Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity of the Municipal Water Sector: Background and Issues for Congress

June 3, 2025

Congressional Research Service
https://crsreports.congress.gov
R48556

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48556

June 3, 2025

Elena H. Humphreys, Coordinator
Analyst in Environmental Policy

Brian E. Humphreys
Analyst in Science and Technology Policy

Cybersecurity of the Municipal Water Sector: Background and Issues for Congress

Cyberattacks pose a threat to the more than 324 million individuals in the United States who regularly receive water from water systems. These cyberattacks include incidents where an adversary manipulates a system's operational technology, which could result in the disruption of potable water supplies or in damage to physical infrastructure. Local drinking water systems are considered a type of *critical infrastructure* (CI), and such systems have been included in broader federal efforts to improve CI cybersecurity. Wastewater systems are grouped with water systems as a type of CI. Water and wastewater systems are a potentially attractive target for cyberattacks, as such systems provide "lifeline" services but may lack resources or technical capacity to adopt stringent cybersecurity practices. Since at least 2002, Congress and the executive branch have taken steps to improve the U.S. municipal water sector's resilience to malicious acts, such as cyberattacks. Congressional attention to water system cybersecurity, including deliberations related to the efficacy and efficiency of federal efforts, has continued in the 119th Congress.

Federal efforts to address water system cybersecurity generally have involved requirements for larger systems and technical and financial assistance for smaller systems. In 2002, Congress first amended the Safe Drinking Water Act (SDWA; codified at 42 U.S.C. §§300f et seq.) 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 these provisions to require such systems to conduct risk-and-resilience assessments. These water systems are required to assess their vulnerabilities to natural hazards in addition to malevolent acts. As a part of their assessment, systems are required to evaluate the resilience of their current physical infrastructure, including "electronic, computer, or other automated systems (including the security of such systems)" and their management practices, as well as their financial capacity to respond to these risks. Risk-and-resilience assessments and emergency response plans are voluntary for small water systems. Congress has established several SDWA assistance programs to support the development of systems that supply safe and reliable water, including cybersecurity improvements.

Key federal coordination authorities for CI security and resilience (CISR) policy date to the late 1990s. Some federal coordination authorities are subject to review under Executive Order 14239, announced on March 18, 2025. One of these is National Security Memorandum 22 (NSM-22), "Critical Infrastructure Security and Resilience," published in 2024. NSM-22 provides specific CISR policy guidance and designates 16 CI sectors, one of which is the "Water and Wastewater Systems" sector, for which the U.S. Environmental Protection Agency (EPA), as the Sector Risk Management Agency (SRMA), is delegated most coordination authorities. NSM-22 reaffirms the 16 CI sectors designated by earlier presidential directives and tasks federal agencies to provide CI risk assessments and plans for risk mitigation on an accelerated timeline. As a SRMA, EPA has undertaken a range of activities to support water systems' and wastewater systems' efforts to address cybersecurity threats. EPA's activities also have included providing technical assistance to water systems and providing cybersecurity assessments. In May 2025, EPA announced a reorganization of the agency's functions. EPA's announcement included that the agency will be "elevating issues of cybersecurity" and indicated that some of EPA's office roles may change.

Reported cyber incidents at water systems have raised questions about the adequacy of existing approaches to address water sector cybersecurity. Efforts to improve water sector cybersecurity generally center on addressing the resilience of individual water systems to such threats and/or addressing federal agency coordination in supporting water system cybersecurity. Several organizations have highlighted factors specific to the water sector that challenge the adoption of practices to mitigate the risk of cyberattacks. Others have questioned EPA's use of other SDWA authorities to address cybersecurity.

Congressional interest in water sector cybersecurity has continued in recent Congresses, with some Members proposing legislation taking various approaches to reduce cybersecurity risks. The 118th Congress held hearings and introduced legislation regarding water sector cybersecurity. In the 119th Congress, some Members have introduced a range of bills that propose adding programs (e.g., circuit rider programs targeted to rural systems) intended to improve cybersecurity or reauthorizing appropriations for existing technical and financial assistance programs. Other proposals seek to establish a different regulatory framework to address water sector cybersecurity. Approaches to improving water and wastewater system cybersecurity may vary depending on what threat they are addressing. Deliberations regarding these proposals raise a number of considerations for policymakers and stakeholders.

Contents

Tables

Appendixes

Contacts

Introduction

Cyberattacks pose a threat to the more than 324 million individuals in the United States who regularly receive water from water systems.[1] These cyberattacks could include ransomware attacks, which may result in a breach of customer or business data, or incidents where an adversary manipulates a system's operational technology, resulting in the disruption of potable water supplies or in damage to physical infrastructure. As the municipal water sector adopts internet-enabled technology to automate certain operations (e.g., the addition of chemicals for drinking water treatment), the sector is a potentially attractive target for cyberattacks, as water systems provide "lifeline" services but may lack resources or technical capacity to adopt stringent cybersecurity practices.[2] This may contribute to an increase in reported cyberattacks on the nation's water systems.

Since at least 2002, Congress has taken steps to improve the resilience of the U.S. municipal water sector to malicious acts, such as cyberattacks. Yet, over time, reported cyberattacks at water systems continue, leading to questions about the efficacy of the existing federal framework for addressing water system cybersecurity. In the 118th and the 119th Congresses, some Members have introduced legislation intended to address water system cybersecurity. Further, multiple Administrations have directed various federal agencies to take certain actions intended to improve the cybersecurity of U.S. critical infrastructure (CI).

Community water systems are considered a type of CI, and such systems have been included in broader federal efforts to improve CI cybersecurity. Wastewater systems are grouped with community water systems as a type of CI. This report focuses on water systems but contains some information on federal efforts to address wastewater system cybersecurity.[3]

Federal efforts to address water system cybersecurity generally have involved requirements for larger systems and technical and financial assistance for smaller systems. In 2018, to respond to cyberthreats, Congress revised requirements for water systems serving more than 3,300 individuals to assess vulnerabilities and create emergency response plans. In 2002, Congress first required water systems to assess their vulnerabilities to terrorist or other intentional acts and, on the basis of the assessment, prepare emergency response plans.[4] After first focusing on security, Congress expanded these Safe Drinking Water Act (SDWA) provisions in 2018 to address water system resilience to a range of risks, including natural hazards.

