COMMITTEE ON
SCIENCE, SPACE AND TECHNOLOGY
CHAIRMAN BRIAN BABIN

SUBCOMMITTEE ON ENVIRONMENT

HEARING CHARTER

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

Thursday, May 21, 2026
2:00 pm
2318 Rayburn House Office Building

Purpose

The purpose of this hearing is to examine how environmental research and development (R&D) can enhance efforts to protect the nation's drinking water and wastewater systems from increasingly sophisticated cyber threats. Growing attempts by foreign adversaries and other malicious actors to exploit water systems underscore the need to better understand vulnerabilities and strengthen defenses.

As the Environmental Protection Agency (EPA) serves as the lead Sector Risk Management Agency for the water sector, it oversees federal cybersecurity efforts for drinking water and wastewater systems. This hearing will assess how federal environmental R&D contributes to identifying and cataloging key risks to critical infrastructure. It will further examine how exploitation of these weaknesses could result in cascading disruptions with significant environmental and public health impacts. The hearing will inform Members about ongoing efforts to strengthen the R&D pipeline supporting practical cybersecurity tools for utilities, as well as the challenges affecting the development, deployment, and sustainment of cybersecurity innovations across the water sector.

Witnesses

- **Mr. David Hinchman, Director, IT & Cybersecurity, U.S. Government Accountability Office**
- **Ms. Virginia Wright, Cyber-Informed Engineering Program Manager, Idaho National Laboratory**
- **Mr. Joshua Corman, Executive in Residence for Public Safety & Resilience, Institute for Security and Technology**
- **Ms. Nicole Tisdale, Founder & Principal, Advocacy Blueprints, LLC**

Background

The United States has approximately 152,000 public drinking water systems, including 50,000 community water systems, and over 16,000 wastewater treatment systems.[1] More than 80 percent of Americans rely on these systems for their drinking water, and about 75 percent have their sanitary sewerage treated by these wastewater systems.[2]

Public water systems are regulated by the Environmental Protection Agency (EPA) under two separate statutes. The Safe Drinking Water Act (SDWA) was originally enacted in 1974 and authorizes the EPA to regulate drinking water facilities.[3] EPA's authority was expanded in 1986[4] and 1996[5] to include regulatory authority over drinking water sources– including rivers, lakes, reservoirs, springs, and groundwater wells. The Federal Water Pollution Control Act was first enacted in 1948 and became colloquially known as the Clean Water Act (CWA) after it was substantially amended in 1972.[6] The CWA authorizes the EPA to set regulatory standards for wastewater quality and to develop national water quality criteria for pollutants in surface water.

While each statute governs different components of water infrastructure and establishes the regulatory framework within which utilities operate, both rely on cooperative federalism, under which states are responsible for implementing requirements overseen by the EPA. As a result, there are varied levels of preparedness and cybersecurity capacity across the United States.

While EPA may issue guidance or enforcement, its authority to require cybersecurity practices is neither explicit nor comprehensive under existing statutes.[7] As a result, federal guidance, research, and voluntary programs play a significant role in advancing cybersecurity across the water sector. Federal investments in research and development are critical to developing tools, models, and best practices that can be adopted across both drinking water and wastewater systems despite differing statutory requirements.

---

[1] Cybersecurity & Infrastructure Sec. Agency, *Water and Wastewater Systems Sector,* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector.

[2] *Id.*

[3] Safe Drinking Water Act, Pub. L. No. 93-523, 88 Stat. 1660 (1974).

[4] Safe Drinking Water Act Amendments of 1986, Pub. L. No. 99-359, 100 Stat. 642.

[5] Safe Drinking Water Act Amendments of 1996, Pub. L. No. 104-182, 110 Stat. 1613.

[6] Federal Water Pollution Control Act Amendments of 1972, Pub. L. No. 92-500, 86 Stat. 816.

[7] Safe Drinking Water Act § 1420A, 42 U.S.C. § 300g-10 (2026); Federal Water Pollution Control Act § 504, 33 U.S.C. § 1364 (2026).

