United States Government Accountability Office

Testimony

Before the Subcommittee on the Environment, Committee on Science, Space, and Technology, U.S. House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Thursday, May 21, 2026

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Persistent Cybersecurity Threats to the Water and Wastewater Sector

Statement of David B. Hinchman, Director,
Information Technology and Cybersecurity

GAO-26-109159

GAO Highlights

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Persistent Cybersecurity Threats to the Water and Wastewater Sector

GAO-26-109159 May 21, 2026

A testimony before the Subcommittee on the Environment, Committee on Science, Space, and Technology, U.S. House of Representatives

Contact: David B. Hinchman at hinchmand@gao.gov or J. Alfredo Gómez at gomezj@gao.gov

What GAO Found

Threat actors, such as state-sponsored hackers or criminal groups, are increasingly capable of carrying out cyberattacks on water and wastewater systems. This capability comes from the increasing connections between operational technologies—which control valves, pumps, and other physical devices—and internet-enabled devices. Internet-enabled devices can provide remote access to control pumps and other infrastructure. Remote access can be helpful over large and widely distributed water and sewer systems. However, the convergence of operational technologies and internet-enabled devices has also increased the ability of online attackers to reach critical operational systems.

Water and wastewater systems have faced challenges reducing their vulnerability to cyberattacks. For example, systems have varying levels of cybersecurity capabilities. Systems are also managing workforce shortages and older technologies that are difficult to update with modern cybersecurity protections. Systems must also prioritize limited financial resources, so meeting regulatory requirements for clean and safe water may out-compete cybersecurity investments.

Water and Wastewater Systems are Vulnerable to Cyberattack

Water systems may contain hundreds of diverse components, making it difficult to properly map and keep operational technologies updated with security patches.

Attackers may use IT networks to steal data or to move within the network to access operational systems.

IT and operational networks may not be properly separated, allowing attackers to access the operational systems and disrupt critical processes.

Sources: Cybersecurity and Infrastructure Security Agency (information); ungvar/Rawpixel/James Thew/stock.adobe.com (photos). | GAO-26-109159

In 2024, GAO found that the Environmental Protection Agency (EPA) had not performed key cybersecurity risk management steps for the sector and made recommendations to address these shortfalls. In response, EPA conducted a water sector risk assessment and developed a risk management plan to guide its efforts to mitigate priority risks.

GAO also reported that EPA had faced legal challenges in its efforts to ensure water and wastewater entities took action to improve their cybersecurity. In response to GAO's recommendation to evaluate the sufficiency of its legal authorities, EPA identified several critical gaps. Specifically, EPA identified a lack of cybersecurity risk assessment requirements for wastewater systems and certain drinking water systems. EPA also identified significant limitations in its authority under federal drinking water and clean water laws to address those gaps. GAO will continue to monitor how EPA addresses these limitations.

Why GAO Did This Study

Recent cyber incidents and security alerts highlight the vulnerability of the close to 170,000 water and wastewater systems that make up the U.S. water and wastewater systems sector (water sector). The water sector is one of 16 critical infrastructure sectors. GAO has identified the cybersecurity of critical infrastructure as a component of the cybersecurity high-risk area, which is one of nine high-risk areas needing focused executive and congressional attention.

A successful cyberattack on a water or wastewater system could lead to service disruptions that harm public health or the environment. These systems have already experienced ransomware attacks, which use malicious software to deny access to IT systems or data.

EPA is responsible for leading, coordinating, and supporting activities to reduce cybersecurity risk to the water sector. EPA works in partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and other federal, state, and local entities.

This statement addresses the cybersecurity challenges facing the water sector and EPA's actions to address the sector's cybersecurity risks.

This statement is based on GAO's August 2024 report on cybersecurity risks to U.S. water and wastewater systems (GAO-24-106744); documents provided by EPA in response to GAO's recommendations; and publicly available information, as of May 2026, regarding challenges and EPA's water sector cybersecurity efforts.