---

[1] U.S. Environmental Protection Agency (EPA), *Safe Drinking Water Information System (SDWIS): Water System Summary*, database accessed February 19, 2025, https://sdwis.epa.gov/ords/sfdw_pub/r/sfdw/sdwis_fed_reports_public/21?clear=RP,RIR. Selected parameters were "community water systems" and "active." EPA's website states that more than 90% of the U.S. population is served by a water system. For more details, see EPA, "How Does Your Water System Work?," January 27, 2025, https://www.epa.gov/ground-water-and-drinking-water/how-does-your-water-system-work-text-only#:~:text=EPA%2C%20states%2C%20and%20water%20utilities,stores%2C%20and%20distributes%20the%20water. Understanding the scale of the threat is a potential challenge to addressing water system cybersecurity.

[2] EPA Office of Inspector General (OIG), *Management Implication Report: Cybersecurity Concerns Relate to Drinking Water Systems*, 25-N-0004, November 13, 2024, https://www.epaoig.gov/sites/default/files/reports/2024-12/Full%20Report%2025-N-0004_Errata.pdf.

[3] This report does not contain information about federally owned water infrastructure and cybersecurity issues. For more information about federal dam safety, see CRS Report R45981, *Dam Safety Overview and the Federal Role*, by Anna E. Normand, particularly the section titled "Efforts to Address Cybersecurity Risks."

[4] Safe Drinking Water Act (SDWA) Section 1433 added by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Preparedness Act; P.L. 107-188, Title IV).

In 2021, a cyberattack in which a hacker attempted to pump dangerous amounts of lye into a water system in Oldsmar, Florida, garnered national attention.[5] In the intervening years, several other cyberthreats resulted in concerns about the security of water systems. As cyberattacks on such systems continue to receive national attention, stakeholders have questioned these requirements' implementation and/or adequacy. In 2024, the U.S. Environmental Protection Agency (EPA) identified "alarming cybersecurity vulnerabilities at drinking water systems across the country."[6] For example, EPA identified instances where water systems failed to change default passwords, used a single login ID for all staff, or failed to curtail access by former employees.[7] Also in 2024, the EPA's Office of Inspector General (OIG) identified "weaknesses with reporting" of cyber incidents at water systems,[8] meaning that additional attacks may go unreported or even unnoticed.

Further, a March 2025 executive order (E.O.) directed changes to existing federal CI security and resilience (CISR) policy, which includes public-private partnerships for CI cybersecurity. The March 2025 E.O. directs responsible officials and agencies to realign more responsibility for CI risk assessment and mitigation to state governments, among other provisions.

This report provides background on the federal role in U.S. water sector cybersecurity as a part of broader CISR improvement efforts, as well as an overview of efforts specifically targeted at improving water system cybersecurity. It also details requirements and authorized financial assistance intended to support the cybersecurity of water systems and surveys related congressional activity. It ends with considerations for policymakers.

Background on Water Systems and the Safe Drinking Water Act (SDWA)

To address intentional acts that may disrupt a safe and reliable water supply, Congress added several provisions to SDWA (codified at 42 U.S.C. §§300f et seq.) in 2002.[9] These provisions are described in this section. SDWA is the key federal law for protecting public water supplies; it applies to privately and publicly owned water systems that provide piped water for human consumption to at least 15 service connections or that regularly serve at least 25 people. To date, this includes approximately 143,000 regulated public water systems.[10] These water systems vary greatly in size and type, ranging from large municipal systems to systems operated by homeowner associations, schools, hospitals, and campgrounds.

[5] Frances Robles and Nicole Perlroth, "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," *New York Times*, February 8, 2021.

[6] EPA, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, June 6, 2024, https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

[7] EPA, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, June 6, 2024.

[8] EPA OIG, *Management Implication Report: Cybersecurity Concerns Relate to Drinking Water Systems.*

[9] Added to SDWA by the Bioterrorism Preparedness Act (P.L. 107-188, Title IV).

[10] Calculated by CRS based on EPA's *SDWIS: Water System Summary* report, generated on February 24, 2025. The search parameters were "public water systems." EPA has established three broad categories of public water systems. A community water system serves the same population year-round. A non-transient noncommunity water system regularly supplies water to at least 25 of the same people at least six months per year but not year-round (e.g., schools, factories, office buildings, and hospitals that have their own wells). Transient noncommunity water systems provide water in places where people do not remain for long periods, such as gas stations and campgrounds.

Nearly 49,500 of these regulated public water systems (34.5%) are *community water systems*, which serve the same residences year-round.[11] These systems provide water to more than 324 million people.[12] EPA defines most community water systems (80.6%) as "small," as they serve 3,300 or fewer individuals.[13] These small systems provide water to just 7.3% of the total population served by community water systems. In contrast, less than 9.2% of community water systems serve populations of 10,000 or more, but these larger systems provide water to 83.7% of the population served (nearly 272 million individuals).

SDWA Water System Security Provisions[14]

In 2002, Congress first required community water systems to assess risks that could disrupt the provision of a safe and reliable water supply and prepare plans to address such risks. Added by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Preparedness Act of 2002; P.L. 107-188, Title IV), SDWA Section 1433 required community water systems to (1) assess their vulnerabilities to terrorist attacks or other intentional acts intended to disrupt water service, (2) submit vulnerability assessments to EPA, and (3) develop emergency response plans based on their assessments.[15] The act directed EPA to provide guidance to small systems (serving fewer than 3,300 people) on how to conduct vulnerability assessments, prepare emergency response plans, and address threats. As initially added to SDWA, Section 1433 did not require community water systems to update their assessments.

In 2018, the America's Water Infrastructure Act (AWIA; P.L. 115-270) revised Section 1433 to require community water systems serving more than 3,300 people to conduct risk-and-resilience assessments. Under the revised section, such water systems are required to assess their vulnerabilities to natural hazards in addition to malevolent acts. As a part of their assessment, community water systems are required to evaluate the resilience of their current physical infrastructure, including "electronic, computer, or other automated systems (including the security of such systems)" and their management practices, as well as their financial capacity to respond to these risks.

For purposes of Section 1433, *resilience* is defined as "the ability of a community water system ... to adapt to or withstand the effects of a malevolent act or natural hazard without interruption to the ... system's function, or if the function is interrupted, to rapidly return to a normal operating condition."[16] According to the statute, on the basis of their assessments, community water systems must develop emergency response plans that address the risk-and-resilience issues that systems may face. Community water systems must self-certify their assessments and submit the certifications to EPA by deadlines specific to their communities' size.[17] Every five years, SDWA

[11] Calculated by CRS based on EPA's *SDWIS: Water System Summary* report, generated on February 24, 2025. The search parameters were "community water systems."

[12] Calculated by CRS based on EPA's *SDWIS: Water System Summary* report, generated on February 24, 2025. The search parameters were "community water systems."

[13] SDWA Section 1433(e) stipulates that EPA is required to provide guidance to "small public water systems" that serve less than 3,300 individuals.