Water system failures can directly affect drinking water safety, wastewater treatment, and the health of surrounding ecosystems. Cyberattacks can potentially threaten the safety and reliability of services for more than 324 million people.[8] These attacks can result in disruption and loss of service, equipment damage, unsafe drinking water, and improper treatment of wastewater. Increasingly, these systems face cyber risks from foreign adversaries, including Russia, China, and Iran.[9] Cyber intrusions targeting water systems can disrupt treatment processes, undermine monitoring systems, and increase the potential for public exposure to contamination events. As these systems become more automated and digitized, they become increasingly appealing targets for cybercriminals and bad actors.[10] EPA maintains an interactive national map of Public Water System Service Areas, which shows the geographic extent of each utility's distribution system and illustrates the scale of populations potentially affected by cyberattacks or operational disruptions.[11]

Cybersecurity has become a key factor in system performance and long-term reliability.[12] Addressing these challenges requires consistent investment in applied scientific research that identifies vulnerabilities, creates solutions, and supports the transition of innovations into tools that utilities can use. As small and rural water systems seek to modernize, they remain especially vulnerable due to limited funding, staffing, and technical capability.[13] These concerns are reflected in a growing number of cyber incidents that have caused or threatened harm to water systems nationwide.[14] Applied research is essential for translating scientific insights into affordable, practical tools that water utilities can realistically deploy to address real-world cybersecurity, operational, and infrastructure challenges.

Cyber Threats and Attacks

Cyberattacks directed at critical infrastructure in the United States, especially water and communications networks, are growing more sophisticated and frequent.[15]

---

[8] Cong. Research Serv., R48556, Cybersecurity of the Municipal Water Sector: Background and Issues for Congress (June 3, 2025), https://www.crs.gov/Reports/R48556#fn5.

[9] Press Release, U.S. Envtl. Prot. Agency, *EPA, FBI, CISA, & NSA Issue Joint Cybersecurity Advisory to Water Systems Regarding Iranian Cyber Threats*, https://www.epa.gov/newsreleases/epa-fbi-cisa-nsa-issue-joint-cybersecurity-advisory-water-system-regarding-iranian.

[10] U.S. Gov't Accountability Office, *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744 (Aug. 1, 2024), https://www.gao.gov/assets/gao-24-106744.pdf.

[11] U.S. Envtl. Prot. Agency, *Public Water System Service Areas*, https://www.epa.gov/ground-water-and-drinking-water/public-water-system-service-areas?tab=map.

[12] U.S. Gov't Accountability Office, GAO-24-106744, *Drinking Water: Agencies Should Strengthen Efforts to Help Utilities Address Cybersecurity Risks* (2024), https://www.gao.gov/products/gao-24-106744.

[13] *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744, at 31 (U.S. Gov't Accountability Off. Aug. 2024), https://www.gao.gov/assets/gao-24-106744.pdf.

[14] *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744, at 23-25 (U.S. Gov't Accountability Off. Aug. 2024), https://www.gao.gov/assets/gao-24-106744.pdf.

[15] U.S. Gov't Accountability Off., *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, GAO-23-105327 (Dec. 2022), https://www.gao.gov/assets/gao-23-105327.pdf.

Water System Intrusions and Operational Technology Exploitation

In April 2026, the EPA, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) issued a joint advisory warning that Iranian-affiliated actors were exploiting operational technology in U.S. water systems.[16] This activity targeted operational technology components such as programmable logic controllers, human-machine interfaces, and sensors.[17] Prior to that, in May 2024, the EPA announced plans to increase enforcement actions to ensure drinking water systems address cybersecurity threats.[18] Together, these developments underscore the need for sustained federal investment in environmental and cybersecurity research to help utilities rapidly identify vulnerabilities and adopt tools that reduce the risk of future intrusions. Beyond these Iran-linked intrusions, federal agencies have also warned of increasingly sophisticated and persistent cyber campaigns conducted by state-sponsored actors from China.[19] These evolving nation-state threats underscore the need for research-driven resilience measures that strengthen detection, harden technology pathways, and ensure utilities can maintain essential services even under advanced and persistent cyber pressures.

