Testimony of Virginia Wright

Cyber-Informed Engineering Program Manager

Idaho National Laboratory

Before the Environment Subcommittee

United States House Committee on Science, Space, and Technology

--

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

May 21, 2026

Chairman Franklin and Ranking Member Amo, and members of the Subcommittee, thank you for the opportunity to testify today. My name is Virginia Wright, and I am a Program Manager at the Idaho National Laboratory—one of 17 U.S. Department of Energy national laboratories where I have spent 19 years working on the cybersecurity of critical infrastructure, including the energy and water sectors.

Background: The Water Sector's Vulnerability Profile

The United States (U.S.) drinking water and wastewater sector serves more than 300 million Americans through approximately 170,000 public water and wastewater systems.[1] These systems range from very small rural systems serving a few hundred people to large metropolitan utilities serving millions. The obvious impact from the water sector is what comes out of the tap and into a glass; however, the water sector also supports industries from data centers to manufacturing, providing water and safely removing wastes to magnify American prosperity. Our water and wastewater sector is under active assault from nation-state and criminal cyber actors, and this committee must use its power to direct and prioritize federal resources to strengthen this core pillar of U.S. prosperity.

Water and wastewater systems of all sizes face the same cybersecurity threat environment but with very different capacities to respond and recover. Smaller systems often have no dedicated cybersecurity staff and limited budgets for cybersecurity investment. However, the consequences of a cyberattack on these systems, just like their larger counterparts, can disrupt

[1] U.S. Government Accountability Office, *EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744 (Washington, DC: GAO, 2024), https://www.gao.gov/assets/gao-24-106744.pdf.

water services, inflict financial burdens, and potentially impact community health and safety. Impacts of a cyberattack on wastewater treatment can include raw sewage overflows, environmental discharge violations, and treatment process disruptions. Ransomware attacks on wastewater treatment plants have already occurred in the United States.[2]

Many water and wastewater utilities rely on legacy digital control systems with default or hard-coded passwords. Because of their age, these systems may have acknowledged vulnerabilities and outdated security approaches and may no longer receive patches and updates from their vendors or support from the third-party integrators who installed them. Furthermore, many asset owners leverage remote access tools for system monitoring and control of their infrastructure, and these remote access capabilities/tools are prime targets for adversary exploitation.[3]

The water sector is undergoing a rapid digital transformation. A recent State of the Water Industry Report[4] highlights upgrading aging infrastructure as the highest priority of responding utilities. With these upgrades, asset owners are adopting automation, remote monitoring, and digital control systems. These technologies reduce operating costs and improve service reliability but also expand the potential for cyberattacks, especially without dedicated cybersecurity staff.

The interplay between legacy systems and digital transformation is a key focus area for the water and wastewater sector. The water sector has been incredibly successful at using manual operations, one of the benefits of their legacy and outdated systems, to limit the consequences of cyberattacks to their subscribers. Lives have been saved and services have been speedily restored because operators could continue services when attacks occurred. As the sector digitizes, it is crucial to ensure that the capability to manually operate critical functions is not digitized away. Even as the Environmental Protection Agency (EPA) aids asset owners to incorporate automation and even autonomy to lower costs and increase the effectiveness of services, they must also encourage asset owners to assess and prioritize manual operations as a proactive capability that reduces attack impacts and enhances recovery.

The Threat Landscape

---

[2] Benjamin Freed, "*Water treatment plant in North Dakota suffered ransomware attack*," *State Scoop*, January 30, 2024, https://statescoop.com/minot-north-dakota-water-treatment-ransomware/.
[3] Dragos, Inc., "Threat Perspective: United States Water and Wastewater," Hanover, MD: Dragos, Inc., 2024, https://5943619.hs-sites.com/hubfs/Reports/Dragos_Report_CyberThreatPerspective_USWater_Wastewater_Complete.pdf.
[4] American Water Works Association, "2026 State of the Water Industry," Denver, CO: AWWA., 2026, https://www.awwa.org/wp-content/uploads/2026-SOTWI-Full-Report.pdf.

