency our national security requires.

Threat Landscape

Water infrastructure in the United States faces an unprecedented convergence of national security threats across cyber, physical, and supply chain attack surfaces. State-sponsored adversaries, including China, Russia, and Iran, alongside foreign and domestic criminal groups and lone wolf attackers continue to pose an urgent threat to America's water and wastewater resources. Cyber threats range from opportunistic attacks to coordinated, strategic campaigns designed to compromise operational technology, establish persistent access, and position adversaries for potential disruption during geopolitical crises. This elevated threat environment has also raised awareness of potential physical attacks targeting water critical infrastructure, including armed attacks, attacks by vehicles and unmanned aircraft systems, and

explosives, from criminals and malicious insiders. The gravity of the situation is such that threats to water infrastructure were singled out in the Director of National Intelligence's 2025 Annual Threat Assessment, which stated that "U.S. water infrastructure has become a more common target" for domestic and international adversaries.²

A 2024 Environmental Protection Agency (EPA) survey found that 97 drinking water systems in the U.S. serving 26 million Americans had a critical or high-risk vulnerability.³ According to the Water Information Sharing and Analysis Center (WaterISAC), physical threats against water facilities increased 105 percent from 2023 to 2024. These incidents include "threats of contamination and poisoning of water supplies, as well as arson attacks, bombs at water utilities, equipment tampering and numerous sabotage incidents at sewage pump stations, fire hydrants, and wastewater manholes; ballistic attacks against water infrastructure, primarily at water towers; bomb threats; and of drones flying over utilities."⁴ The aging nature of U.S. water infrastructure compounds these vulnerabilities. Many systems were designed at a time when security considerations focused primarily on accidental failures rather than deliberate attacks. Updating legacy water infrastructure with modern IT and OT security requirements presents significant technical and financial challenges, particularly for smaller water utilities with limited resources. Unlike critical infrastructure sectors that are concentrated in specific facilities, water systems necessarily extend across broad areas to serve distributed populations. This geographic spread makes comprehensive physical security extremely challenging and creates numerous vulnerabilities.

The People's Republic of China poses the most sophisticated and persistent cyber threat to U.S. water infrastructure, combining advanced technical capabilities with long-term strategic positioning. The Chinese Communist Party's hybrid warfare strategy blends cyber operations with economic and diplomatic pressure, exemplified by the cyber group "Volt Typhoon," which U.S. agencies have confirmed as a nation-state actor pre-positioning for disruptive or destructive attacks in the event of a crisis. In one case, Volt Typhoon compromised a water facility in Littleton, Massachusetts (<10,500 residents),⁵ remaining undetected for at least nine months and potentially accessing systems tied to water treatment plants, wells, an electrical substation, operational technology, and network security devices.

Russia, by contrast, has taken a more aggressive and overt approach, mirroring tactics used in Ukraine. In January 2024, the Sandworm group—linked by Mandiant to Russian actors—caused tank overflows at a water facility in Muleshoe, Texas (<5,500),⁶ with similar incidents reported in two nearby towns. These operations tend to escalate quickly from network access to direct manipulation of operational technology, signaling both technical capability and psychological intent. Iranian operations present a third distinct profile, often blending state-backed actors with proxy hackers and focusing on systems tied to public health and safety. In 2023, Iranian hackers attacked the Municipal Water Authority of Aliquippa, Pennsylvania (<9,500),⁷ in retaliation for its use of Israeli-made Unitronics PLCs. Although the intrusion merely triggered an alarm and shut off the system, it demonstrated how U.S. utilities can become proxy targets of geopolitical conflicts far beyond their control.

Beyond traditional nation-state threat groups, water facilities face both targeted and opportunistic attacks from cyber criminals domestic and foreign. The primary method of attack in this context is ransomware, which can disable both critical information technology (IT) and operational technology (OT) systems. While segregation of IT and OT networks may minimize the technical ability to jump from one system to another, utilities have historically closed both when either is attacked out of an abundance of caution. The country's largest water utility company, American Water, was attacked by ransomware in 2024, disrupting business enterprise systems. Conversely, a much smaller water utility servicing 11,000 residents in

Arkansas City, Kansas (<12,000 residents)⁸ experienced a cybersecurity incident in September 2024 that forced authorities to switch to manual controls.⁹ These two incidents demonstrate that cybersecurity incidents impact water utilities regardless of size.

Threat Impact

The growing importance of rural water as a resource for strategic economic, technological, and military goals makes securing the sector an increasingly urgent concern. According to the U.S. Water Alliance, a one-day disruption in water service across the U.S. could put \$43.5 billion in economic activity at risk.¹⁰ The concentration of cyber, physical, and supply chain risk to U.S. water infrastructure extends far beyond the Water Sector itself. Water is fundamental to economic activity, public health, and social stability. Significant disruptions to water services could cascade across multiple sectors, creating compound effects that adversaries might seek to exploit during geopolitical crises.

The May 2021 ransomware attack on Colonial Pipeline is a prime example of the cascading impact of a cyber-attack on critical infrastructure. The resulting lack of fuel on the east coast of the U.S. caused not only short-term economic crises, but societal panic and a lack of confidence in the government to resolve the issue. Whether China or Russia, U.S. adversaries take note of these vulnerabilities and broader dependence on critical infrastructure. When considering this case study in the context of the Water Sector, it is easy to see parallels between the water and pipeline sectors and the negative impacts that can result from a major incident.

Military Base Dependency

Civilian critical infrastructure supporting U.S. military bases include small water systems. More than 400 military installations across the U.S. rely heavily on water infrastructure that often extends far beyond base boundaries, creating dependencies on rural water and wastewater systems that may lack adequate protections. In 2017, Hurricane Irma damaged parts of Cape Canaveral, Florida (<10,000 residents),¹¹ including a bridge that contained the sole water main supplying Patrick Air Force base. Had the bridge collapsed, the base would have been without water for an indefinite period of time.¹²

An initial analysis reveals significant military base dependencies on water facilities across the United States. The below table counts facilities based on FEMA regions:

FEMA Region	# of Installations	General Area
Region 1	14	New England (CT, ME, MA, NH, RI, VT)
Region 2	19	Mid-Atlantic & Territories (NY, NJ, PR, VI)
Region 3	52	Mid-Atlantic (DE, MD, PA, VA, DC, WV)

FEMA Region	# of Installations	General Area
Region 4	90	Southeast (AL, FL, GA, KY, MS, NC, SC, TN)
Region 5	40	Midwest – Great Lakes (IL, IN, MI, MN, OH, WI)
Region 6	53	South Central (AR, LA, NM, OK, TX)
Region 7	15	Central Plains (IA, KS, MO, NE)
Region 8	28	Rocky Mountains/High Plains (CO, MT, ND, SD, UT, WY)
Region 9	71	West Coast & Pacific (AZ, CA, HI, NV, Pacific Territories)
Region 10	40	Northwest & Alaska (AK, ID, OR, WA)
Total	422	

Many military bases, particularly in rural areas, depend on shared water resources, treatment facilities, or cooperative agreements with local municipalities. This dependency means that compromised rural water and wastewater systems can have direct impacts on military readiness, training operations, and personnel welfare. Cyber-attacks on water and wastewater systems could ripple through military communities in myriad harmful ways, including disrupting firefighting capabilities, exercises at military bases, and life-saving work at medical facilities. Understanding military installations' direct or indirect connectivity to rural water and wastewater systems should be considered step one in assessing the risk posed to these systems from an adversary perspective. Additionally, recognizing these connections could potentially unlock greater Department of Defense (DOD) and federal resources to help remediate risks.

