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.