In October 2024, American Water, the largest water utility in the United States, experienced a cyberattack that shut down key systems, including billing.[20] Throughout 2024, small water utilities in Texas, Kansas, and Indiana were similarly compromised when attackers remotely accessed systems, manipulated operational controls, caused water tank overflows, and forced utilities in multiple states to revert to manual operations.[21] In 2023, an intrusion at the Municipal Water Authority of Aliquippa in Pennsylvania compromised internet-connected operational technology, also requiring manual override.[22]

Vulnerabilities Across Water Systems

Federal assessments show that many water utilities face basic technical weaknesses, including insecure remote access, outdated software, and insufficient separation between business information technology (IT) and operational technology (OT) in water systems.[23] Because these

---

[16] Press Release, U.S. Envtl. Prot. Agency, *EPA, FBI, CISA, & NSA Issue Joint Cybersecurity Advisory to Water Systems Regarding Iranian Cyber Threats*, https://www.epa.gov/newsreleases/epa-fbi-cisa-nsa-issue-joint-cybersecurity-advisory-water-system-regarding-iranian.

[17] Cybersecurity & Infrastructure Sec. Agency & U.S. Envtl. Prot. Agency, *Internet-Exposed Human Machine Interfaces Pose Cybersecurity Risks to Water and Wastewater Systems* (Dec. 13, 2024), https://www.epa.gov/system/files/documents/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf.

[18] U.S. Envtl. Prot. Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities* (May 2024), https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

[19] Chris Jaikaran, Cong. Research Serv., IF12798, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications* (2025), https://www.crs.gov/Reports/IF12798.

[20] Spencer Kimball, *American Water, Largest U.S. Water Utility, Targeted by Cyberattack*, CNBC (Oct. 8, 2024), https://www.cnbc.com/2024/10/08/american-water-largest-us-water-utility-cyberattack.html.

[21] James, *11 Recent Cyber Attacks on the Water and Wastewater Sector*, Wisdiam (Oct. 13, 2024), https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/.

[22] *Id.*

[23] U.S. Gov't Accountability Off., *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744, at 31 (Aug. 2024), https://www.gao.gov/assets/gao-24-106744.pdf.

systems were not originally designed with cybersecurity in mind, structural gaps allow attackers to move from IT networks into OT environments that manage pumps, chemical dosing, and treatment processes. These unintended design weaknesses further demonstrate the need for science-driven modernization of water infrastructure.

Workforce and Capacity Constraints

A persistent workforce shortage, especially in small and rural utilities, limits the sector's ability to hire or afford specialized, dedicated cybersecurity staff.[24] According to the Government Accountability Office, many utilities rely on general IT employees or outside contractors, reducing their capacity to implement, manage, and update modern OT security controls.[25]

EPA technical assistance programs also recognize that staffing limitations reduce the ability of utilities to continuously monitor threats, manage system updates, and respond to incidents that ultimately impact operational technology environments.[26] As a result, cybersecurity readiness varies widely across the country. Strengthening research and development can help generate tools, training, and workforce development resources designed for utilities with limited staff.

Telecommunications Dependencies and Connectivity Gaps

Water and wastewater systems increasingly depend on telecommunications infrastructure to operate modern supervisory control and data acquisition (SCADA) systems, remote sensors, and cloud-based monitoring platforms to transmit operational data in real time.[27] This interdependence creates cyber-physical risks: disruptions or compromises in telecommunications systems can impair utilities' real-time visibility or remote control of operations.[28] Because encrypted remote-access tools and fiber or cellular links are used to manage pumps, chemical dosing, and pressure systems, telecommunications failures can translate into operational disruption.[29]

Federal risk frameworks, including those developed by CISA, highlight how vulnerabilities in communications networks can cascade into water system operations that rely on continuous connectivity to maintain safe drinking water and wastewater treatment operations.[30]

Applied research is critical to understanding these interdependencies and ultimately necessary to developing solutions that keep water systems resilient even if communications networks become compromised.