Global Technology and AI impacts

As technology companies seek lower-cost land and energy sources outside major metropolitan areas to meet growing demands for artificial intelligence and data centers, rural communities are grappling with the massive water demands of these facilities— often without the infrastructure capacity and security resources to support them safely. Currently, there are more than four-thousand data centers across the U.S. and more states are building data centers to meet these demands, often with limited water resources. Based on open source research¹³, the following is a breakdown of data centers per FEMA region:

FEMA Region	# of Data Centers	General Area
-------------	-------------------	--------------

Region 1	138	New England (CT, ME, MA, NH, RI, VT)
Region 2	224	Mid-Atlantic & Territories (NY, NJ, PR, VI)
Region 3	810	Mid-Atlantic (DE, MD, PA, VA, DC, WV)
Region 4	538	Southeast (AL, FL, GA, KY, MS, NC, SC, TN)
Region 5	646	Midwest – Great Lakes (IL, IN, MI, MN, OH, WI)
Region 6	471	South Central (AR, LA, NM, OK, TX)
Region 7	205	Central Plains (IA, KS, MO, NE)
Region 8	169	Rocky Mountains/High Plains (CO, MT, ND, SD, UT, WY)
Region 9	539	West Coast & Pacific (AZ, CA, HI, NV, Pacific Territories)
Region 10	278	Northwest & Alaska (AK, ID, OR, WA)

Total	4,018	
--------------	--------------	--

A successful cyber-attack that disrupts water services to a major data center could have cascading effects across digital services, cloud computing platforms, and internet infrastructure that extends far beyond the local community; and with limited cybersecurity budgets, personnel, and aging infrastructure, rural water and wastewater systems serving data centers are even more lucrative targets for adversaries, particularly by cyber means. Rural water systems no longer serve only rural communities. Rather, rural water is a vehicle to broader geostrategic and technologically advantageous infrastructure that must be protected accordingly.

In addition to cascading effects to our national and regional interdependent critical infrastructure, rural communities face particular vulnerabilities to attacks on chemical treatment processes, water storage, and distribution systems which could disrupt the water availability. Because of their scale, small water systems often have limited redundancy and fewer backup treatment options. Unlike urban systems that may have multiple treatment plants or alternative sources, rural utilities typically operate single-point-of-failure systems where chemical dosing errors can immediately impact the entire service population.

Broader Public Health and Civil Defense Implications

Water provides the foundation for fire suppression, medical care, decontamination procedures, mass feeding operations, and sanitation services that are essential during emergency response operations. These cascading effects are particularly relevant in the context of civil defense and potential conflict with nation-states. The China strategy, which includes reducing society's will to fight and placing pressure on public health resources, can be a method for forcing the U.S. to decide between conflict and the public's health, or at the very least make conflict a very unpopular tradeoff. Rural infrastructure is geographically dispersed, making cascading impacts to critical infrastructure and services from water attacks difficult to remediate, which further stresses other regional and state resources. Firefighting services in rural communities often use tanker shuttle services that rely on pumping stations without backup systems. The same premise largely applies to other critical infrastructure and civil defense resources. When water systems fail, the resulting impacts on firefighting capabilities can lead to uncontrolled fires that damage additional infrastructure. Failed medical facilities can create public health crises that overwhelm remaining emergency response capabilities. Disabled communication systems can prevent effective coordination of resources.

The Workforce Crisis

America's rural water and wastewater systems are facing a workforce crisis that threatens not just clean drinking water, but our nation's critical infrastructure security. NRWA's comprehensive analysis of 10,833 survey responses from across the rural water and wastewater industry reveals a perfect storm of challenges that demand immediate federal attention and investment. This is not just a water industry problem—it is a national security vulnerability hiding in plain sight.

The numbers paint a stark picture: **57 percent of rural water and wastewater workers plan to retire within the next ten years, with nearly one-third (32 percent) retiring in the next five years alone¹⁴.** The average age when respondents expect to retire from the water industry is 65 years old, creating an unprecedented knowledge drain from systems that serve millions of Americans and support critical economic sectors including agriculture, energy, and manufacturing.

This crisis, however, also represents a major opportunity. We have comprehensive data that clearly identifies the problems, engaged stakeholders ready to act, and proven models for federal investment that can build a more resilient and secure rural water and wastewater workforce. The question is not whether we can solve this challenge—it is whether we will act with the urgency that our national security requires.

The Five Front Battle

America's rural water and wastewater systems are already engaged in a five front battle that threatens not just operational capacity, but our nation's critical infrastructure security. NRWA's comprehensive analysis of 10,833 survey responses reveals that rural water and wastewater professionals are simultaneously fighting on five interconnected fronts:

1. **Insufficient pay and benefits (46%)**
2. **Aging and retiring workforce (46%)**

3. **Shrinking talent pool (42%)**
4. **Regulatory burdens (35%)**
5. **Financial or budgetary strains (30%)**

These are not isolated skirmishes but rather coordinated pressures that create cascading vulnerabilities in our nation's water infrastructure—exactly the battlefield conditions that foreign adversaries seek to exploit. When rural water and wastewater systems are already stretched thin fighting these five battles simultaneously, they become easier targets for the cyberattacks that Russia, China, and Iran are launching against American water infrastructure. Understanding this five front battle is essential for developing the strategic federal response needed to secure our rural water and wastewater systems and strengthen our national defense.

The Compensation Crisis: More Than Just Low Pay

The compensation challenge goes far beyond simple salary concerns. Rural water and wastewater professionals consistently report that **wages are low relative to the level of responsibility, pay scales do not align with those in other sectors, and benefits are perceived as limited.**¹⁵ This creates a direct national security vulnerability: when critical infrastructure operators cannot afford to stay in their jobs, system knowledge walks out the door, leaving communities and the broader economy exposed to both operational failures and security threats.

