Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

July 2026 Water System Cyber Incidents: Considerations for Congress

August 27, 2026

Reports of cyberattacks on water systems in at least seven states in July 2026 have increased attention on the security of the nation's municipal water infrastructure. These and other cyber incidents have raised questions about the effectiveness of existing approaches to address water sector cybersecurity. Municipal water systems and wastewater systems are paired together as a type of critical infrastructure (CI) covered by broader efforts to improve CI security. Executive Order 13636 designated the U.S. Environmental Protection Agency (EPA) as the sector risk management agency (SRMA) for water sector cybersecurity.

Federal efforts to address the cybersecurity of the water sector have primarily focused on drinking water systems rather than wastewater systems. Authorized through the Safe Drinking Water Act (SDWA), these federal efforts have generally involved specific vulnerability assessment requirements for larger drinking water systems and technical and financial assistance for smaller systems. This In Focus discusses EPA efforts under SDWA to address cybersecurity. It does not include information on Cybersecurity and Infrastructure Security Agency (CISA) authorities or EPA's SRMA role.

Regulated Water Systems

SDWA applies to the nearly 144,000 privately and publicly owned *public water systems*, which provide piped water to at least 15 service connections or that regularly serve at least 25 people. Nearly 49,500 of these regulated public water systems (35%) are *community water systems*, which serve the same residences year-round. These systems provide water to more than 324 million people. EPA defines 81% of community water systems as "small," serving 3,300 or fewer individuals. These systems provide water to 7% of the total population served by community water systems. Less than 10% of community water systems serve populations of 10,000 or more, but these larger systems provide water to 84% of community water system customers.

SDWA Assessments and Response Plans

In 2002, Congress amended SDWA to require community water systems serving more than 3,300 individuals to assess risks that could disrupt the provision of a safe and reliable water supply and prepare plans to address such risks. In 2018, the America's Water Infrastructure Act (AWIA; P.L. 115-270) revised SDWA Section 1433 to require such systems to conduct risk-and-resilience assessments and to prepare emergency response plans. These water systems are required to assess their vulnerabilities to malevolent acts (and natural hazards). In their assessments, systems are required to evaluate the resilience of their infrastructure, including "electronic, computer, or other automated systems (including the security of such systems)," as well as their financial capacity to respond to these risks. Based on their assessments, community water systems must develop emergency response plans that address the risk-and-resilience issues their systems may face. Community water systems must self-certify their assessments and submit the certifications to EPA by deadlines determined by water system size. Every five years, SDWA requires water systems to review, and, if needed, revise their assessments, and resubmit their self-certifications to EPA. Risk-and-resilience assessments and emergency response plans are voluntary for small water systems.

SDWA Cybersecurity Assistance Programs

AWIA also added SDWA Section 1433(g), which authorizes technical assistance (TA) for community water systems of all sizes, and supports plans or projects to increase resiliency for small community water systems. In 2021, the Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58) added SDWA Section 1459F, which directs EPA to establish a grant program for water systems serving 10,000 or more individuals to improve resilience to natural hazards and to reduce cybersecurity vulnerabilities. IIJA also reauthorized appropriations for SDWA Section 1442(b), which authorizes EPA to provide TA and make grants to states and public water systems to assist in responding to emergency situations. IIJA also amended SDWA Section 1442(b) to include cybersecurity events as an emergency situation. IIJA added SDWA Section 1459G, which authorizes a grant program for advanced technologies, including those that address cybersecurity. It also added SDWA Section 1420A, which requires EPA, with CISA, to develop a framework to identify water systems that, if degraded or rendered inoperable because of an incident, would lead to significant impacts. It requires EPA and CISA to develop a water system "Technical Cybersecurity Support Plan."

Selected Implementation Issues

Reported cyberattacks on water systems have raised questions about the effectiveness of the sector's approach to cybersecurity. SDWA Section 1433 requirements are targeted to systems serving a larger number of individuals because, if disrupted, the public health impact would be larger. Also, these larger systems benefit from economies of scale, resulting in greater capacity to update technology, adopt practices, or hire security specialists. SDWA assessments and plans are voluntary for smaller systems.

Some have raised concerns about SDWA Section 1433 compliance and the quality of larger systems' vulnerability assessments and emergency response plans. A 2024 EPA enforcement notice indicated that larger systems were experiencing compliance challenges, stating that more than "70% of systems inspected by EPA since September 2023 are in violation of basic SDWA Section 1433 requirements." Between 2020 and 2024, EPA conducted at least 100 enforcement actions due to violations of SDWA Section 1433. Also in 2024, EPA's Office of Inspector General (OIG) conducted a cybersecurity assessment of 1,062 water systems that serve 50,000 or more

individuals. Of the 1,062 systems, OIG "identified 97 … water systems serving approximately 26.6 million users as having either critical or high-risk cybersecurity vulnerabilities."