---

[24] U.S. Gov't Accountability Office, GAO-24-106744, *Drinking Water and Wastewater Infrastructure: Federal Efforts to Address Cybersecurity Risks* (2024), https://www.gao.gov/products/gao-24-106744.
[25] *Id*.
[26] U.S. Envtl. Prot. Agency, *Cybersecurity for Water Sector Systems*, https://www.epa.gov/cyberwater/cybersecurity-assessments.
[27] U.S. Envtl. Prot. Agency & Cybersecurity & Infrastructure Sec. Agency, *Internet-Exposed Human-Machine Interfaces Pose Cybersecurity Risks to Water and Wastewater Systems* (Dec. 13, 2024), https://www.epa.gov/system/files/documents/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf.
[28] *Id.*
[29] U.S. Envtl. Prot. Agency, *Water Sector Guide to Telecommunications During Power Outages* (June 2022), https://www.epa.gov/system/files/documents/2022-06/TelecomGuide_508c.pdf.
[30] Cybersecurity & Infrastructure Sec. Agency, *Communications Sector*, https://www.cisa.gov/communications-sector.

Relevant Agencies

Strengthening the cybersecurity and resilience of drinking water and wastewater systems depends on coordinated work across multiple federal agencies that support a highly diverse set of utilities nationwide.

- EPA plays a central role in advancing and coordinating this work as the lead Sector Risk Management Agency for the water sector.[31] It also leads federal efforts to strengthen cybersecurity across drinking water and wastewater systems. EPA provides voluntary technical assistance, training, and security tools to utilities, all of which are underpinned by foundational scientific research and development.[32]
- CISA provides threat intelligence, vulnerability advisories, scanning services, and operational cyber support and works alongside other federal law enforcement and intelligence agencies. Through this operational role, CISA delivers guidance, technical support, and coordinated response efforts that help utilities reduce risk and improve resilience across the sector.[33] CISA also promotes a Secure by Design approach, which requires security to be built into products from the start rather than added after deployment, reducing common weaknesses such as weak default credentials, insecure remote access, and avoidable software flaws.[34]
- The Department of Energy (DOE) supports applied, federally funded cybersecurity and infrastructure resilience research through its national laboratories, including Idaho National Laboratory (INL), which is home to the Water Security Test Bed (WSTB) originally developed by EPA researchers.[35] INL's work through WSTB reflects a shift toward designing infrastructure that remains resilient under real-world conditions.[36] It also prioritizes embedding safety directly into engineered systems rather than relying only on cybersecurity tools.[37]
- The National Institute of Standards and Technology (NIST) develops federal cybersecurity frameworks and risk management guidance used across critical infrastructure sectors, including water systems. Its Cybersecurity Framework and Industrial Control Systems (ICS) Security guidance provide structured approaches to identifying, protecting, detecting, responding to, and recovering from cyber threats.[38]

---

[31] Press Release, U.S. Envtl. Prot. Agency, *EPA, FBI, CISA, & NSA Issue Joint Cybersecurity Advisory to Water Systems Regarding Iranian Cyber Threats*, https://www.epa.gov/newsreleases/epa-fbi-cisa-nsa-issue-joint-cybersecurity-advisory-water-system-regarding-iranian.

[32] U.S. Envtl. Prot. Agency, *Cybersecurity for Water Sector Systems*, https://www.epa.gov/waterresilience/cybersecurity-water-sector.

[33] Cybersecurity & Infrastructure Sec. Agency, *Water and Wastewater Systems Sector*, https://www.cisa.gov/water-and-wastewater-systems-sector.

[34] Cybersecurity & Infrastructure Sec. Agency, *Secure by Design*, https://www.cisa.gov/securebydesign.

[35] U.S. Envtl. Prot. Agency, *Water Security Test Bed*, https://www.epa.gov/emergency-response-research/water-security-test-bed.

[36] *Id.*

[37] Idaho Nat'l Lab., *Cyber-Informed Engineering*, https://inl.gov/national-security/cie/.

[38] Nat'l Inst. of Standards & Tech., Nat'l Cybersecurity Ctr. of Excellence, *Securing Water and Wastewater Utilities: Cybersecurity for the Water and Wastewater Systems Sector* (June 20, 2023), https://www.nccoe.nist.gov/sites/default/files/2023-06/securing-water-and-wastewater-utilities-project-description-final.pdf.