The data also reveals generational divides that underscore the urgency of this challenge. **Respondents aged 18-34 (57 percent) and 35-44 (58 percent) are far more likely to cite insufficient pay as a workforce challenge compared to those over 65 (34 percent).**¹⁶ This means the very workers we need to recruit and retain to replace retiring professionals are driven away by compensation inadequacy. Concerningly, laboratory technicians, who often handle the most technical and security-sensitive aspects of water operations, cite insufficient pay at even higher rates (56 percent) than other respondents.

Geographic analysis reveals that compensation concerns are not evenly distributed across rural America. **The Southern region shows the highest rate of compensation concerns (51 percent), followed by the Southwest and Rocky Mountains (49 percent each).**¹⁷ Meanwhile, the Pacific Coastal region shows the lowest concern (33 percent), suggesting that federal investment strategies must account for regional economic variations and target resources where the compensation gap is most severe.

The Aging Workforce: A Ticking Clock for National Security

The aging workforce challenge represents more than demographic transition—it signals a looming loss of institutional knowledge that could leave rural water and wastewater systems vulnerable to both operational failures and security breaches. **More than half (54 percent) of respondents over 65—who represent state government system workers, and laboratory technicians—identify an aging workforce as a significant challenge.**¹⁸ These are precisely the professionals with the deepest knowledge of older systems and the most experience managing complex operational and security challenges.

This impending retirement wave creates specific national security vulnerabilities. Many rural water and wastewater systems rely on **decades-old infrastructure and legacy IT systems that lack modern cybersecurity measures.**¹⁹ As workers who understand these older systems retire, communities face

knowledge gaps regarding older systems and challenges in onboarding new staff.²⁰ This creates windows of vulnerability that malicious actors could exploit.

Regional patterns in aging workforce concerns reveal where the retirement crisis will hit hardest. **New England (50 percent) and the Pacific Coastal region (51 percent) show the highest concern about aging workforce, while the Southwest shows the lowest (41 percent).**²¹ This geographic distribution suggests that federal workforce development strategies must prioritize regions facing the most severe knowledge transfer challenges.

The Shrinking Talent Pool: When Supply Cannot Meet Demand

The shrinking talent pool represents the culmination of compensation inadequacy and aging workforce challenges. **More than half of systems serving 25,001-50,000 connections (52 percent) and over 100,000 connections (52 percent) identify shrinking talent pool as a top challenge.**²² Larger rural systems face particular recruitment difficulties because they often compete directly with urban utilities that can offer higher compensation and more robust benefit packages to job seekers.

The challenge is most acute in private for-profit systems, where **51 percent identify shrinking talent pool as a workforce challenge.**²³ These systems often serve critical industrial and agricultural customers whose operations have direct national security implications. When private rural water and wastewater systems cannot maintain adequate staffing, the ripple effects extend beyond local communities to affect food processing, energy generation, and other critical economic sectors.

The data shows that younger workers and smaller systems are less likely to perceive staff shortages as critical challenges. **Only 36 percent of respondents aged 18-34 and 35 percent of those serving 101-500 connections cite shrinking talent pool as a concern.**²⁴ This suggests that the talent shortage is most severe in larger, more complex systems that require specialized skills and experience—precisely the systems whose failure would have the greatest national security implications.

The Skills and Security Gap: What the Numbers Reveal

The NRWA survey reveals a concerning shift in the applicant pool that threatens water system security. While current employees—seasoned professionals who have developed their skills over years of hands-on experience—demonstrate strong competency levels, with 93 percent performing or excelling in balancing tasks and 95 percent in creative problem-solving, the incoming workforce faces a steeper learning curve. Only 56 percent of job applicants currently possess the ability to balance different tasks, and just 50 percent demonstrate creative problem-solving skills at the time of application.²⁵

This gap reflects not a failure of individuals, but rather a structural challenge in workforce development and recruitment pipelines. These capabilities—task management and adaptive problem-solving—are not merely operational necessities; they are foundational cybersecurity competencies that typically develop through experience and training. Water system operators must manage multiple priorities simultaneously and adapt quickly to unexpected situations to defend against social engineering attacks and respond effectively to security incidents.

As experienced workers retire, water systems face the dual challenge of losing institutional knowledge while onboarding less-experienced workers who have not yet had the opportunity to develop these critical skills. The urgency is clear: rural water systems need not just more workers, but enhanced training

programs and support systems to help new hires rapidly develop the cognitive flexibility and multitasking abilities essential for maintaining security in an increasingly complex threat environment.

The cybersecurity implications become more pronounced when considering that **roughly two-thirds (65 percent) of water system respondents indicated that cybersecurity is managed by local, internal staff rather than external suppliers.**²⁶ Ultimately, rural systems face a fundamental contradiction: they want local internal cybersecurity control but lack the workforce capacity to maintain adequate expertise. This creates a vulnerability window where systems may delay necessary cybersecurity investments or operate with inadequate protection because they cannot staff appropriate positions.

Starkly, only 29 percent of executives or those familiar with the hiring process express confidence in their company's ability to hire a licensed operator.²⁷ This hiring confidence crisis extends beyond basic operations to specialized cybersecurity roles. When water system leaders lack confidence in their ability to recruit qualified personnel, they may defer critical cybersecurity upgrades or rely on inadequate stopgap measures that increase system vulnerability.

Regulatory Burdens and Financial Strains: When Compliance Diverts Resources from Security

The fourth and fifth components of rural water and wastewater workforce challenges—**regulatory burdens (35 percent) and financial or budgetary strains (30 percent)**—create a dangerous dynamic where systems must choose between regulatory compliance and cybersecurity investments.²⁸ This represents a critical national security vulnerability: when rural water and wastewater systems exhaust their limited resources on compliance paperwork and regulatory requirements, they have fewer resources available to defend against the very cyberattacks that foreign adversaries are launching against American water infrastructure.

Recent intelligence assessments confirm that **municipalities across the U.S. have faced cyberattacks from foreign adversaries like Russia, China, and Iran.**²⁹ The U.S. Intelligence Community's 2025 Annual Threat Assessment specifically highlights that **"U.S. water infrastructure has become a more common target," with criminal actors conducting cyberattacks against both large and small water utilities, possibly inspired by attacks from Russian hacktivists and Iranian cyber actors.**³⁰ When rural systems are already stretched thin by regulatory compliance burdens, they become easier targets for these sophisticated threat actors.

The data reveals a troubling pattern: the smallest rural systems face the highest regulatory burden concerns. **Systems serving fewer than 100 connections cite regulatory burdens as a challenge at 43 percent, compared to only 20 percent for systems serving over 100,000 connections.**³¹ This inverse relationship means that the most resource-constrained systems—those least capable of simultaneously managing compliance and cybersecurity—face proportionally higher regulatory pressure. These small systems often serve critical agricultural and food production communities whose compromise could have cascading effects on food security.