Others have questioned EPA's use of its SDWA authorities to address cybersecurity. For example, in March 2023, EPA issued an interpretive memorandum to require states, as a part of their SDWA primary enforcement responsibilities, to evaluate water system operational technology cybersecurity during triennial inspections, called "sanitary surveys." Sanitary surveys are on-site inspections of a water system's components (e.g., treatment technologies) and operational functions. Stakeholders filed a petition for judicial review, arguing that EPA did not follow the Administrative Procedure Act when issuing the memorandum and that EPA's expansion of the sanitary survey exceeded its statutory authority under SDWA. In October 2023, EPA rescinded the interpretive memorandum and its requirements.

Legislation in the 119th Congress

In the 119th Congress, some Members have introduced legislation regarding water sector cybersecurity. The Water Resources Development Act of 2026 (S. 4949), for example, includes several cybersecurity provisions. S. 4949 would

- reauthorize appropriations for SDWA Section 1459F;
- revise an existing SDWA small and disadvantaged communities grant program to make "reducing cybersecurity vulnerabilities" an eligible funding activity;
- amend an existing water infrastructure workforce grant program to include support for cybersecurity training;
- authorize a wastewater cybersecurity grant program;
- authorize a digital infrastructure grant program; and
- direct EPA to establish, subject to appropriations, a program to support participation in the Water Information Sharing and Analysis Center (WaterISAC), and to report on water sector cybersecurity within three years of enactment.

Other bills have water sector cybersecurity as their primary focus. These bills use different approaches, such as

- authorizing new grant programs (e.g., H.R. 2109/S. 1018, H.R. 9776/S. 3967, H.R. 2344/S. 1118);
- reauthorizing appropriations for existing authorities (e.g., H.R. 10083, S. 1549);
- reauthorizing appropriations for SDWA Section 1442(b) and authorizing a wastewater grant program (e.g., H.R. 9690/S. 4980);
- revising SDWA Section 1433 vulnerability assessment requirements for water systems, expanding oversight of water system vulnerability assessments, and adding similar wastewater requirements (e.g., S. 5368); and
- establishing a new framework to require systems to adopt cybersecurity standards developed and enforced by an independent organization (e.g., H.R. 2594).

Considerations for Congress

Members may consider several issues regarding water sector cybersecurity. In the 119th Congress, several bills propose to add cybersecurity grant programs for specific types of systems (e.g., rural) or to reauthorize appropriations for existing TA and/or grant programs. One consideration is whether new programs would be additive to or duplicative of existing ones. Another is whether existing programs are receiving appropriations. Congress has not specified appropriations for cybersecurity TA and grants under SDWA Section 1433(g) or the advanced technology grants under SDWA Section 1459G. Congress has provided appropriations for SDWA Section 1442(b) emergency assistance to address the Jackson, MS, water crisis and damage from Hurricanes Helene and Milton. In addition, Congress began funding resiliency grants for larger systems under SDWA Section 1459F in FY2023.

Other considerations may involve revising SDWA Section 1433 risk-and-resilience assessments and emergency response planning to include specific standards. In prior Congresses, some bills (e.g., H.R. 3258 in the 111th Congress) proposed a similar approach but were not enacted. Considerations for this approach could include how these standards would affect systems that face challenges in meeting the existing requirements. Another potential consideration involves EPA's or a state's ability to develop or oversee standards, as some have questioned whether water system expertise extends to cybersecurity expertise.

Another consideration relates to the risks of sharing water systems' vulnerability information with entities tasked with overseeing or supporting cybersecurity. Proposals to require water systems to transmit vulnerability assessments to EPA, states, or an independent organization to check compliance with certain standards may risk creating a repository of water system vulnerabilities that could be targeted for a cyberattack. Similarly, ensuring the cybersecurity of third-party entities that provide TA to specific water systems may be another consideration for proposals to expand TA.

Policymakers are considering a proposal to establish an independent organization to set cybersecurity standards for adoption by water systems. Several water associations support this approach. Under this proposal, EPA would retain oversight of the standard-setting organization, similarly to how the Federal Energy Regulatory Commission (FERC) oversees cybersecurity standards developed by the North American Electric Reliability Corporation (NERC) in the electricity sector. Policymakers assessing this approach may consider the differences between the electricity and water sectors, such as interconnectedness. Local electricity distribution systems connect to a larger transmission network, so an attack on transmission could affect several states. NERC standards apply to the interconnected network. Water systems generally are not interconnected, so any disruption from an attack would be limited to a community rather than affecting water service in several states. Although water systems are not interconnected at the state level, the effect of an attack (e.g., water contamination) could be significant, as some systems serve millions of people.

Elena H. Humphreys, Specialist in Environmental Policy

IF13298

Disclaimer