Threats facing the water sector are escalating and intensifying. Nation-states, state-sponsored proxies, hacktivists, and criminal ransomware organizations have all demonstrated both the intent and the capability to compromise water system operational technology.[5]

The incidents of recent years form a clear pattern. In November 2023, Iranian-backed Cyber Av3ngers compromised the municipal water authority in Aliquippa, Pennsylvania.[6] They specifically targeted an Israeli-manufactured programmable logic controller. This demonstrated that water system components could be identified by manufacturer and model and targeted by nation-state actors. In January 2024, the Cyber Army of Russia Reborn (CARR) compromised industrial control systems at water utilities in Abernathy, Muleshoe, and Hale Center, Texas.[7] Water storage tanks overflowed and tens of thousands of gallons of water were lost. CARR also gained control of the Supervisory Control and Data Acquisition (SCADA) system of a U.S. energy company,[8] but did not cause harm. In April of this year, EPA, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) released a joint cybersecurity advisory warning of Iranian targeting of internet-connected programmable logic controllers affecting multiple sectors, including the water and wastewater sectors. These attacks, similar to attacks in 2023, manipulated control logic and data resulting in operational disruption and financial loss.[9]

The threat extends beyond our borders in ways that carry direct lessons for American utilities. Poland's Internal Security Agency, the ABW, documented in its 2024–2025 activities report[10] that hacktivist groups compromised water treatment stations in five Polish municipalities, gaining access and potential control of industrial control systems. The ABW attributed these intrusions to inadequate password management and unsecured device management panels directly accessible on the public internet. Though not within the U.S., these are small municipal water systems serving rural and semi-rural populations with limited resources and aging infrastructure and they are operationally and organizationally analogous to thousands of

---

[5] U.S. Environmental Protection Agency, "EPA, FBI, CISA, NSA Issue Joint Cybersecurity Advisory for Water System Regarding Iranian Activity," Last modified 2024, https://www.epa.gov/newsreleases/epa-fbi-cisa-nsa-issue-joint-cybersecurity-advisory-water-system-regarding-iranian.

[6] Ribeiro, Anna, "Iranian Hacker Group CyberAv3ngers Allegedly Breach Municipal Water Authority of Aliquippa," *Industrial Cyber*, November 27, 2023, https://industrialcyber.co/industrial-cyber-attacks/iranian-hacker-group-cyberav3ngers-allegedly-breach-municipal-water-authority-of-aliquippa/.

[7] Scheve, Annasofia, "Overflowing Water Tank Linked to Russian Cyber Attack," *Government Technology*, January 23, 2024, https://www.govtech.com/security/overflowing-water-tank-linked-to-russian-cyber-attack.

[8] Arghire, Ionut, "US Sanctions Russian Hacktivists for Targeting Critical Infrastructure," *Security Week*, February 23, 2024, https://www.securityweek.com/us-sanctions-russian-hacktivists-for-targeting-critical-infrastructure/.

[9] Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency. *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure*. Washington, DC, 2026. https://www.ic3.gov/CSA/2026/260407.pdf.

[10] Aktywnosci, Wybrane. Agencja Bezpieczeństwa Wewnętrznego (ABW): 2024–2025: Warsaw: ABW, 2025, https://www.abw.gov.pl/download/24/4867/ABWraport20242025.pdf.

American water utilities. What happened to them can happen here, through the same vulnerabilities, exploited by the same methods.[11]

On this front, however, there is some recent good news. In October 2024, a commercial company, Censys, discovered just under 400 human-machine interfaces (HMIs), the control interfaces for water systems, exposed to the internet. All used the same software, 95 were configured to require authentication, 264 were configured for public read-only access, and 40 had no authentication. Censys immediately contacted the vendor and the EPA, and the EPA took quick action to work with the vendor and affected utilities. When last reported in May 2025, less than 6% of the systems remained accessible in a read-only or unauthenticated state.[12] This vignette shows that it is possible to quickly increase water and wastewater security with the right technical insights and focus.

That focus is needed now. Current reporting suggests that attackers are starting to leverage artificial intelligence (AI) technology to enhance their targeting and offensive depth. In early 2026, Dragos, Inc. documented an intrusion into a municipal water and drainage utility in Monterrey, Mexico.[13] The adversary used commercial AI tools to conduct reconnaissance, map the environment, and develop command and control tools. The AI independently identified an internally accessible SCADA interface as a high-value target and generated a targeted attack capability for the attacker. Dragos notes that the attempts to breach that interface were ultimately unsuccessful and no access to the underlying operational technology (OT) environment was achieved. Nevertheless, Dragos concludes that the significance of this case is that AI materially lowered the barrier to OT targeting. As Dragos states, AI "can make operational technology systems more visible to adversaries already operating inside information technology environments." They recommended that asset owners increase the maturity of their detection and response capabilities and move beyond prevention-only security strategies, which, as AI tools continue to improve, are becoming insufficient on their own. This advice is particularly important given that most rural and small water and wastewater systems have no or very limited attack detection capabilities and no resources to enhance them.