[14] For more information about SDWA water system security and resilience provisions, see CRS In Focus IF11777, *Safe Drinking Water Act (SDWA): Water System Security and Resilience Provisions*, by Elena H. Humphreys.

[15] 42 U.S.C. §300i-2.

[16] 42 U.S.C. §300i-2(h).

[17] SDWA Section 1433(a)(3) (42 U.S.C. §300i-2(a)(3)) required community water systems to certify their assessments by different deadlines depending on how many people they served: systems serving 100,000 or more individuals had to certify by March 31, 2020; systems serving between 50,000 and 99,999 individuals had to certify by December 31, (continued...)

requires water systems to review their assessments, revise them if needed, and resubmit their self-certification to EPA.[18]

Risk-and-resilience assessments and emergency response plans are voluntary for small water systems (i.e., those that serve 3,300 or fewer individuals). AWIA amended SDWA to authorize appropriations of $10 million for each of FY2020 and FY2021 for grants to public water systems serving fewer than 3,300 people and grants to nonprofit organizations to support risk assessment and response planning activities.[19] Similar to P.L. 107-188, AWIA requires EPA to provide guidance and technical assistance to small water systems regarding how to conduct resilience assessments, prepare emergency response plans, and address threats from natural hazards and malevolent acts.[20]

Between 2020 and 2024, EPA reports that it took at least 100 enforcement actions against community water systems for violating SDWA Section 1433 (discussed in "Implementation of SDWA Requirements").[21] EPA's enforcement actions apply to the almost 9,600 community water systems serving more than 3,300 people. These 9,600 systems comprise roughly 19% of the total number of community water systems, though they serve almost 93% of the total number of individuals who receive water from community water systems.

In addition, the Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58) amended SDWA to add Section 1420A, which requires EPA, in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), to develop a framework to identify water systems that, if degraded or rendered inoperable because of an incident, would lead to significant public health and safety impacts and requires EPA and CISA to develop a plan to support water systems. Pursuant to Section 1420A, EPA published a prioritization framework in May 2022 and a technical cybersecurity support plan in August 2022.[22] EPA's technical cybersecurity support plan outlines EPA's and CISA's current offering of cybersecurity services, such as self- or facilitated cybersecurity assessments, and outlines planned future support for systems (e.g., a checklist of cybersecurity best practices and a "standing service" for cybersecurity support).[23]

SDWA Water Security Financial Assistance

Congress has established several SDWA financial assistance programs to support the development of systems that supply safe and reliable water, including to improve their resilience to cyberattacks. These are discussed below.

2020; and systems serving between 3,300 and 49,999 individuals had to certify by June 30, 2021. Community water systems were required to develop emergency response plans within six months of their certification due dates.

[18] 42 U.S.C. §300i-2(a)(3)(B).

[19] 42 U.S.C. §300i-2(g).

[20] 42 U.S.C. §300i-2(e).

[21] EPA, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, June 6, 2024.

[22] EPA, *Prioritization Framework for Technical Cybersecurity Support to Public Water Systems—Report to Congress*, EPA 817-R-22-001, May 2022, https://www.epa.gov/system/files/documents/2022-08/Prioritization%20Framework%20RtC%20final.pdf; and EPA, *Technical Cybersecurity Support Plan for Public Water Systems—Report to Congress*, EPA 817-R-22-002, August 2022, https://www.epa.gov/system/files/documents/2022-08/9910_RtC-Technical%20Cybersecurity%20Support%20Plan_20220818_final.pdf.

[23] EPA, *Technical Cybersecurity Support Plan for Public Water Systems—Report to Congress*, EPA 817-R-22-002, August 2022, https://www.epa.gov/system/files/documents/2022-08/9910_RtC-Technical%20Cybersecurity%20Support%20Plan_20220818_final.pdf.

Drinking Water State Revolving Fund (DWSRF)

Authorized by SDWA Section 1452, the DWSRF is the primary federal financial assistance program to help water systems finance infrastructure projects needed to comply with drinking water regulations and to meet health protection objectives.[24] The DWSRF provision authorizes states to receive annual capitalization grants from EPA to provide primarily subsidized loans to water systems for drinking water projects and related activities. The IIJA reauthorized appropriations for the DWSRF program. The authorization of appropriations for DWSRF capitalization grants are

- $2.40 billion for FY2022,
- $2.75 billion for FY2023,
- $3.00 billion for FY2024,
- $3.25 billion for each of FY2025 and FY2026.[25]

Congress provides appropriations for the DWSRF within EPA's state and tribal assistance grants (STAG) account within the Interior, Environment, and Related Agencies appropriations act. For FY2025, the Full-Year Continuing Appropriations and Extensions Act, 2025 (P.L. 119-4), provided $1.1 billion for the DWSRF.[26] In addition, the IIJA (P.L. 117-58) provided five fiscal years of supplemental appropriations (i.e., for each of FY2022 through FY2026) for the DWSRF. CRS Report R46892, *Infrastructure Investment and Jobs Act (IIJA): Drinking Water and Wastewater Infrastructure*, provides more information about these appropriations.

Each year, each state must match 20% of its annual capitalization grant and develop an intended-use plan (IUP) indicating how the allotted funds will be used. SDWA requires states to prioritize funding to projects that address the most serious human health risks, are necessary to ensure compliance with SDWA, and assist systems most in need on a per-household basis according to state affordability criteria. Over time, those systems repay the loan to the state fund. Together, the capitalization grant, state match, repayments, and leveraged funds were intended to be a sustainable source of financial assistance for drinking water infrastructure at the state level. EPA's guidance provides examples of types of DWSRF-eligible projects.[27] Infrastructure improvements for water system security or resilience are among the eligible projects listed in the guidance. These include projects that address "vulnerability of a water system to disruption of safe water delivery, whether natural or of human origin, [and] capability to recover from disruption of safe water delivery."

SDWA DWSRF provisions also direct or authorize states to set aside portions of their capitalization grants for specific purposes. These set-aside provisions provide states with flexibility to tailor their individual DWSRF program to address state priorities. SDWA authorizes a state to set aside portions of its capitalization grant for public water system capacity development and for strategy development and implementation. According to EPA DWSRF guidance, these activities may include "security inspections and exercises (including physical

[24] 42 U.S.C. §300j-12. For more information about the DWSRF program, see CRS Report R47935, *Changes to the Drinking Water State Revolving Fund (DWSRF) Program*.

[25] 42 U.S.C. §300j-12(m).

[26] For more information about recent appropriations for the DWSRF, see CRS In Focus IF12950, *U.S. Environmental Protection Agency (EPA) Water Infrastructure Programs and FY2025 Appropriations*.