Chairman Franklin, Ranking Member Amo, and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on the cybersecurity challenges facing our nation's water and wastewater systems sector (water sector). The water sector is made up of over 153,000 drinking water systems and 16,500 wastewater systems. These systems are governed by multiple federal, state, and local authorities with responsibility for public health, environmental protection, and security measures.

The U.S. Environmental Protection Agency (EPA), in collaboration with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), is responsible for coordinating water sector activities and supporting sector risk management, among other duties.[1] EPA is also expected to coordinate its security efforts with other federal agencies, state and local governments, private sector entities and associations, and critical infrastructure owners and operators.

A successful cyberattack on a water or wastewater facility could lead to service disruptions that harm public health or the environment. Further, the consequences of a successful attack can cascade beyond the water sector and affect energy, heath care, and other sectors that rely on water and wastewater for their operations. Ransomware attacks—a cyberattack using malicious software to deny access to IT systems or data until a ransom is paid—have already affected water and wastewater systems. For example, ransomware attacks on water and wastewater systems in California, New Jersey, and Nevada have disrupted computer systems and required operations to temporarily run systems manually.

Water and wastewater systems are also facing new and more destructive cyberattacks, ranging from insider threats from witting or unwitting employees, to attacks from around the globe. For example, in November 2023, multiple organizations—including a Pennsylvania water system—were hacked by an Iran-affiliated group. Workers at the Pennsylvania

[1]The April 2024 White House National Security Memorandum on Critical Infrastructure Security and Resilience categorized the nation's critical infrastructure into 16 sectors with at least one federal agency designated as Sector Risk Management Agency for the sector, although the number of sectors and Sector Risk Management Agency assignments are subject to review and modification. See 6 U.S.C. § 652a(b); The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum 22 (NSM-22) (Washington, D.C.: Apr. 30, 2024) (rescinding and replacing the 2013 Presidential Policy Directive-21).

system had to temporarily halt pumping in a station and operate the system manually. Following these and other attacks, EPA, CISA, and others issued an April 2026 advisory warning water and wastewater systems that Iran-affiliated groups were targeting technologies commonly used at drinking water and wastewater systems.

My statement today discusses the cybersecurity challenges facing the water sector and EPA's efforts to address the sector's cybersecurity risks, including efforts to address our August 2024 cybersecurity-related recommendations.[2] To review the status of these efforts, we relied on prior GAO reports, information provided by EPA in response to our recommendations, and publicly available information, as of May 2026, regarding cybersecurity challenges and EPA actions.

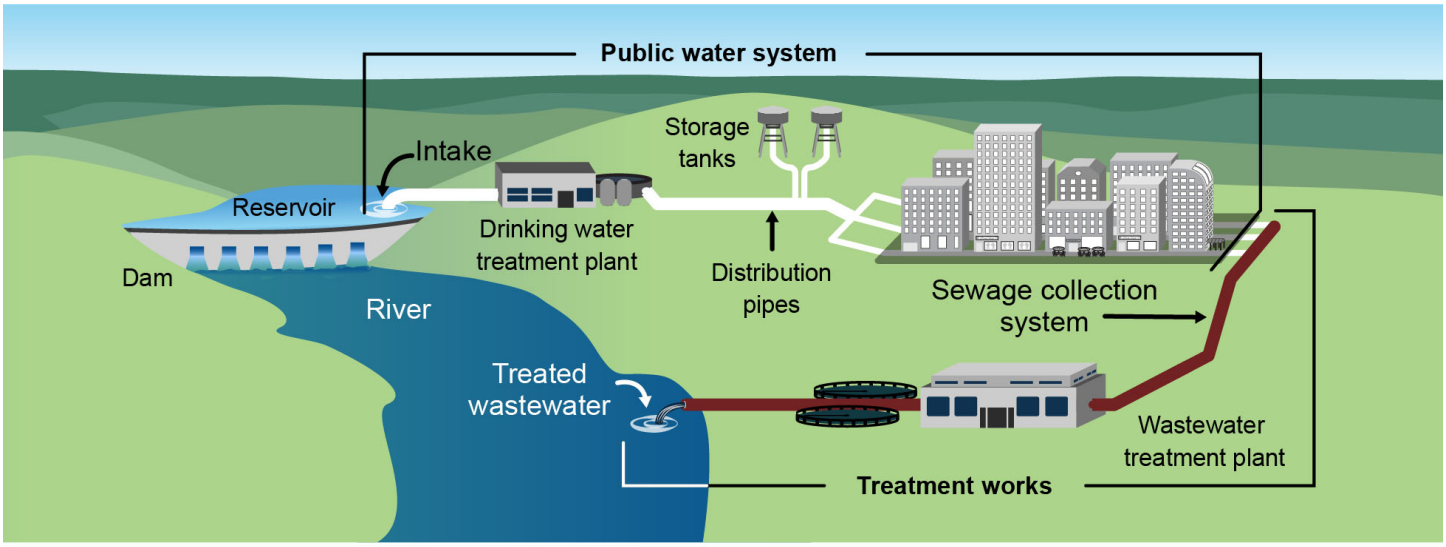
We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Water and wastewater infrastructure is often widely dispersed, covering large geographic areas of piped distribution and collection networks connected to centralized treatment facilities (see fig. 1).