The gap between the threat the water sector faces and the resources available to defend against it is not a gap that utilities can close on their own. EPA, often partnered with CISA, offers assistance in the form of assessments, technical assistance, cybersecurity evaluations and

---

[11] EPA, *Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems*. Washington, DC: U.S. Environmental Protection Agency, Office of Inspector General, Report No. 25-N-0004, November 13, 2024. https://www.epa.gov/sites/default/files/oig/documents/Full%20Report%2025-N-0004_Errata.pdf.

[12] Censys, "Turning Off the Information Flow: Working with the EPA to Secure Hundreds of Exposed Water HMIs," *Censys Blog*, June 5, 2025, https://censys.com/blog/turning-off-the-information-flow-working-with-the-epa-to-secure-hundreds-of-exposed-water-hmis.

[13] Deen, Jay, "AI-Assisted Compromise of Mexican Water Utility with OT Implications," May 2026, https://5943619.hs-sites.com/hubfs/116-Whitepapers/dragos-2026-ai-mexico-water-attack-intel-brief.pdf.

guidance, like the bulletin mentioned above.[14] These capabilities may be a good start for asset owners with the capacity to request and receive them, but to date, do not fully meet the needs of the sector. Especially for rural water and wastewater asset owners, near-term mitigations and long-term research and development (R&D) outcomes must be targeted to the asset owner environment and accompanied by technical assistance to support implementation.[15] R&D timelines are usually long, creating capabilities for a future that is years, and sometimes decades away. EPA must prioritize R&D to address the threats currently in our systems while we anticipate and prepare for the next generation of threats.

The Innovation Pipeline: Barriers and Federal Roles

Federal R&D investment serves multiple purposes. It advances scientific and technical knowledge. It also produces tools, methods, and trained personnel that critical infrastructure operators can use. For the water sector, the pipeline from early-stage research to deployed operational capability faces significant barriers at nearly every stage.

The most fundamental barrier to adopting research outcomes is resource scarcity at the utility level. For community water systems with no dedicated cybersecurity staff, solutions must be designed to be low or no cost and easy to deploy, function with limited maintenance and oversight, and be supplied with support for their installation and use. Training and technical assistance must be free and accessible. Federal programs must actively reach utilities rather than expecting utilities to find their way to federal resources. In addition, since many water utility systems are operated and supported by third-party engineering firms or solution integrators, federal programs must reach beyond sector operators into the ecosystem of vendors and service providers that support them.

To rapidly advance water-sector cybersecurity at the pace of the oncoming threats, EPA should direct research into the following six R&D focus areas:

- Engineer cybersecurity resilience into water infrastructure
- Secure the water sector hardware and software supply chain
- Build the cybersecurity workforce the water sector needs
- Anticipate high-consequence threats and proactively protect the sector
- Enhance attack detection and response for even the smallest utilities

---

[14] U.S. Environmental Protection Agency, "EPA Cybersecurity for the Water Sector." Accessed May 2026, https://www.epa.gov/cyberwater/epa-cybersecurity-water-sector.

[15] Tisdale, Nicole, "Rural Water's Ripple Effect: National Security, Cyber Threats, and the Future of Water," National Rural Water Association, March 2026, 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.

- Drive cybersecurity investment through market incentives and insurance.

Several applicable federal programs could be directly used or tailored for water sector needs. In addition to the existing EPA and CISA efforts focused on the water sector, the following capabilities and programs would enhance EPA's ability to deliver R&D capabilities that address the growing threat environment in alignment with water sector constraints.

Existing Capabilities and Their Application to the Water Sector

The Water Security Test Bed. Cybersecurity research for OT requires physical test environments. Researchers need infrastructure for research that mimics the operational scope and scale of a water utility. Though physical and digital models and digital twin technology can be useful for predicting and demonstrating aspects of system behavior, they are not a replacement for a physical testbed operating at the scope and scale of the actual industrial process. At-scale testbeds allow the study of complex interactions between system components necessary for quantitative research outcomes.