[27] EPA, *Drinking Water State Revolving Fund Eligibility Handbook*, EPA 816-B-17-001, June 2017.

infrastructure and cybersecurity assessments)," which could be a part of efforts to "develop cybersecurity effective practices or measures."[28]

SDWA Grant Programs

To increase the resilience of public water systems, SDWA Section 1433(g) directed EPA to establish the Drinking Water Infrastructure Risk and Resilience Program and authorized appropriations of $25 million for each of FY2020 and FY2021 for EPA to make grants to community water systems to plan or implement projects to increase their system's resiliency.[29] Congress did not provide appropriations for this program.

SDWA Section 1442(b) authorizes EPA to provide technical assistance and make grants to states and public water systems to assist in responding to and alleviating emergency situations.[30] The Bioterrorism Preparedness Act amended SDWA Section 1442(d) to authorize appropriations for such emergency assistance of not more than $35 million for FY2002 and such sums as may be necessary for each fiscal year thereafter.[31] IIJA amended SDWA Section 1442(b) to specifically include cybersecurity events as an emergency situation.[32] IIJA also amended SDWA Section 1442(d) to reauthorize appropriations of $35 million for each of FY2022 through FY2026 for SDWA Section 1442(b). In the Consolidated Appropriations Act, 2023 (P.L. 117-328), Congress provided $150 million to SDWA Section 1442(b) to assist the water system serving the City of Jackson, Mississippi, in responding to an emergency situation that was not related to cybersecurity; Congress has not otherwise funded activities under SDWA Section 1442(b).

Added by the IIJA, SDWA Section 1459F 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.[33] To support these grants, SDWA Section 1459F authorizes appropriations of $50 million annually for FY2022 through FY2026. Under this provision, EPA is directed to use 50% of amounts available for grants for water systems serving between 10,000 and 100,000 individuals, and 50% for systems serving more than 100,000 individuals. Congress has not provided appropriations for this program.

SDWA Section 1459G requires EPA, subject to appropriations, to study technologies, including those used to address cybersecurity vulnerabilities, and requires EPA to establish a technology grant program to identify and/or deploy such technologies. Eligible entities for these grants include water systems serving 100,000 or fewer individuals, and small and disadvantaged water systems.[34] SDWA Section 1459G authorizes appropriations of $10 million annually for FY2022 through FY2026. Congress has not provided appropriations for this program.

Other Initiatives

Water systems have collaborated to take steps to address the security of the sector. To address water system technical capacity, industry associations established the Water Information Sharing

[28] SDWA §1452(g)(2)(B) and §1452(k)(2); 42 U.S.C. §300j-12(g)(2)(B) and §300j-12(k)(2). EPA, *Drinking Water State Revolving Fund Eligibility Handbook*, EPA 816-B-17-001, June 2017, p. 33. Time constraints prevented CRS from reviewing DWSRF annual reports from the states and Puerto Rico to calculate the total spent on such activities.

[29] 42 U.S.C. §300i-2(g).

[30] 42 U.S.C. §300j-1(b).

[31] 42 U.S.C. §300j-1(d).

[32] Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58, §50101).

[33] 42 U.S.C. §300j-19g.

[34] 42 U.S.C. §300j-19h.

and Analysis Center (WaterISAC) in 2002 in coordination with EPA. WaterISAC operates as an information hub to gather and promulgate relevant threat information to its members.[35]

Background on Critical Infrastructure Security and Resilience (CISR)

Key federal coordination authorities for CISR policy date to the late 1990s.[36] After the September 11, 2001, terrorist attacks, Congress passed the Homeland Security Act of 2002 (P.L. 107-296), which expanded certain coordination authorities first established under the Clinton Administration and added others. The Homeland Security Act created the Department of Homeland Security (DHS) as the lead agency for implementation of the new CISR coordination authorities. P.L. 107-296 authorizes the Secretary of Homeland Security (the Secretary) to create and manage private sector advisory councils, develop public-private partnerships, provide security-related services, and assist the private sector in development and promotion of best practices to secure CI.

As defined by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act; P.L. 107-56), CI refers to systems and assets for which "incapacity or destruction … would have a debilitating impact on security, national economic security, national public health or safety, or any combination" of them.[37] Presidential National Security Memorandum 22 (NSM-22), "Critical Infrastructure Security and Resilience," published in 2024, provides specific CISR policy guidance for federal agencies with infrastructure risk management responsibilities.[38]

National Security Memorandum 22 (NSM-22) and the Role of the U.S. Environmental Protection Agency (EPA)

Under NSM-22, CISA, a component of DHS, serves as National Coordinator for CISR. NSM-22 reaffirms all 16 CI sectors—including the Water and Wastewater Systems sector—established under previous directives that it supersedes. Under NSM-22, EPA remains the Sector Risk Management Agency (SRMA) for the Water and Wastewater Systems sector. SRMAs are federal agencies with sector-relevant responsibilities and expertise that coordinate federal risk management activities in a given sector. As with previous CI directives, NSM-22 supports existing public-private partnerships based on voluntary standards and best practices. In addition, NSM-22 directs agencies to establish minimum security and resilience requirements for CI, and to formulate requests for additional regulatory authorities to address regulatory gaps.[39] Further, it

[35] See Water Information Sharing and Analysis Center (WaterISAC), "The Security Network of the Water and Wastewater Sector," https://www.waterisac.org/about-us. Under SDWA, EPA is required to disseminate information to WaterISAC that it gathered from its review of methods for preventing, detecting, and responding to such disruptions and methods for providing alternative drinking water supplies if a water system is destroyed or impaired.

[36] Presidential Decision Directive 63 (PDD-63), "Critical Infrastructure Protection," May 22, 1998.

[37] 42 U.S.C. §5195c(e).

[38] Biden White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024, https://web.archive.org/web/20250118023435/https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/. CRS In Focus IF12716, *The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience*, by Brian E. Humphreys contains more details.