[2]GAO, *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744 (Washington, D.C.: Aug. 1, 2024).

Figure 1: Water and Wastewater Sector Infrastructure



Sources: U.S. Environmental Protection Agency and Department of Homeland Security (information); GAO (graphic). | GAO-26-109159

Most water and wastewater facilities rely on operational technology systems and IT systems to function.[3] Operational technology systems provide remote and automated controls of valves, pumps, and other physical elements to treat, store, distribute, and monitor water for contaminants, among other functions. For example, operational technology systems can monitor water levels in different tanks and can turn pumps on or off to move water through pipes, add chemicals, adjust water pressure, or conduct similar functions.

Water and wastewater facilities can use IT systems to link operational monitoring and control systems at the facility. This connectivity can provide facility operators with remote control of water treatment or distribution, which can be helpful for managing large and widely distributed water and sewer systems. Water and wastewater facilities can also have business IT systems, which include customer billing, email, and other internet-based applications and tools.

The increased connections between operational technologies and internet-enabled devices, along with increased automation and remote

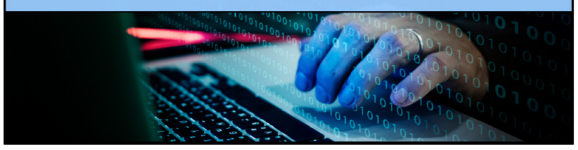
[3]Operational technology systems are programmable systems and devices that interact with or manage devices that interact with the physical environment. National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, Special Publication 800-82, Rev. 3 (Gaithersburg, Md.: September 2023).

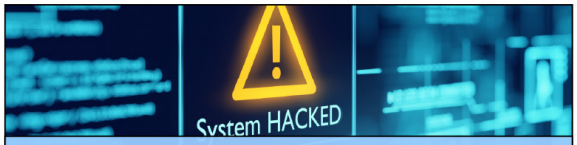
The increased connections between operational technologies and internet-enabled devices, along with increased automation and remote access capabilities, have made water and wastewater systems more vulnerable to cyberattacks. Specifically, operational systems that were previously isolated from the internet and from business IT systems have become increasingly connected with those systems, both within and outside the organization. This convergence increases the ability of online attackers to reach critical operational systems (see fig. 2).

Figure 2: Example of Water and Wastewater System Vulnerability to Cyberattack

Water systems may contain hundreds of diverse components, making it difficult to properly map and keep operational technologies updated with security patches.

Attackers may use IT networks to steal data or to move within the network to access operational systems.





IT and operational networks may not be properly separated, allowing attackers to access the operational systems and disrupt critical processes.

Sources: Cybersecurity and Infrastructure Security Agency (information); ungvar/Rawpixel/เฉิศลักษณ์ ทิพชัย/James Thew/stock.adobe.com (photos). | GAO-26-109159

Threat actors, such as state-sponsored hackers or criminal groups, are also increasingly capable of carrying out cyberattacks on water and wastewater systems. Although national-level reporting requirements for cyber incidents remain under development and the full scope of incidents is currently unknown, a number of known cybersecurity incidents in the U.S. over the past several years have disrupted water and wastewater system operations. Future incidents could have serious consequences including financial loss, drinking water contamination, and environmental pollution. Disruptions to the water supply could also affect the critical

infrastructure that depends on water, including hospitals—which are dependent on water for patient care—and energy production—which relies on water for steam generation and cooling.

