GAO Highlights

Highlights of GAO-24-106744, a report to congressional requesters

August 2024

CRITICAL INFRASTRUCTURE PROTECTION

EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems

Why GAO Did This Study

Recent cyber incidents highlight the vulnerability of the 170,000 water and wastewater systems in the U.S. water sector. EPA is responsible for leading, coordinating, and supporting activities to reduce cybersecurity risk to the water sector. The agency works in partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and other federal, state, and local entities.

GAO was asked to review cybersecurity threats facing the water sector and the federal government's efforts to address these threats. This report (1) describes cybersecurity risks and incidents; (2) examines actions by selected federal and nonfederal entities to improve cybersecurity; and (3) evaluates EPA's actions to address known risks.

GAO analyzed documents from EPA, CISA, and other entities on cyber threats, threat actors, and sector efforts to reduce risk. GAO interviewed federal and nonfederal officials with relevant cybersecurity responsibilities. GAO also visited and interviewed officials from large and small systems selected to provide varying perspectives.

What GAO Recommends

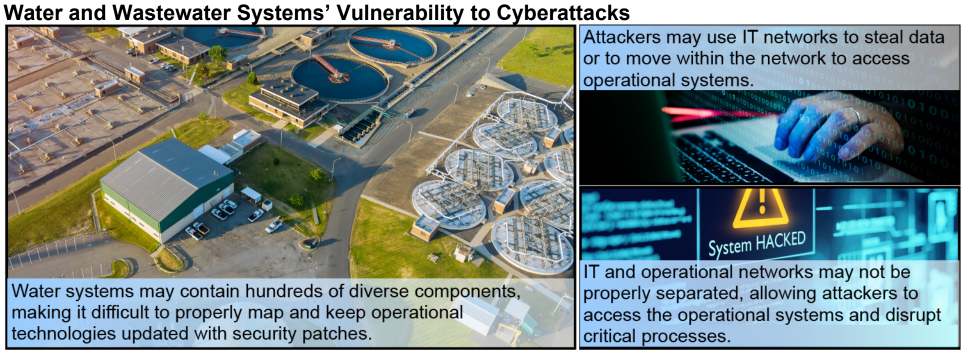
GAO is making four recommendations, including that EPA assess sector risk; develop and implement a national cybersecurity strategy; and evaluate the sufficiency of its legal authorities to carry out its cybersecurity responsibilities and seek additional authority as necessary. EPA concurred with the recommendations and said it is taking action to complete them.

View GAO-24-106744. For more information, contact J. Alfredo Gómez at (202) 512-3841 or gomezj@gao.gov, or David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov

What GAO Found

The water sector faces increasing cybersecurity-related risk. While national reporting requirements for cyber incidents are being developed, known incidents have disrupted water sector operations. Nations (including Iran and China), cybercriminals, and others have targeted water systems. For example, foreign hackers targeted multiple water systems in late 2023. Cyberattacks threaten public health, the environment, and other critical infrastructure sectors.

Water and Wastewater Systems' Vulnerability to Cyberattacks



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

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

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-24-106744

Federal agencies and other entities have acted to improve water sector cybersecurity, but reported challenges such as workforce skills gaps and older technologies that are difficult to update with cybersecurity protections. Further, the sector has made limited investments in cybersecurity protections because water systems prioritize funding to meet regulatory requirements for clean and safe water, while improving cybersecurity is voluntary. In a May 2024 alert, the Environmental Protection Agency (EPA) said it planned to increase enforcement activities to ensure drinking water systems address cybersecurity threats.

EPA has assessed aspects of cybersecurity risk but has not conducted a comprehensive sector-wide risk assessment or developed and used a risk-informed strategy to guide its actions. EPA is required by law, as well as National Security Memorandum 22 (NSM-22), to identify, assess, and prioritize water sector risk. EPA official said they have assessed threats, vulnerabilities, and consequences, but have not integrated this work in a comprehensive assessment. Without a risk assessment and strategy to guide its efforts, EPA has limited assurance its efforts address the highest risks.

EPA has faced challenges using its existing legal authority and voluntary approaches to manage cybersecurity risks but has not fully evaluated either approach. In March 2023, EPA interpreted existing legal requirements to include cybersecurity assessments at drinking water systems but withdrew the requirement 7 months later after facing legal challenges. Previous requirements and NSM-22 direct EPA to identify the authorities it needs to compel the sector to address risks. In July 2024, EPA officials said they had evaluated their authorities and would release the evaluation in 2025 with their risk assessment and strategy. Doing so and seeking additional authority as necessary can help EPA ensure the water sector is better prepared for any future cyberattacks.