[39] Biden White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024.

directs SRMAs to identify "Systemically Important Entities" that could cause cascading infrastructure failures on a national scale in case of loss or disruption, and to provide CI risk assessments and plans for risk mitigation on an accelerated timeline.[40]

For the Water and Wastewater Systems sector, CISA delegates most coordination authorities to EPA as the designated SRMA. EPA serves as chair of the Government Coordinating Council (GCC)—an interagency coordination body that includes relevant federal agencies, certain state and local environmental or public health agencies, the Association of State Drinking Water Administrators, the National Association of Regulatory Utility Commissioners, and certain other organizations. Operators of water and wastewater systems are represented in the Water and Wastewater Systems Sector Coordinating Council (SCC)—a self-governed organization of nearly two dozen industry associations, utility operators, foundations, sanitation departments, and other similar entities.[41]

The water GCC and SCC have directed a workgroup to produce four strategic "roadmaps" for addressing the sector's security priorities.[42] Published in 2024, the fourth roadmap includes both near- and long-term cybersecurity-related priorities, which include the following:

- cybersecurity should be a consideration in all areas where technology is used,
- cybersecurity capacity must be developed at smaller systems, and
- cyber incident reporting should be promoted and understood.[43]

To achieve these objectives, the roadmap suggests near-term goals of maintaining and promoting basic cybersecurity practices, as well as moving beyond minimum cybersecurity practices, and developing cybersecurity policies and trainings to improve the sector's risk management.[44]

Potential Changes to Federal and State Government Roles

In March 2025, President Trump issued E.O. 14239, "Achieving Efficiency Through State and Local Preparedness," which requires "a review of all infrastructure, continuity, and preparedness policies to modernize and simplify federal approaches."[45] E.O. 14239 would place increased responsibility on the states to ensure CI resilience. It calls for state and local governments to take the lead in enacting "commonsense approaches and investments" in infrastructure resilience.

[40] For more information on NSM-22, see CRS In Focus IF12716, *The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience*, by Brian E. Humphreys.

[41] See CISA, "Water and Wastewater Systems Sector: Council Charters and Membership," https://www.cisa.gov/water-sector-council-charters-and-membership.

[42] The water sector coordinating council (SCC) also conducted a survey in 2021 of water and wastewater systems to better understand the sector's cybersecurity challenges and needs. Water Sector Coordinating Council, *Water and Wastewater Systems: Cybersecurity 2021 State of the Sector*, June 2021, https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf.

[43] 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, https://www.epa.gov/system/files/documents/2024-02/water-sector-roadmap-013024-508.pdf. Broader than cybersecurity, the roadmap identified other vulnerabilities such as supply chain risk management, extreme weather and natural disasters, physical and workforce safety, contamination incidents, and infrastructure degradation.

[44] Water and Wastewater Sector Strategic Roadmap Work Group, *Roadmap to a Secure and Resilient Water and Wastewater Sector*.

[45] White House, "Fact Sheet: President Donald J. Trump Achieves Efficiency Through State and Local Preparedness," March 18, 2025, https://www.whitehouse.gov/fact-sheets/2025/03/fact-sheet-president-donald-j-trump-achieves-efficiency-through-state-and-local-preparedness/.

E.O. 14239 directs the federal government to support such efforts by providing a National Risk Register to quantify "natural and malign risks to our national infrastructure, related systems, and their users" and by streamlining "overlapping and overbroad" policy guidance that might impede effective communication among federal, state, and local governments. The E.O. directs the Assistant to the President for National Security Affairs (APNSA) to complete a review of NSM-22 and certain other related directives within 180 days, and to recommend "revisions, recissions, and replacements necessary to achieve a more resilient posture."[46]

Further, the directive mandates a "shift from an all-hazards approach to a risk-informed approach" based on a review by APNSA of NSM-22 and other existing guidance.[47] The E.O. does not provide detailed explanation of how these approaches differ from one another. All-hazards approaches often incorporate risk assessments of event likelihood, asset vulnerability, and consequence of loss or disruption for purposes of prioritizing mitigation investments. According to a White House fact sheet on the E.O., risk-informed approaches prioritize "resilience and action over mere information sharing."[48]

Previous White House and agency guidance over several Administrations emphasized information sharing as a core element of risk assessment and awareness among relevant stakeholders. E.O. 14239 does not specify what specific forms "resilience and action" would take under new policy guidance.[49] The E.O. tasks APNSA with developing detailed revisions of existing CISR guidance and providing detailed new guidance to support implementation of a forthcoming National Resilience Strategy. The strategy is due to be completed within 90 days (i.e., by June 17, 2025).[50] This latter document would supersede the National Resilience Strategy published by the Biden Administration in January 2025.[51]

EPA Activities Within Federal CISR Efforts

As a SRMA, EPA has undertaken a range of activities to help water systems and wastewater systems address cybersecurity threats. EPA's role has primarily involved providing technical assistance to water systems intended to improve cybersecurity. In May 2025, EPA announced a reorganization of the agency's functions.[52] EPA's announcement included that the agency will be "elevating issues of cybersecurity," indicating that the EPA office roles outlined below may

[46] Executive Order (E.O.) 14239 of March 18, 2025, "Achieving Efficiency Through State and Local Preparedness," 90 *Federal Register* 13267, March 21, 2025, https://www.federalregister.gov/documents/2025/03/21/2025-04973/achieving-efficiency-through-state-and-local-preparedness.

[47] E.O. 14239, "Achieving Efficiency Through State and Local Preparedness," §3(b).

[48] White House, "Fact Sheet: President Donald J. Trump Achieves Efficiency Through State and Local Preparedness."

[49] White House, "Fact Sheet: President Donald J. Trump Achieves Efficiency Through State and Local Preparedness."

[50] E.O. 14239, "Achieving Efficiency Through State and Local Preparedness."

[51] White House, *National Resilience Strategy*, January 2025, https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/National-Resilience-Strategy.pdf.

[52] EPA, "EPA Announces Next Phase of Organizational Improvements to Better Integrate Science into Agency Offices, Deliver Clean Air, Land, and Water to All Americans," press release, May 2, 2025, https://www.epa.gov/newsreleases/epa-announces-next-phase-organizational-improvements-better-integrate-science-agency. Certain industry articles indicate that EPA's reorganization plan would result in the creation of the "Office of Water Cybersecurity and Infrastructure Resiliency." See, for example, "EPA Reorganization Plan Signals Shift in Science, Climate, and Water Programs," *Smart Water Magazine*, May 12, 2025.

change.[53] Given the uncertainty, this report discusses EPA's cybersecurity-related activities and roles as they were prior to the restructuring announcement.