The Idaho National Laboratory (INL) established the Water Security Test Bed (WSTB)[16] in 2013 through a partnership with EPA. It is located within INL's Critical Infrastructure Test Range, part of INL's 890-square-mile site. In its current configuration, the facility includes approximately 450 feet of 8-inch water main line, a service line to a premise plumbing room, and a wastewater lagoon for bulk water event testing. To date, it has been used for research to evaluate impacts and recovery opportunities from chemical or biological contamination events.

Initiated this fiscal year, efforts are underway to expand the capabilities of the WSTB. This project has begun to install a SCADA system and infrastructure systems, and additional infrastructure components are planned to enable the testbed to more closely mirror how a municipal water system is structured, monitored, and controlled. Eventually this proposed expansion will add pilot-scale water and wastewater treatment capabilities and would complete the test bed's coverage of all three interconnected segments of a municipal water system: water treatment, water distribution, and wastewater treatment.

With these enhancements, the WSTB will be instrumental for R&D to develop proactive protection from emerging threats, and it will play a strong role in each of the suggested research objectives. The WSTB will also provide an environment for workforce development by supporting exercises and training on at-scale infrastructure. It can serve as a platform to generate data for use in educational and research programs that is technically precise and sharable, without operational sensitivities.

[16] INL, "Water Security Test Bed Overview," Idaho Falls, ID: Idaho National Laboratory, 2021, https://inl.gov/content/uploads/2023/07/Water-Security-Test-Bed.pdf.

This full-system test bed will allow researchers to study how attacks propagate across interconnected water infrastructure and will speed development and validation of the detection, response, and recovery capabilities that utilities need.

Cyber-Informed Engineering. Cyber-Informed Engineering (CIE) deepens the defenses of water and wastewater systems by using engineering to eliminate the worst consequences of cyberattack, even when digital defenses fail. This methodology, developed by the Department of Energy's (DOE) Cybersecurity, Energy Security, and Emergency Response (CESER) organization, is directly applicable to the water sector, and adoption is underway.

The American Water Works Association (AWWA) has adopted CIE and published specific guidance for water asset owners.[17] In Idaho, INL worked with the Idaho Department of Environmental Quality (DEQ) to integrate CIE into the state's grant and loan funding cycle for water and wastewater infrastructure projects.[18] For 2026 projects, 66% of Idaho's State Revolving Fund (SRF) funded projects committed to use CIE, and for 2027 this increased to 85%. EPA's October 2025 guidance on cybersecurity in SRF programs specifically recognizes Idaho DEQ's CIE approach as distinctive among state programs, noting that it goes beyond traditional cybersecurity elements to emphasize engineered cybersecurity controls that provide safety and redundancy benefits in addition to cybersecurity protection.[19] EPA could expand this adoption by encouraging CIE as an approach that complements the basic cybersecurity hygiene requirements that states are beginning to implement and by offering technical assistance that will make it meaningful for small systems to engineer out the cybersecurity impacts. EPA could aid in the development of tools and design guidance for asset owners that make CIE inexpensive to apply.

One of the simplest CIE approaches mentioned in the AWWA guidance is for asset owners to conduct a "Day without Automation" exercise, where they assess the organization's ability to operate if digital systems were unreliable or unavailable. Adding this to EPA's existing Tabletop Exercise Inventory would allow asset owners to identify and address critical assumptions about

---

[17] Ohrt, Andrew, and Daniel Groves, *Resilience through Cyber-Informed Engineering: An Engineering and Operations Approach to Cybersecurity,* Denver, CO: American Water Works Association, 2025,

[18] Idaho Department of Environmental Quality, *GPR-02 Cyber-Informed Engineering (CIE) Analysis Guidance,* Boise, ID: Idaho Department of Environmental Quality, 2026, https://www2.deq.idaho.gov/admin/LEIA/api/document/download/24361.

[19] U.S. Environmental Protection Agency, Strengthening and Integrating Cybersecurity Measures into State Revolving Fund (SRF)–Funded Projects, Washington, DC: U.S. Environmental Protection Agency, October 2025, https://www.epa.gov/system/files/documents/2025-10/strengthening-and-integrating-cybersecurity-measures-into-state-revolving-fund-srf-funded-projects.pdf.

their readiness for a cyberattack. This exercise concept complements and extends the Department of Homeland Security (DHS) CISA approach for critical infrastructure fortification.[20]

For the most consequential facilities, INL's Consequence-Driven Cyber-Informed Engineering methodology (CCE) provides a more rigorous approach. CCE is a structured four-phase process that identifies critical functions, predicts how adversaries would compromise them, and identifies engineering and operational mitigations. INL has licensed CCE to water sector industry partners for application in the water and wastewater sector.[21]

CyTRICS. The Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program is sponsored by DOE CESER. CyTRICS works with vendors to identify high-priority OT components, perform expert testing to find supply chain vulnerabilities, and inform improvements in component design. It leverages six DOE national laboratories and strategic industry partnerships. Many water sector component manufacturers are also energy sector manufacturers, and several are already participants in CyTRICS.