Geographic patterns in regulatory concerns align with regions facing the most severe cybersecurity threats. **The Mid-Atlantic region shows the highest regulatory burden concerns (44 percent), followed by New England (40 percent).**³² These are precisely the regions with high concentrations of critical infrastructure and proximity to major population centers, making them ideal targets for foreign adversaries seeking maximum impact from cyberattacks.

The financial strain component compounds these vulnerabilities in ways that directly enable cyberattacks. Recent incidents demonstrate how budget constraints lead to critical security failures: **attackers have successfully exploited internet-connected controllers using default passwords—basic security measures that remain unchanged due to staffing and resource limitations.**³³ When rural systems cannot afford dedicated cybersecurity personnel, they rely on overworked operators who may not have time to implement fundamental security practices like changing default credentials.

Tribal government systems face the most severe financial strain, with 48 percent citing budgetary constraints as a workforce challenge.³⁴ This creates particular national security concerns because tribal water systems often serve isolated communities with limited backup infrastructure. A successful cyberattack on tribal water systems could create humanitarian crises that strain federal emergency response resources and create propaganda opportunities for adversaries seeking to highlight American infrastructure vulnerabilities.

The regulatory and financial pressures create a workforce security paradox: **executives (47 percent) and utility managers (42 percent) are most likely to cite regulatory burdens as challenges.**³⁵ These are precisely the personnel responsible for cybersecurity oversight. When leadership attention is consumed by regulatory compliance, cybersecurity becomes a secondary priority—exactly the vulnerability that foreign cyber actors seek to exploit.

Federal Policy Gaps

The unprecedented cybersecurity crisis faced by America's rural water and wastewater systems exposes fundamental gaps in federal policy and investment. As previously mentioned, the threat to U.S. water infrastructure has become a more common target. Yet federal cybersecurity programs remain systematically misaligned with rural operational realities, creating exactly the vulnerabilities that sophisticated adversaries are actively exploiting.

NRWA's comprehensive analysis of 10,833 survey responses reveals that rural water and wastewater systems are fighting a five-front battle—insufficient pay and benefits (46%), aging workforce (46%), shrinking talent pool (42%), regulatory burdens (35%), and financial strains (30%)—while simultaneously defending against cyberattacks from foreign adversaries. This convergence of workforce vulnerabilities and cyber threats creates compound risks that extend far beyond individual communities to threaten national security, economic resilience, and public health.

The data demonstrates that federal approaches designed for urban areas with dedicated resources cannot serve rural communities operating with single operators managing multiple responsibilities. **Rural water professionals must simultaneously excel at a complex array of critical tasks that underscore the vital nature of their work:**

- **Equipment monitoring and control systems operation** (required by 60% and 63% of employers respectively)
- **Balancing multiple simultaneous tasks** (identified as critical by 77% of respondents)
- **Creative problem-solving for complex technical challenges** (critical skill noted by 70%)

- **Customer service and community relations** (essential for 52% of positions)
- **Data interpretation and applied mathematics** (required technical competencies)
- **Emergency response and on-call availability** (76% of workers are on-call employees, with 58% available 24/7)
- **Tasks beyond formal job descriptions** (37% regularly perform duties outside their official roles)³⁶

While Congress has established important cybersecurity authorities and programs, implementation gaps leave rural water and wastewater systems without the sustained, embedded support they need to defend against increasingly sophisticated threats. The opportunity exists today to bridge these gaps through targeted federal action that leverages proven models and addresses documented vulnerabilities.

Current Federal Authorities: Strong Foundation, Implementation Gaps

State and Local Cybersecurity Grant Program (SLCGP): Landmark Legislation with Rural Challenges

The **State and Local Cybersecurity Grant Program (SLCGP)** is the federal government's most significant investment in local cybersecurity. The U.S. Government Accountability Office (GAO) analysis shows that as of August 2024, DHS provided \$172 million to 33 states and territories for 839 cybersecurity projects, demonstrating substantial federal commitment to local infrastructure protection.

Program Strengths:

- **\$1 billion over four years** represents unprecedented federal investment in state and local cybersecurity
- **80% pass-through requirement** ensures funding reaches local communities rather than remaining at state level
- **25% rural set-aside** acknowledges that rural communities face unique cybersecurity challenges
- **Flexible project categories** allow communities to address their most pressing cybersecurity needs

Implementation Challenges for Rural Water and Wastewater Systems: The program's design, while well-intentioned, creates barriers that prevent rural water and wastewater systems from accessing available resources:

- **25% rural allocation shared across all rural infrastructure** means water systems compete against transportation, healthcare, and education sectors
- **"Match or pay first, reimburse later" structure** excludes cash-strapped rural communities unable to advance project costs
- **Competitive application process** requires grant-writing expertise that rural systems typically lack

- **Complex documentation requirements** assume administrative capacity that single-operator systems cannot provide
- GAO documentation confirms that **"rural water utilities can and should apply, but must compete with other rural stakeholders unless the state provides a targeted focus"** (GAO-25-107313) - highlighting how well-designed federal programs can inadvertently overlook specific sector needs.

Environmental Protection Agency (EPA) Water Infrastructure Authorities: Regulatory Framework Without Cybersecurity Integration

The **Clean Water Act and Safe Drinking Water Act** provide comprehensive regulatory frameworks for water system operations but contain limited cybersecurity integration, creating compliance burdens without corresponding protection capabilities or investment opportunities.

Existing EPA Cybersecurity Authorities:

- **Drinking Water State Revolving Fund** can fund eligible cybersecurity activities through low-interest loans
- **Clean Water State Revolving Fund** supports wastewater treatment cybersecurity through state-administered lending
- **Risk and Resilience Assessment requirements** mandate vulnerability identification for larger systems
- **Emergency Response Plan requirements** include cybersecurity incident procedures

Rural Implementation Barriers:

- **GAO analysis reveals that EPA's revolving fund programs "function like a bank in each state" with loan terms up to 40 years (GAO-24-106223)**, making them inappropriate for rural communities that need immediate cybersecurity grants rather than long-term debt obligations. Furthermore, only a portion of State Revolving Fund loan applicants receive funding each year. Rural systems facing cybersecurity threats require rapid implementation funding, not additional financial obligations that strain already limited operational budgets.
- The 2023, 7th annual Drinking Water Infrastructure Needs Survey and Assessment Report to Congress estimated the 20-year national drinking water infrastructure need is \$625 billion for pipe replacement, treatment plant upgrades, storage tanks, and other key assets. This is a 32% increase over the 6th assessment (\$472.6 billion). This existing almost insurmountable need competes with resources needed to emerging nation state cyber threat to water critical infrastructure.
- **Survey data shows that 35% of rural water and wastewater professionals cite regulatory burdens as significant workforce challenges**, yet compliance mandates arrive without adequate corresponding federal technical assistance or funding.³⁷ For example, the 2024 EPA estimates the cost of implementing the PFAS rule alone to be approximately \$1.548 billion per year for public water systems and primacy agencies.³⁸ While other industry analysis estimates compliance with the new PFAS regulation will cost \$37.1 to \$48.3 billion nationally to install new PFAS drinking

water treatment systems over the next five years.³⁹ The annualized cost of operations and maintenance is projected to be between \$2.7 to \$3.5 billion.⁴⁰ This analysis highlights the significant financial commitment required to address PFAS contamination in drinking water. Rural systems must simultaneously satisfy EPA water quality standards and emerging cybersecurity requirements while lacking sufficient dedicated personnel for either compliance area.