EPA's Office of Homeland Security (OHS) has coordinated national and homeland security activities in several areas, including critical water infrastructure protection. OHS has worked with DHS, the U.S. Army Corps of Engineers (USACE), and the Intelligence Community on the development of new homeland and national security policies and requirements; OHS also has worked with EPA's water programs to address water security efforts.[54] While activities have been undertaken by OHS and other agencies, EPA reported in 2024 that "the federal government should adopt a more aggressive posture towards [water system] cybersecurity."[55]

In addition, EPA has implemented statutory and presidential directives relating to homeland security through its Water Infrastructure and Cyber Resilience program.[56] This program has provided technical assistance to water utilities, state officials, and federal emergency responders to become more resilient against a range of hazards, including cyberattacks, that may threaten the continuity of water and wastewater services. In addition, EPA's activities have included providing technical assistance to water utilities, such as through cybersecurity assessments.[57] Through its Water Technical Assistance (WaterTA) initiative, EPA has provided drinking water, wastewater, and stormwater utilities with trainings on water sector cybersecurity threats, vulnerabilities, consequences, best practices, resources, and program development. Under this initiative, EPA has made available confidential assessments and cybersecurity technical assistance to interested drinking water and wastewater utilities. The agency also has posted cybersecurity funding opportunities and various other resources intended to improve water sector cybersecurity.[58]

Cybersecurity and Infrastructure Security Agency (CISA) Activities

In addition to coordinating public-private partnerships under the NSM-22 framework, CISA has administered infrastructure protection programs and activities that support utilities and other CI owner-operators. Support has been available to any infrastructure owner-operator, but CISA has prioritized support for owner-operators in designated CI sectors. These programs and services have included—but have not been limited to—the Water and Wastewater Systems sector.

Cybersecurity Services

CISA has provided cybersecurity assessments, detection and prevention, information sharing and awareness, and training and career development services to CI owner-operators. Cybersecurity Advisors "act as liaisons to CISA cyber programs" and "provide cyber preparedness, assessments

[53] EPA, "EPA Announces Next Phase of Organizational Improvements to Better Integrate Science into Agency Offices, Deliver Clean Air, Land, and Water to All Americans."

[54] EPA, *Fiscal Year 2025 Justification of Appropriation Estimates for the Committees on Appropriations*, March 2024, p. 124-130.

[55] EPA, *Fiscal Year 2025 Justification of Appropriation Estimates for the Committees on Appropriations*, p. 128.

[56] EPA, *Fiscal Year 2025 Justification of Appropriation Estimates for the Committees on Appropriations.*

[57] In 2007, EPA's Water-Sector Specific Plans outlined an implementation strategy for drinking water and wastewater utilities, and others, to better prepare for and recover from terrorist attacks, other intentional acts, natural disasters, and other hazards. See EPA, *Water-Sector Specific Plan*, December 2007.

[58] For more information, see EPA, "EPA Cybersecurity for the Water Sector," accessed April 7, 2025, https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector.

and protective resources, strategic messaging, working group support and leadership, partnership in public-private development, and incident coordination and support in times of cyber threat, disruption, and attack."[59] Services have been offered through CISA regional offices.[60] CISA has also administered issue-specific cybersecurity initiatives relevant to the sector, including industrial control systems and supply chain risk management for information and communications technology.[61] In addition, CISA has also provided physical security assessments on a voluntary basis through its Protective Security Advisor program.[62]

Information Sharing

CISA has maintained operational incident reporting and information-sharing capabilities through its CISA Central hub, which "coordinates situational awareness and response to national cyber, communications, and physical incidents."[63] CISA may share relevant vulnerability and threat information directly with owner operators, or through designated Information Sharing and Analysis Centers (ISACs)—including WaterISAC.[64] In addition, CISA has administered the Protected Critical Infrastructure Information (PCII) Program, which implements Title 6, Section 673 of the *U.S. Code*, "Protection of Voluntarily Shared Critical Infrastructure Information." The PCII program has provided an avenue for CI owner-operators to share sensitive information on infrastructure-related vulnerabilities, threats and hazards, and incidents—including cyber—while maintaining confidentiality. Under statutory guidelines, CISA has shielded such information from disclosure under the Freedom of Information Act, from direct use in civil lawsuits, and from disclosure or use in certain other circumstances. Reporting by private sector entities has been voluntary.

Cyber Incident Reporting for Critical Infrastructure Act of 2022

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA; P.L. 117-103, Division Y) directed CISA to create a mandatory cyber incident and ransomware reporting program that covers certain CI entities across all sectors. In April 2024, CISA issued a proposed rule to implement this directive. The proposed rule would apply to certain corporate entities—or "critical infrastructure entities" that have significant operations within one or more critical infrastructure sectors.[65] It notes that as of April 2024, there were no current cyber incident reporting requirements for water and wastewater systems, which complicated federal cybersecurity efforts in the sector.

Under the proposed rule, certain entities in the Water and Wastewater Systems sector would be covered by the mandatory reporting requirements if they exceed a certain number of employees

[59] See CISA, "Technical Support," https://www.dhs.gov/law-enforcement-resources/resource-type/technical-assistance.

[60] The CISA regional offices are in the same cities as, or in close proximity to, the 10 existing Federal Emergency Management Agency (FEMA) offices.

[61] See CISA, "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)," https://www.cisa.gov/supply-chain; and CISA, "Securing Industrial Control Systems," https://www.cisa.gov/publication/securing-industrial-control-systems.

[62] For details about these services, see CISA, "Free Cybersecurity Services and Tools," https://www.cisa.gov/cyber-resource-hub.

[63] See CISA, "CISA Central," https://www.cisa.gov/central.

[64] For an example of threat reporting, see CISA, "Alert (AA21-287A) Ongoing Cyber Threats to U.S. Water and Wastewater Systems," https://us-cert.cisa.gov/ncas/alerts/aa21-287a.

[65] Department of Homeland Security (DHS), "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23644, April 4, 2024.

or revenue threshold. CISA claimed that larger entities are more likely to be targeted by malicious cyber actors and that such attacks are likely to have more severe consequences, including disruption of CI. The rulemaking proposes regulatory coverage of water and wastewater facilities serving more than 3,300 people to "provide the Federal government with sufficient reporting to better understand the Water and Wastewater Systems Sector's cyber threat environment."[66] The rule has not been finalized as of the date of this report.

Observations on Approaches to Water Sector Cybersecurity

Reported cyber incidents at water systems have raised questions about the adequacy of existing approaches to addressing water sector cybersecurity. Efforts to improve water sector cybersecurity generally center on addressing the resilience of individual water systems to such threats, and/or addressing federal agency coordination in supporting water system cybersecurity.

Individual Systems

Broadly, approaches to improving water system cybersecurity have focused on individual systems—by establishing assessment and planning requirements intended to address cybersecurity threats, as well as providing technical and financial assistance.