EPA could leverage CyTRICS as a model to develop a similar program or partner with DOE. Testing high-priority water sector components would benefit thousands of utilities that have no insight into the security characteristics of the equipment they operate, and it would speed mitigation of issues by water sector vendors.

Liberty Eclipse. Liberty Eclipse is an annual full-scale cybersecurity preparedness exercise sponsored by DOE CESER. During this exercise, energy utilities defend a physical test bed that replicates real energy infrastructure against test effect payloads designed to replicate real adversary attacks. National Guard cybersecurity units participate alongside utility teams. Liberty Eclipse is not a tabletop discussion; instead, it is an operational, real-time exercise that allows utilities to validate response plans, identify assumptions and gaps, and build relationships between operational and cybersecurity teams.

The water sector has no equivalent exercise. The WSTB, once its buildout is complete, could serve as the physical foundation for a water sector version of Liberty Eclipse. Water utilities could defend a representative system against a simulated attack, test incident response plans in real time, and build the interagency relationships that effective response requires.

---

[20] CISA, "CI Fortify: Strengthening Resilience Across Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, accessed May 2026, https://www.cisa.gov/topics/industrial-control-systems/ci-fortify.
[21] Idaho National Laboratory, "Consequence-Driven, Cyber-Informed Engineering," *INL National Security*, accessed May 2026, https://inl.gov/national-security/cce/.

ICS Cybersecurity Training. INL hosts a suite of advanced industrial control systems (ICS) cybersecurity training courses at its Control Systems Analysis Center in Idaho Falls. These courses are sponsored by DHS/CISA and are available at no cost to participants.[22]

ICS 301 is a 4-day advanced Red Team versus Blue Team exercise conducted in an immersive IT/OT environment. ICS 311 is an intelligence-driven threat detection course. It is conducted in a live cybersecurity range with industrial controllers, field devices, and physical processes. It teaches asset owners to use open-source cybersecurity detection tools including Malcolm, Security Onion, and Wireshark. ICS 401 is a structured eight-step cybersecurity evaluation methodology course. It was explicitly designed for small- and medium-sized organizations without dedicated cybersecurity risk management personnel, which is exactly the profile of most American water utilities. All three courses are free, IACET-accredited, and directly applicable to water sector needs. Water utility participation in these courses remains dramatically lower than energy sector participation, comprising less than 5% of participants.

INL's cybersecurity escape rooms reinforce these concepts in a time-bound entertaining way. Participants analyze evolving threats and make coordinated decisions under pressure while developing skills in attack detection, mitigation, and system recovery. INL also has a wastewater skid that provides a scaled-down wastewater treatment environment with real control systems and cybersecurity threats. INL's escape rooms could be good additions at meetings or conferences where water sector stakeholders gather, and the wastewater skid can be leveraged virtually for many different training scenarios.

Coordinated federal outreach through EPA, the WaterISAC, and AWWA, and financial aid for attendee travel could substantially increase water sector participation in ICS training. Support for adding escape rooms or virtual exercises on the wastewater skid at sector events would enhance workforce development at minimal cost.

Malcolm. Malcolm is an open-source network traffic analysis tool developed to give OT operators visibility into the networks interconnecting their control systems. Malcolm provides dozens of pre-built dashboards to provide awareness of network traffic and identify potential malicious activity. Malcolm was originally developed for the Bureau of Reclamation under CISA sponsorship, and it is available for open download at no license cost, a critical characteristic for under-resourced water utilities. INL is currently helping multiple water sector partners deploy, install, and use Malcolm as part of CISA's Critical Infrastructure Shared Services Pilot program[23]

---

[22] Idaho National Laboratory, "ICS Cybersecurity Training," INL National Security, accessed May 2026, https://inl.gov/national-security/ics-cybersecurity-training/.