United States Department of Agriculture (USDA) Rural Development Authorities: Proven Technical Assistance Model, Cybersecurity Gap

There is broad agreement that the Circuit Rider Program, which has been in place since 1980, is the most successful federal technical assistance program for rural water and wastewater systems. However, this program currently excludes dedicated cybersecurity assistance.

Circuit Rider Program Strengths:

- **50+ years of proven success** in delivering embedded on-site training and technical assistance to rural water and wastewater systems
- **Trusted community relationships** built through sustained engagement and practical support
- **Understanding of rural operational constraints** and resource limitations
- **Cost-effective model** that leverages regional expertise and community networks

Cybersecurity Authority Gap: While USDA possesses unmatched rural community relationships and technical assistance infrastructure, the agency lacks cybersecurity regulatory authority and specialized expertise. This creates a critical gap where the federal agency best positioned to serve rural communities cannot address their most pressing security threat.

Legislative Recognition of Model Effectiveness: Recent legislation through the Department of Energy (DOE) introduced **Circuit Rider Program** that demonstrates congressional understanding that circuit rider models work effectively for rural technical assistance. The legislation would authorize the DOE program at \$25 million and provide 3-6 year grants with 75 percent federal cost share for energy efficiency support, showing that Congress recognizes rural communities need sustained, embedded assistance for complex technical challenges.

Cybersecurity and Infrastructure Security Agency (CISA) Critical Infrastructure Authorities: National Coordination Without Rural Engagement

Cybersecurity and Infrastructure Security Act established CISA as the federal lead for critical infrastructure cybersecurity, including water systems, but implementation remains focused on larger utilities with dedicated security personnel.

CISA Water Sector Authorities:

- **Critical infrastructure protection coordination** across all **16** critical infrastructure sectors
- **Threat intelligence sharing** through sector-specific information sharing organizations
- **Incident response coordination** for significant cybersecurity events

CISA Rural Challenges

- **Engagement Limitations:** CISA's training programs are modeled for scale across larger urban systems and assumptions of robust organization structures, consistent high-speed broadband access, and dedicated IT personnel. The reality is that many rural systems lack the workforce capacity to implement CISA's guidance without sustained technical assistance.
- **Intelligence-Action Gap:** While CISA provides threat intelligence confirming that foreign adversaries are targeting water infrastructure, this information doesn't translate to actionable protection measures for rural systems operating with minimal cybersecurity expertise and limited resources.

Federal Investment Patterns: Massive Energy Investment, Fragmented Water Support

Department of Energy (DOE) Cybersecurity Leadership Model

DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) demonstrates how dedicated federal investment can provide comprehensive sector support with \$200 million annually for energy cybersecurity coordination.

CESER Comprehensive Approach:

- **Sector-specific research and development** addressing energy infrastructure cybersecurity challenges
- **Coordinated technical assistance** tailored to energy industry operational requirements
- **Emergency response capabilities** with dedicated energy sector expertise
- **Industry partnership** based on deep understanding of energy operational constraints

Water Sector Investment Disparity: Energy cybersecurity receives dedicated federal investment reflecting critical infrastructure priority, while water cybersecurity competes for generic funding across multiple local government sectors. **Congressional Research Service (CRS) analysis shows the energy-water nexus makes this disparity strategically problematic - thermoelectric cooling represents 38 percent of freshwater withdrawals nationally (CRS R43199), yet water receives a fraction of energy's cybersecurity investment.**

Fragmented Water Cybersecurity Investment

Multiple Agency Approach Without Coordination:

- **EPA:** Focuses on regulatory compliance and revolving fund loans
- **CISA:** Provides generic cybersecurity guidance across all critical infrastructure sectors
- **USDA:** Delivers rural technical assistance but lacks cybersecurity authority
- **FEMA/DHS:** Administers SLCGP but treats water as one among many local government responsibilities and grantees

No Designated Water Cybersecurity Lead: Unlike energy infrastructure, which benefits from CESER's coordinated leadership, water cybersecurity remains fragmented across agencies with different missions, authorities, and priorities. This ensures that no federal entity takes comprehensive responsibility for rural water and wastewater cybersecurity.

Workforce-Cybersecurity Intersection: Compounding Vulnerabilities

The Five-Front Battle Creates Cyber Vulnerabilities

NRWA data reveals that rural water and wastewater systems simultaneously face five interconnected challenges that create exactly the conditions foreign adversaries seek to exploit:

Workforce Challenges Enabling Cyber Threats:

- **46% cite insufficient pay and benefits** - driving experienced operators away during critical cybersecurity transition period
- **46% cite aging workforce concerns** - creating knowledge gaps as workers understanding legacy systems retire
- **42% cite shrinking talent pool** - limiting ability to recruit cybersecurity-capable personnel
- **35% cite regulatory burdens** - diverting limited resources from cybersecurity to compliance activities
- **30% cite financial strains** - preventing investment in cybersecurity infrastructure and personnel

Geographic Vulnerability Patterns:

- **Southern region shows highest compensation concerns (51%)** - regions with critical agricultural infrastructure face greatest workforce retention challenges
- **Mid-Atlantic region shows highest regulatory burden concerns (44%)** - areas with dense critical infrastructure face greatest compliance pressures
- **New England and Pacific Coastal regions show highest aging workforce concerns (50-51%)** - regions facing retirement waves also have highest concentrations of legacy infrastructure requiring specialized knowledge

Rural Systems Need External Cybersecurity Support but Face Multiple Barriers

A 2025 Water Report shows that 65 percent of water systems prefer cybersecurity managed by internal staff rather than external suppliers.⁴¹ However, this preference reflects practical constraints for rural communities rather than strategic choice. Rural water and wastewater systems face significant barriers to accessing external cybersecurity support that make internal management appear to be the only viable option, even when communities lack the expertise to implement effective protection.

1. **Geographic and Economic Barriers to External Support:** Rural communities struggle to access external cybersecurity services due to their remote locations and limited economic base. Most

cybersecurity consulting firms concentrate in urban areas where they can serve multiple clients efficiently, making rural service calls expensive and infrequent. When external expertise is available, rural systems often cannot afford the premium rates that specialized cybersecurity consultants command, particularly for the ongoing monitoring and incident response that effective cybersecurity requires.