Identifying water-sector-specific challenges provide context to policy options that may improve water system cybersecurity. Because of the number of water systems as well as the range of water system sizes, cybersecurity challenges faced by the sector may differ from those of other CI sectors (e.g., the energy sector) that have relatively few providers. In the 2024 report *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, the U.S. Government Accountability Office (GAO) highlighted several issues specific to the water sector.[67] GAO identified that some systems rely on older technology or legacy systems that, to update, would create extended outages, potentially disrupting water service. Because of this, systems may use out-of-date operational technologies no longer supported by the manufacturer. For certain systems, a reluctance to increase water rates may limit financial resources available to update operational technology or to hire cybersecurity expertise. Particularly for smaller water systems, limited financial resources for information technology or other technical resources, such as security specialists, may create challenges to administering a cybersecurity program.[68]

Technical Assistance

One approach to addressing water system cybersecurity involves technical and financial assistance for cybersecurity improvements, such as EPA's WaterTA initiative. The effectiveness of such assistance depends in part on its availability and its use by systems. GAO reports that from 2023 to March 2024, EPA provided cybersecurity assessments to 191 water or wastewater

[66] DHS, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23644, April 4, 2024, p. 23701.

[67] U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, GAO-24-106744, August 1, 2024, https://www.gao.gov/assets/gao-24-106744.pdf.

[68] EPA, "Water Sector Cybersecurity Brief for States," June 2018, https://www.epa.gov/sites/default/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf.

systems, and received 24 requests from systems for assistance on cybersecurity topics.[69] Further, the agency conducted 21 trainings since FY2022 with participants from more than 3,000 systems, at the same time posting resources on the internet for operators to review.[70] State agencies or nonprofit organizations may also provide water system cybersecurity technical and financial assistance for specific systems. Given the number of water systems operating nationally, understanding the extent to which water systems are using this assistance or their characteristics may be useful to developing approaches to improve cybersecurity.

Implementation of SDWA Requirements

Congress has used another approach to address water system cybersecurity, specifically SDWA requirements. SDWA vulnerability assessment and planning requirements are targeted to those systems serving a larger number of individuals, because if disrupted, the impact to public health would be larger. In addition, these larger systems benefit from economies of scale, resulting in greater capacity to update technology, to hire security specialists, or to adopt practices to improve cybersecurity. At the same time, in an enforcement notice, EPA highlights that such systems appear to still experience compliance challenges with these requirements, as the agency stated that more than "70% of systems inspected by EPA since September 2023 are in violation of basic SDWA Section 1433 requirements."[71] This raises questions regarding whether or how to use other existing authorities or other options to improve water system cybersecurity.

Federal Agency Actions and the Role of Coordination

Different entities have questioned EPA's activities with regard to cybersecurity. For example, in March 2023, EPA issued an interpretive memorandum to use an authority under SDWA to require states, as a part of their SDWA primary enforcement responsibilities, to evaluate water system operational technology cybersecurity as a part of the states' triennial inspections, called "sanitary surveys."[72] Sanitary surveys are on-site inspections of a water system's components (e.g., source, treatment, distribution system, finished water storage, pumps) and operational functions (e.g., monitoring and reporting, management and operations, and operator compliance).[73] Several stakeholders filed a petition for judicial review of EPA's action, arguing that the agency did not follow the Administrative Procedure Act when issuing the memorandum and that the agency's expansion of the sanitary survey exceeds EPA's statutory authority under SDWA.[74] Following this, EPA rescinded this approach in October 2023.[75]

Other stakeholders have identified that EPA's activities could better assist systems in addressing cybersecurity risks. For example, GAO issued a report finding that EPA had not "taken key steps

[69] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*.

[70] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*.

[71] EPA, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, June 6, 2024. In its enforcement alert, EPA did not state how many systems it had inspected since September 2023.

[72] Memorandum from Radhika Fox, Assistant Administrator of EPA, to State Drinking Water Administrators, "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process," March 3, 2023.

[73] 40 C.F.R. §142.14.

[74] The Administrative Procedure Act is codified at 5 U.S.C. §553. State of Missouri v. EPA, No. 23-1787 (8th Cir. 2023).

[75] Memorandum from Radhika Fox, Assistant Administrator of EPA, to State Drinking Water Administrators, "Withdrawal of Cybersecurity Memorandum of March 3, 2023," October 11, 2023.

that would help target its efforts and more effectively address cybersecurity risk."[76] As reported by GAO, these steps include developing a national water sector strategy for cybersecurity that would enable the agency to measure its progress toward cybersecurity objectives (e.g., the number of water systems EPA wants to see develop cybersecurity programs), and to coordinate responsibilities.[77] GAO reports that in response to its recommendations, EPA issued a "Water and Wastewater Systems Sector Risk Management Plan" in January 2025.[78]

When responding to specific cyberthreats, EPA's activities typically involve federal agency coordination, though some have identified such coordination as an area for improvement. For example, DHS's Office of the Inspector General (OIG) recommended in 2024 that CISA and EPA (1) formalize their collaboration through a memorandum of understanding and (2) develop and implement policies and procedures to coordinate roles, communication, and information sharing. In addition, the DHS OIG recommended that CISA formalize internal procedures to improve communication among CISA divisions regarding the Water and Wastewater Systems sector.[79] Thus, the existing framework for federal agency coordination regarding water sector cybersecurity has also been the subject of attention.

Legislative Activity in the 118th and 119th Congresses

The 118th Congress held hearings and introduced legislation regarding water sector cybersecurity. Both the House Committee on Energy and Commerce and the House Committee on Homeland Security held hearings on water system cybersecurity.[80]

Some Members also introduced legislation aimed at improving water sector cybersecurity. **Table 1** and **Table 2** include water sector cybersecurity bills introduced in the 118th and 119th Congresses, respectively. These tables include bills that have water sector cybersecurity as their primary focus and more comprehensive proposals that include provisions addressing water sector cybersecurity.

[76] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*.

[77] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*.

[78] See "Recommendations" section of GAO's website "Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems," https://www.gao.gov/products/gao-24-106744.

[79] DHS Office of the Inspector General (OIG), *CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector*, OIG-24-09, January 9, 2024, https://www.oig.dhs.gov/sites/default/files/assets/2024-01/OIG-24-09-Jan24.pdf.

[80] U.S. Congress, House Energy and Commerce Committee, Environment Subcommittee, *Ensuring the Cybersecurity of America's Drinking Water Systems*, 118th Cong., January 31, 2024. U.S. Congress, House Homeland Security Committee, Cybersecurity and Infrastructure Protection Subcommittee, *Securing Operational Technology: A Deep Dive into the Water Sector*, 118th Cong., 2nd sess., February 6, 2024.