[23] Cybersecurity and Infrastructure Security Agency, "CI Program Fact Sheet," September 2025, https://www.waterisac.org/wp-content/uploads/2025/09/CI-Program-Fact-Sheet-Sept-25.pdf.

and has developed specific capabilities for flow monitoring to address water sector needs. This tool could be a crucial capability for attack detection for more resourced water utilities.

CI Fortify:

CI Fortify[24] is a new initiative from DHS CISA that is being applied to the water sector. This defensive strategy trains asset owners in times of crisis, to isolate operational networks from external connections and execute pre-planned resilience strategies, including transitioning to manual operations. Consistent with the advice in this document, CISA is targeting CI Fortify at the ecosystem level, including asset owners, vendors, and suppliers, managed service providers and integrators, security vendors, and volunteers. CI Fortify could help to ensure that water and wastewater operators, especially rural and small asset owners, have tailored recovery plans focused on service delivery. To be most effective, CI Fortify could be paired with Cyber-Informed Engineering to provide technical assistance, aid asset owners to plan recovery actions, and extend the depth of their defenses. Full details on the planned program are still emerging; however, this is an appropriate step for this infrastructure sector.

Recommendations

Now:

1. Continue to prioritize full-scale applied testing capabilities like the WSTB and support its utilization through ongoing R&D, testing, and training programs. Once complete, the WSTB will emulate all three municipal water system segments and will serve as the sector's first full-scale, integrated cyber-physical research and training facility.
2. Build on existing SRF cybersecurity momentum using the Idaho DEQ model as a template. Advise baseline cybersecurity practices such as the SANS Top Five Critical Controls[25] to complement the use of CIE. Provide dedicated federal technical assistance funding, delivered through EPA's Office of Water Emergency Response and Cybersecurity and national laboratory partnerships, to ensure that small systems can implement CIE as they upgrade critical infrastructure.
3. Increase federal outreach to sector utilities, integrators and service providers regarding existing no-cost federal training, including DHS/CISA-sponsored ICS 301, 311, and 401 courses hosted at INL. Coordinate this outreach through EPA, the Water ISAC, and AWWA and provide support for travel and other costs where needed.

[24] CISA, "CI Fortify: Strengthening Resilience Across Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, Accessed May 2026, https://www.cisa.gov/topics/industrial-control-systems/ci-fortify.
[25] SANS Institute, "The Five ICS Cybersecurity Critical Controls," Accessed May 2026, https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls.

4. Encourage DOE and EPA to assess how the CyTRICS supply chain vulnerability program can be extended to include water sector OT components.

Soon:

5. Create design templates for water and wastewater systems with incorporated engineering protections to ease adoption of Cyber-Informed Engineering. This will lower costs and establish repeatable patterns for security.
6. Develop a full-scale water sector cybersecurity exercise program modeled on Liberty Eclipse. The WSTB could serve as the physical testbed for this exercise.

Longer Term:

7. Develop incentive structures for the ecosystem to ensure investments in water sector modernization are equally investments in its security.
8. Use the WSTB to operationalize anticipatory threat research, moving water sector cybersecurity defense from reactive to proactive.

Conclusion

The water sector is a crucial capability for American health and prosperity, yet it lacks the tools, resources, and federal support to defend itself against sophisticated nation-state adversaries, AI-assisted attacks, and criminal ransomware groups.

EPA, in collaboration with CISA, is providing capabilities to address this need, but more is needed. Many R&D capabilities for critical infrastructure cybersecurity exist and can be tailored to the needs of the water sector.

Cyber-Informed Engineering provides a methodology for engineering cybersecurity protection into water infrastructure, and the Idaho DEQ example provides a model for its implementation at scale. The WSTB provides the physical foundation for a research and training program the sector urgently needs. Liberty Eclipse, CyTRICS, Malcolm, CI Fortify, and the DHS/CISA-sponsored training courses hosted at INL represent a portfolio of capabilities that, if extended and applied systematically to the water sector, can materially improve its security posture.

Sustained federal attention, coordination, and investment are needed to connect these capabilities to the utilities that need them – now – and to anticipate future threats, including the growing use of AI to enhance cyberattacks. The community water systems that protect the health of every American are largely small, under-resourced, and facing a threat landscape that is growing more sophisticated every year. They cannot close that gap alone. Federal R&D can help if it is focused on impact reduction over compliance, applied with urgency and designed for the realities of the water sector.

I appreciate the opportunity to testify before this committee, and I look forward to your questions.