2. **Scale and Complexity Mismatches:** Cybersecurity vendors typically design services for larger utilities with dedicated IT departments and substantial budgets. Rural water and wastewater systems with single operators managing multiple responsibilities cannot utilize cybersecurity solutions that assume full-time IT personnel, complex network architectures, or sophisticated monitoring capabilities. **Only 29% of rural water and wastewater executives express confidence in their ability to hire licensed operators,** and this hiring confidence crisis extends to specialized cybersecurity contractors who must understand both cybersecurity and water system operations.⁴²
3. **Trust and Relationship Challenges:** Rural communities often prefer working with local contractors who understand their operational constraints and can provide immediate, hands-on support during emergencies. Cybersecurity services increasingly require remote monitoring and cloud-based management that conflicts with rural preferences for direct, relationship-based support. Rural operators may hesitate to grant external entities access to critical infrastructure systems, particularly when those vendors lack Water Sector experience or established community relationships.
4. **Limited Competition and Service Options:** Rural areas often lack competitive markets for specialized services, leaving communities with few options for cybersecurity support. When external cybersecurity services are available, rural systems may face vendor lock-in situations with limited alternatives if service quality or pricing becomes problematic. This creates dependency relationships that rural communities, already struggling with workforce and financial constraints, seek to avoid.
5. **Federal Technical Assistance Gap:** The preference for internal cybersecurity management reflects the absence of sustained federal technical assistance that could bridge the gap between rural needs and external expertise. Circuit rider programs work effectively for traditional water system operations because they provide trusted, ongoing relationships with technical experts who understand rural constraints. The lack of equivalent cybersecurity circuit rider programs forces rural systems to choose between inadequate internal capabilities and inaccessible external services.

Policy Recommendations

America's rural water and wastewater systems stand at a crossroads. The infrastructure that delivers clean water to millions of Americans—the same systems that support our military bases, power our data centers, and sustain our agricultural economy—faces an unprecedented crisis that threatens both local communities and national security.

The convergence is stark and undeniable: 57 percent of rural water and wastewater workers plan to retire within the next decade, just as sophisticated cyber adversaries from China, Russia, and Iran intensify their attacks on our water infrastructure. This isn't merely a workforce challenge—it's a national security vulnerability that demands immediate federal action.

NRWA's comprehensive analysis of over 10,000 rural water and wastewater professionals reveals the full scope of this crisis. Rural water and wastewater systems are fighting what we call "the five-front battle"—simultaneously grappling with 1) insufficient compensation, 2) an aging workforce, 3) a shrinking talent pool, 4) crushing regulatory burdens, and 5) severe financial constraints. These interconnected pressures create exactly the conditions that foreign adversaries seek to exploit.

The window for effective action is narrowing rapidly. With nearly one-third of rural water and wastewater workers planning to retire in the next five years, we face an unprecedented loss of institutional knowledge at precisely the moment when cybersecurity expertise is most critical. The workers who understand decades-old infrastructure and legacy systems—the very systems most vulnerable to cyberattacks—are preparing to leave the workforce.

But this crisis also presents an unprecedented opportunity. The data reveals clear patterns. Engaged stakeholders stand ready to act. Proven models for federal investment already exist. The question isn't whether we can address these challenges—it's whether we will act with the urgency our national security requires.

A Strategy Built on Proven Success

The policy recommendations that follow represent more than theoretical solutions. They are practical, data-driven approaches designed to leverage existing federal authorities, build on successful programs, and meet rural water and wastewater systems where they are. Each recommendation recognizes a fundamental truth: rural communities operate with different constraints, capabilities, and needs than their urban counterparts.

These proposals deliberately build on what works. The Circuit Rider Program has successfully delivered technical assistance to rural water and wastewater systems for over 50 years. The State and Local Cybersecurity Grant Program represents landmark federal investment in local infrastructure protection. DOE's cybersecurity coordination office demonstrates how dedicated federal leadership can provide comprehensive sector support.

These proposals recognize that rural water and wastewater systems cannot simply adapt urban solutions. They need targeted federal support that accounts for single operators managing multiple responsibilities, limited cash flow that prevents advance project funding, and geographic isolation that makes traditional cybersecurity services impractical.

Threat Intelligence Recommendations

1. Annual Water Threat Assessment

The Ask: Congress should direct the Office of the Director of National Intelligence to conduct annual water threat assessments and integrate findings into its Annual Threat Assessment to Congress and the

American people, providing policymakers with water-specific threat analysis, federal investment effectiveness evaluation, and early identification of emerging vulnerabilities. This assessment should include a comprehensive analysis of rural water and wastewater systems directly supporting the Defense Industrial Base to access enhanced federal cybersecurity resources including domain name system protection, threat intelligence feeds, and specialized technical assistance.

The Problem and Threat: While the 2025 Annual Threat Assessment acknowledges water infrastructure has "become a more common target," it lacks both robust Water Sector and rural-specific analysis needed to develop targeted federal responses, allocate resources effectively, and identify emerging threats before they can be exploited by adversaries. Many rural water and wastewater systems unknowingly support critical defense operations but remain unaware of their defense connections or the enhanced cybersecurity resources available through Defense Industrial Base membership.

The Solution: Create dedicated intelligence assessment providing policymakers with water-specific threat analysis, enabling intelligence-driven policymaking and resource allocation while providing early warning of new threats targeting water systems.

Why This Matters:

- Enables intelligence-driven policy making and resource allocation for water security
- Provides early warning system for emerging threats targeting water infrastructure
- Creates accountability mechanism for assessing effectiveness of federal cybersecurity investments
- Ensures Congress and stakeholders receive actionable intelligence for decision making

The Setup: Integrate rural water and wastewater analysis into existing Annual Threat Assessment process and Intelligence Community capabilities, leveraging established intelligence gathering and analysis frameworks while providing Congress with actionable intelligence for oversight and resource allocation.

Technical Assistance Recommendations

2. Rural Water and Wastewater Cybersecurity Circuit Rider Program

The Ask: Congress should authorize and appropriate funds for the launch of the Rural Water and Wastewater Cybersecurity Circuit Rider Program at \$25 million annually for fiscal years 2026-2030 to establish a specialized cybersecurity circuit rider program within USDA. This new program's authority and funding should exist as separate but coordinated effort to the existing Rural Water Circuit Rider Program

The Problem and Threat: Rural water and wastewater systems face sophisticated cyber threats from state-sponsored actors including Volt Typhoon (China), Sandworm (Russia), Iran-based cyber groups, and cybercriminals worldwide, but lack the expertise and resources to defend themselves. Generic cybersecurity training assumes personnel and experience that most rural systems simply don't have. Additionally, rural communities' geographic dispersion makes them particularly challenging to support during cybersecurity emergencies, while the U.S. Water Alliance estimates one-day water

disruption could put \$43.5 billion in economic activity at risk. Current emergency response capabilities are not designed for the unique challenges of rural water and wastewater infrastructure.