Protecting the cybersecurity of critical infrastructure has been part of GAO's High Risk List since 2003.[4] In September 2018, we issued an update to the High Risk List that identified actions that federal agencies needed to take to address cybersecurity challenges.[5] We later identified ensuring the nation's cybersecurity as one of nine high-risk areas that needed especially focused executive and congressional attention.[6] We continue to identify the cybersecurity of critical infrastructure as a component of the cybersecurity high-risk area, as reflected in our high-risk updates on major cybersecurity challenges.[7]

The federal government has taken some steps to address challenges in protecting the cybersecurity of critical infrastructure. For example, in April 2024, the White House issued the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), which describes the approach the federal government will take to strengthen U.S. critical infrastructure resilience. Among other actions, the memorandum requires the Secretary of Homeland Security to develop a biennial National Risk Management Plan. This plan is to summarize U.S. government efforts to manage risk to the nation's critical infrastructure. It also directs agencies

[4]We first designated information security as a government-wide high-risk area in 1997. In 2003, we expanded this area to include cyber critical infrastructure protection. See GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[5]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[6]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[7]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021); *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure*, GAO-23-106441 (Washington, D.C.: Feb. 7, 2023); *Cybersecurity High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231 (Washington, D.C.: June 2024).

to establish minimum security and resilience requirements within and across critical infrastructure.[8]

Water and Wastewater Systems Face Challenges Reducing Their Vulnerability to Cyber Attacks

In our August 2024 report, we found that water and wastewater systems faced challenges reducing their vulnerability to cyberattacks. These challenges included addressing varying levels of cybersecurity capabilities and focus, managing workforce shortages, maintaining legacy systems that are difficult to update with cybersecurity protections, and prioritizing limited resources. For example, a lack of basic cyber hygiene—actions to improve online security such as changing default passwords and keeping operating systems up to date—was a significant challenge for water and wastewater systems, according to CISA regional staff we interviewed.[9]

A January 2025 water sector cybersecurity task force report echoed these challenges.[10] For example, the task force reported that many water and wastewater systems were designed before today's heightened cyber risk environment. Aging operational technology systems are often incompatible with modern IT security protocols, and upgrades would require capital investments that may be out of reach for lower-capacity water and wastewater systems. Additionally, other imperatives, like meeting regulatory requirements for clean and safe water, can out-compete cybersecurity for attention and budgetary resources.

[8]Executive Order 14239, *Achieving Efficiency Through State and Local Preparedness* (March 18, 2025), directs the Assistant to the President for National Security Affairs, in coordination with the Director of the Office of Science and Technology Policy and the heads of relevant agencies, to conduct a review of critical infrastructure policies, including NSM-22, and recommend to the President necessary revisions, recissions, and replacements necessary to achieve a more resilient posture; shift from an all-hazards approach to a risk-informed approach; move beyond information sharing to action; and implement the National Resilience Strategy. The review was to be completed within 180 days from the date of the executive order, but as of May 2026, no modifications have been publicly proposed or issued.

[9]GAO-24-106744.

[10]Water Sector Cybersecurity Task Force, *Securing the Future of Water: Addressing Cyber Threats Today* (Jan. 2025).

EPA Has Actions Underway to Address Water Sector Cybersecurity Risks, but More Work Remains

We reported in August 2024 that EPA had not conducted a comprehensive assessment of the water sector's cybersecurity risk or used a risk-informed strategy to guide its actions, which our past work has shown is essential for better managing federal programs and activities.[11] We recommended EPA conduct a water sector risk assessment, considering physical security and cybersecurity threats, vulnerabilities, and consequences. We also recommended EPA develop and implement a risk-informed cybersecurity strategy to guide its water sector cybersecurity programs. We stated that such a strategy should include information from a risk assessment and identify objectives, activities, and performance measures; roles, responsibilities, and coordination; and needed resources and investments.