The Solution: Integrate cybersecurity expertise into USDA's proven Circuit Rider Program model, providing expedited on-the-ground support from experts who understand rural operational constraints and resource limitations. As part of this program, Cybersecurity Circuit Riders would be able to respond to rural water and wastewater systems that are under cyberattack.

Why This Matters:

- Leverages the NRWA and USDA's 50-year successful partnership and track record of successful technical assistance
- Rural water and wastewater systems already trust and rely on this delivery model
- Creates immediate pathway for deploying protective measures to vulnerable communities, including in emergency situations
- Designed for rural realities—single operators, part-time volunteers managing multiple responsibilities
- Minimizes economic impact and public health risks from successful cyber attacks
- Demonstrates federal commitment to protecting rural communities during crisis situations

The Setup: Build cybersecurity technical assistance into the existing Circuit Rider framework that rural water and wastewater systems know and trust, rather than creating entirely new programs they must learn to navigate.

3. Rural Water Cybersecurity Set-Aside in State and Local Cybersecurity Grant Program

The Ask: Congress should reauthorize (current extension **set to expire on January 30, 2026**) the State and Local Cybersecurity Grant Program (SLCGP) to create a dedicated 10 percent annual allocation specifically for rural water and wastewater systems, while eliminating the "match first, reimburse later" requirement for rural water and wastewater utilities serving fewer than 10,000 people.

The Problem and Threat: The current program's 25 percent rural allocation is shared across all critical infrastructure sectors, forcing water systems to compete with transportation, healthcare, and education for limited resources. The reimbursement model excludes cash-strapped rural communities who cannot advance project costs while waiting months for federal reimbursement.

The Solution: Create a dedicated Water Sector allocation within the existing grant program structure, with direct grant funding that recognizes rural cash flow limitations and provides immediate access to cybersecurity resources.

Why This Matters:

- Rural water and wastewater systems lack cash flow to advance project costs while waiting for reimbursement

- Competition with other infrastructure sectors leaves water systems consistently underserved
- Targeted approach addresses water-specific vulnerabilities identified in national threat assessments
- Eliminates fundamental financial barrier preventing rural participation

The Setup: Amend existing State and Local Cybersecurity Grant Program legislation to create sector-specific allocation within proven grant program structure, building on established state administrative capabilities while eliminating barriers to rural participation.

4. Water Industry Workforce Support through Apprenticeship

The Ask: Congress should enact the following pending provision contained in the House FY2026 Labor, Health and Human Services, Education, and Related Agencies appropriations legislation: “The Committee directs DOL to make \$20,000,000 in grant funding available to establish, implement, expand, and administer registered apprenticeship programs consistent with the National Guideline Standards of Apprenticeship for Water and Wastewater System Operations Specialists to address nationwide shortages of qualified drinking water and wastewater operators, especially in rural America.” (page 18)

The Problem and Threat: The more than 380,000 skilled workers who operate the nation’s rural water and wastewater systems keep our drinking water safe; protect our lakes, streams, and groundwater; and help our nation’s rural communities stay economically viable. But up to 50% of these workers could retire within the next 10 years. Most rural water systems have been unable to attract, train and retain the next generation workforce due to the lack of an identifiable career path, coupled with both low salary levels and population density. Meanwhile, advancements in water treatment and supply technology have increased the skills and training required.

The Solution: The NRWA Apprenticeship Program will enhance water workforce participation and retention in small, rural and tribal communities, protect the federal investment in America’s water and wastewater systems, improve these vital services to customers, certify water worker proficiency with an identifiable career path, modernize the water industry’s approach to workforce development, enhance professionalism and upskill the incumbent worker, increase the recognition of the public benefit that water and wastewater systems deliver to their communities, schedule wage increases, and provide access to sophisticated and advanced technology.

Why This Matters:

- Leverages the apprenticeship model for the rural water industry to attract and retain trained water and wastewater professionals
- Rural water and wastewater systems already trust and rely on the partnerships established through NRWA and State Rural Water Associations
- Creates an immediate pathway to attract and retain water and wastewater professionals for rural America’s water and wastewater utilities
- Demonstrates federal commitment to ensuring small and rural communities have the ability and pathways to support the rural water workforce

The Setup: The NRWA National Apprenticeship Program includes 4,000 hours of on-the-job training with a one-to-one mentor to apprentice ratio and 288 hours of technical instruction over a 2-year period with an increasing wage schedule suggested every six months. NRWA Apprenticeship Program graduates serve as public health officials and will often be the only person responsible for complying with the multitude of applicable federal Safe

Drinking Water Act and Clean Water Act regulations to supply their small community with safe drinking water and sanitation services every second of every day.

Strategic Coordination Recommendations

5. Coordinated Federal Rural Water and Wastewater Security Strategy

The Ask: Congress should require development and implementation of a coordinated federal strategy across United States Department of Agriculture (USDA), Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), Department of Labor (DOL), and National Security Agency (NSA) for rural water and wastewater security, with federal agencies reporting effectiveness to Congress rather than imposing additional reporting requirements on rural systems, and explicit prohibition of new compliance burdens on already overwhelmed rural water and wastewater operators.

The Problem and Threat: Current fragmented approach across multiple federal agencies creates duplicated efforts, conflicting directives, and coverage gaps while rural systems struggle with existing compliance burdens that divert scarce resources from cybersecurity and operations to administrative reporting.

The Solution: Create unified federal strategy coordinating all rural water and wastewater security efforts under clear leadership while explicitly protecting rural systems from additional reporting burdens, focusing accountability at the federal level rather than local level.

Why This Matters:

- Eliminates duplicated federal efforts and conflicting directives that confuse rural operators
- Focuses limited rural resources on operations and security rather than compliance reporting
- Creates federal accountability for coordination and effectiveness rather than local reporting burdens
- Ensures comprehensive, coordinated approach to rural water and wastewater security across all relevant agencies

The Setup: Model similar to the successful Federal Interagency Collaboration to Reduce Food Loss and Waste, demonstrating how effective multi-agency efforts can exist while leveraging specialized expertise from partner agencies through formal interagency agreements and shared resources.

Conclusion

The evidence is overwhelming: America's rural water and wastewater infrastructure faces a perfect storm of challenges that no single community can solve alone. While state-sponsored adversaries position themselves for future disruption and cybercriminals exploit basic vulnerabilities, the knowledge and expertise needed to defend these systems walks out the door with each retiring worker.

This analysis reveals more than problems—it illuminates solutions. The federal government possesses the partnerships, authorities, resources, and proven models needed to transform rural water and wastewater security. From leveraging NRWA’s unmatched rural relationships to scaling successful cybersecurity programs, the building blocks for holistic and comprehensive reform already exist.

The recommendations presented here chart a pragmatic path forward that recognizes rural realities while addressing national security imperatives. They prioritize immediate protection through emergency circuit riders and targeted grants, build sustained capacity through workforce development and coordination offices, and establish long-term resilience through modernization and emergency response capabilities.

The choice is not between competing priorities but between proactive investment and crisis response. Our national security and collective success depends on federal leadership that matches the sophistication of the threat to America’s rural water and wastewater systems.

This page is intentionally left blank

-
- ¹ National Rural Water Association, & McKinley Advisors. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ² Office of the Director of National Intelligence. (2025, March). *Annual Threat Assessment of the U.S. Intelligence Community, 2025 [Unclassified report]*. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>
 - ³ U.S. Environmental Protection Agency, Office of Inspector General. (2024, November 13). *Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems (Report No. 25-N-0004)*. https://www.epaoig.gov/sites/default/files/reports/2024-11/full_report_-_25-n-0004t_1.pdf
 - ⁴ The Driller. (n.d.). *Water facilities have increased cybersecurity, but most still fall short, says security expert*. Retrieved from <https://www.thedriller.com/articles/93394-water-facilities-have-increased-cybersecurity-but-most-still-fall-short-says-security-expert>
 - ⁵ U.S. Census Bureau. (n.d.). *QuickFacts: Littleton, Middlesex County, Massachusetts*. Retrieved from https://data.census.gov/profile/Littleton_town,_Middlesex_County,_Massachusetts?g=060XX00US2501735950
 - ⁶ U.S. Census Bureau. (n.d.). *QuickFacts: Muleshoe City, Texas*. Retrieved from https://data.census.gov/profile/Muleshoe_city,_Texas?g=160XX00US4849968
 - ⁷ U.S. Census Bureau. (n.d.). *QuickFacts: Aliquippa City, Pennsylvania*. Retrieved from https://data.census.gov/profile/Aliquippa_city,_Pennsylvania?g=160XX00US4200820
 - ⁸ U.S. Census Bureau. (n.d.). *QuickFacts: Arkansas City, Kansas*. Retrieved from https://data.census.gov/profile/Arkansas_City_city,_Kansas?g=160XX00US2002300
 - ⁹ Greig, J. (2024, September 25). *CISA warns of continuing attacks on water systems after Kansas town reports incident*. The Record. <https://therecord.media/cisa-warns-of-attacks-against-water-systems-arkansas-city>
 - ¹⁰ US Water Alliance. (2017, March 22). *New analysis finds closing the investment gap in water infrastructure would create 1.3 million jobs, \$220 billion in economic activity*. <https://uswateralliance.org/new-analysis-finds-closing-the-investment-gap-in-water-infrastructure-would-create-1-3-million-jobs-220-billion-in-economic-activity/>
 - ¹¹ U.S. Census Bureau. (n.d.). *Profile: Cape Canaveral city, Florida [Data set]*. Retrieved from https://data.census.gov/profile/Cape_Canaveral_city,_Florida?g=160XX00US1210250
 - ¹² Florida Today. *Irma leaves Sykes Creek Bridge in limbo*. Sept. 22, 2017. Retrieved from <https://www.floridatoday.com/story/news/2017/09/22/irma-leaves-sykes-creek-bridge-limbo/693985001/>
 - ¹³ DataCenterMap. (n.d.). *USA Data Centers: 4,055 facilities from 1,712 operators*. Retrieved from <https://www.datacentermap.com/usa/>
 - ¹⁴ McKinley Advisors, & National Rural Water Association. (2025, September 2). *NRWA Workforce Research 2024 Industry Study*. Retrieved from <https://content.nrwa.org/white-papers/document/15754347/nrwa-workforce-research-2024-industry-study>
 - ¹⁵ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ¹⁶ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ¹⁷ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ¹⁸ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ¹⁹ Schingh, B. (2025, May 26). *Securing the flow: Addressing the national security vulnerabilities in the US water supply*. Small Wars Journal. Retrieved from <https://smallwarsjournal.com/2025/05/26/water-security-national-infrastructure-cyber-threats/>
 - ²⁰ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²¹ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²² McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²³ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²⁴ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²⁵ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²⁶ Black & Veatch. (2025). *2025 Water Report*. <https://www.bv.com/en-US/resources/water-report>
 - ²⁷ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²⁸ McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
 - ²⁹ Gallego, R., & Cotton, T. (2025, May 1). *Gallego, Cotton introduce bipartisan bill to strengthen America's water infrastructure against cyber attacks [Press release]*. Retrieved from <https://www.gallego.senate.gov/press-releases/gallego-cotton-introduce-bipartisan-bill-to-strengthen-americas-water-infrastructure-against-cyber-attacks/>
 - ³⁰ Office of the Director of National Intelligence. (2025, March). *Annual Threat Assessment of the U.S. Intelligence Community, 2025 (Unclassified report)*. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>

-
- 31 McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
- 32 McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
- 33 Schingh, B. (2025, May 26). *Securing the flow: Addressing the national security vulnerabilities in the US water supply*. Small Wars Journal. Retrieved from <https://smallwarsjournal.com/2025/05/26/water-security-national-infrastructure-cyber-threats/>
- 34 McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
- 35 McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
- 36 McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
- 37 McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>
- 38 U.S. Environmental Protection Agency. (2024, April 8). *Benefits and costs of reducing PFAS in drinking water* [Fact sheet]. https://www.epa.gov/system/files/documents/2024-04/pfas-npdwr_fact-sheet_cost-and-benefits_4.8.24.pdf
- 39 Association of State Drinking Water Administrators. (2024, August 2). *AWWA releases updated national PFAS cost estimate* [Press release]. <https://www.asdwa.org/2024/08/02/awwa-releases-updated-national-pfas-cost-estimate/> (asdwa.org)
- 40 Association of State Drinking Water Administrators. (2024, August 2). *AWWA releases updated national PFAS cost estimate* [Press release]. <https://www.asdwa.org/2024/08/02/awwa-releases-updated-national-pfas-cost-estimate/> (asdwa.org)
- 41 Black & Veatch. (2025). *2025 Water Report*. <https://www.bv.com/en-US/resources/water-report>
- 42 McKinley Advisors, & National Rural Water Association. (2024, October). *NRWA 2024 Industry Study*. <https://p1-cms-assets.imgix.net/mindful/rmm/workspaces/default/uploads/2025/09/whitepaper-final-nrwa-2024-industry-study.cmAFCRRNM4.pdf>