In January 2025, EPA addressed our recommendations by issuing a sector-specific risk assessment and risk management plan. The risk assessment evaluated physical security and cybersecurity threats aligned with the threat categories identified in EPA's 2024 *Roadmap to a Secure and Resilient Water and Wastewater Sector*, which EPA coordinated with the water sector to develop.[12] EPA's risk assessment and risk management plan identified gaps in the water sector's existing risk management practices and recommended corresponding lines of effort to mitigate priority risks.

The initial version of the plan provided a broad, qualitative assessment of measures of success. For future iterations of the plan, EPA stated that it intends to work with sector partners to identify quantifiable measures of success coupled with strategies to assess progress against those measures. These strategies could include efforts by private sector partners or EPA to gather voluntary information from water and wastewater systems. We determined that these recommendations to EPA have been implemented. These actions should help EPA direct its programs and resources to effectively address the sector's cybersecurity risks.

[11]GAO-24-106744.

[12]Water and Wastewater Sector Strategic Roadmap Work Group, *Roadmap to a Secure and Resilient Water and Wastewater Sector*, EPA 810-R-24-002 (January 2024). The roadmap identified six categories of threats affecting the water sector, including supply chain risk management, extreme weather and natural disasters, physical and workforce security, contamination incidents, infrastructure degradation, and cybersecurity and cyber risk management.

However, the extent to which EPA's efforts will ultimately improve the sector's cybersecurity preparedness and resilience is yet to be determined. For one, efforts to improve water sector cybersecurity are voluntary and based on a partnership among EPA, CISA, other federal agencies, utilities, and sector associations. EPA's strategy builds on this partnership and relies on it to continue. But proposed reductions to key CISA programs may limit the federal government's ability to support water and wastewater systems in their efforts to conduct vulnerability assessments, engage in resilience planning, and access risk-management support.[13]

We also reported in 2024 that EPA's efforts to ensure water and wastewater entities take action to improve their cybersecurity had faced legal and other challenges.[14] As a result, we recommended EPA evaluate the sufficiency of its existing legal authorities for carrying out its cybersecurity responsibilities. In response, EPA identified several critical gaps affecting wastewater and small drinking water systems. Specifically, EPA identified a lack of cybersecurity risk assessment requirements for these systems, among other issues. EPA also identified significant limitations in its authority under federal drinking water and clean water laws to address those gaps. We will continue to monitor EPA's plans to address these limitations to its statutory authority, as well as EPA's efforts to use its existing authority to mitigate the critical gaps it identified. Such actions by EPA can help ensure the water sector is better prepared for any future cyberattacks.

As work continues on this important effort, it is vital that EPA—in partnership with CISA and its other state, local, and private sector entities—continue to target its efforts to most effectively address the persistent cybersecurity risks facing the water sector. For a sector as large and decentralized as the water sector, a risk-informed strategy is essential. And while a strategy can help identify and prioritize assets, justify and target resources, and aid in the development of performance measures, enduring success will depend on the extent to which key

[13]The Department of Homeland Security's fiscal year 2027 budget request for infrastructure assessments and related security efforts is about fifty eight percent of its fiscal year 2026 level. Similarly, its budget request for CISA's stakeholder engagement efforts, which includes coordinating with Sector Risk Management Agencies and providing technical assistance to public and private owners and operators responsible for the nation's critical infrastructure, is about 65 percent less than its fiscal year 2026 level.

[14]GAO-24-106744.

federal agencies can provide sustained support to the sector as owners and operators seek to reduce cybersecurity-related risk.

Chairman Franklin, Ranking Member Amo, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions you might have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact David B. Hinchman, Director of Information Technology and Cybersecurity, at hinchmand@gao.gov or J. Alfredo Gómez, Director, Natural Resources and Environment, at gomezj@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Michael Gilmore (Assistant Director), Susan Iott (Assistant Director), Charlotte Gamble (Analyst in Charge), Jillian Clouse, Kavita Daitnarayan, Scott Pettis, and Linda Tsang.