Table 1. Selected Legislation Introduced in the 118th Congress on Water System Cybersecurity

By date of introduction (oldest first)

Bill	Title	Date of Introduction	Latest Action	Description of Selected Provisions
S. 660	Water System Threat Preparedness and Resilience Act of 2023	March 6, 2023	Referred to Senate Committee on Environment and Public Works (EPW)	Would have required the U.S. Environmental Protection Agency (EPA) to establish a program to support membership, particularly of smaller water and wastewater systems, in the Water Information Sharing and Analysis Center (WaterISAC). The bill's program would have required EPA to offset membership dues for water and wastewater systems, coordinate with WaterISAC for incident reporting and analysis, and "enhance" WaterISAC's monitoring tools and preparedness resources. Would have authorized $10 million in appropriations for each of FY2024 and FY2025 to carry out this program.
H.R. 1367	Water System Threat Preparedness and Resilience Act of 2023	March 10, 2023	Referred to House Transportation and Infrastructure (T&I) Committee and House Energy and Commerce (E&C) Committee	Would have required EPA to establish a program to support membership, particularly of smaller water and wastewater systems, in the WaterISAC. The bill's program would have required EPA to offset membership dues for water and wastewater systems, coordinate with WaterISAC for incident reporting and analysis, and "enhance" WaterISAC's monitoring tools and preparedness resources. Would have authorized $10 million in appropriations for each of FY2024 and FY2025 to carry out this program.
H.R. 3809	Cybersecurity for Rural Water Systems Act of 2023	July 10, 2023	Referred to House Committee on Agriculture	Would have amended the U.S. Department of Agriculture (USDA) rural water and wastewater circuit rider program to include cybersecurity technical assistance. Such technical assistance may have included assessing system efficacy in protecting against cyber threats, and implementing cybersecurity plans, procedures, and technologies to protect against cyberthreats. Would have reauthorized appropriations for the rural water and wastewater circuit rider program at $32.5 million for each of FY2024 through FY2028, of which $7.5 million in each fiscal year would have been dedicated for cybersecurity technical assistance.
S. 2388	Cybersecurity for Rural Water Systems Act	July 19, 2023	Referred to Senate Committee on Agriculture, Nutrition, and Forestry	Would have directed USDA to establish a cybersecurity circuit rider program to provide technical assistance to rural water or wastewater systems to (1) provide rapid assessments of the system's current ability or inability to respond to cybersecurity threats and protect cyber infrastructure, (2) develop reasonable protocols to enhance cybersecurity protection, (3) provide assistance to address inadequate cyber protection plans, and (4) document a system's current state of water supply cyber protection. Would have authorized $10 million in appropriations for each of FY2024 through FY2028 to carry out this program.

Bill	Title	Date of Introduction	Latest Action	Description of Selected Provisions
H.R. 7922	To establish a Water Risk and Resilience Organization to develop risk and resilience requirements for the water sector	April 12, 2024	Referred to House T&I Committee and House E&C Committee	Would have established a framework for addressing cybersecurity wherein EPA would have certified a "water risk and resilience organization" (WRRO), which would have established cybersecurity risk and resilience requirements, that the WRRO would have enforced among water and wastewater systems, with oversight from EPA. Would have authorized $5 million in appropriations to support the WRRO.
S. 5335	Rural Prosperity and Food Security Act of 2024	November 18, 2024	Referred to Senate Committee on Agriculture, Nutrition, and Forestry	Section 6405 would have directed USDA to establish a cybersecurity circuit rider program to provide technical assistance to rural water or wastewater systems to (1) provide rapid assessments of the system's current ability or inability to respond to cybersecurity threats and protect cyber infrastructure, (2) develop reasonable protocols to enhance cybersecurity protection, (3) provide assistance to address inadequate cyber protection plans, and (4) document a system's current state of water supply cyber protection. Would have authorized $10 million in appropriations for each of FY2025 through FY2029 to carry out this program.
H.R. 10389	Water Authority Cybersecurity Protection Act	December 12, 2024	Referred to House E&C Committee	Would have reauthorized and increased appropriations from $25 million to $50 million for each of FY2026 and FY2027 for SDWA Section 1433 technical assistance to improve water system resiliency, and would have extended EPA's authority to provide such technical assistance to specific communities.
H.R. 10483	Water Cybersecurity Enhancement Act	December 18, 2024	Referred to House E&C Committee	Would have extended appropriations for SDWA Section 1433 technical assistance to FY2030, and would have added participation in security and resilience training programs to the eligible uses of funds.
H.R. 10529	Prioritizing American Farmers and Agricultural Industry Over Bureaucracy Act	December 19, 2024	Referred to House Committee on Agriculture	Section 5402 would have variously amended the rural water and wastewater circuit rider program, including to add cybersecurity as an eligible use for technical assistance provided from such circuit rider program. Would have authorized $25 million in appropriations for each of FY2025 through FY2029 to carry out this program.

Source: Compiled by CRS from Congress.gov; Congress.gov, "Policy Areas—Field Values," https://www.congress.gov/help/field-values/policy-area; and Congress.gov, "Legislative Subject Terms—Field Values," https://www.congress.gov/help/field-values/legislative-subject-terms. CRS used the following search terms to identify bills in the 118th Congress: "water system," "drinking water," "wastewater," "sewage," "treatment works," "cybersecurity," "cyber security," "cyber threat," "cyber incident," "cyber attack," "hacking," "spyware," "malicious software," "malware." Note that the legislation search did not include amendments offered during the 118th Congress. Further, the bills identified with the use of search terms listed above may not necessarily be comprehensive of all such legislation, as other bills may use differing terms in reference to water system cybersecurity.

Notes: This table includes legislation or provisions in which the primary focus was addressing water sector cybersecurity, based on a CRS review of the results of the legislation search. Appropriations acts providing funding for water system cybersecurity grant programs are not included.

Table 2. Selected Legislation Introduced in the 119th Congress on Water System Cybersecurity

By date of introduction (oldest first), as of May 23, 2025

Bill	Title	Date of Introduction	Latest Action	Description of Selected Provisions
S. 1018	Cybersecurity for Rural Water Systems Act	March 13, 2025	Referred to Senate Committee on Agriculture, Nutrition, and Forestry	Would direct the U.S. Department of Agriculture (USDA) to establish a cybersecurity circuit rider program to provide technical assistance to rural water or wastewater systems to (1) provide rapid assessments of the system's current ability or inability to respond to cybersecurity threats and protect cyber infrastructure, (2) develop reasonable protocols to enhance cybersecurity protection, (3) provide assistance to address inadequate cyber protection plans, and (4) document a system's current state of water supply cyber protection. Would authorize appropriations of $10 million for each of FY2025 through FY2029.
H.R. 2109	Cybersecurity for Rural Water Systems Act	March 14, 2025	Referred to House Committee on Agriculture	Would amend the USDA rural water and wastewater circuit rider program to include cybersecurity technical assistance. Such technical assistance may include assessing system efficacy in protecting against cyber threats, and implementing cybersecurity plans, procedures, and technologies to protect against cyberthreats. Would reauthorize appropriations for the rural water and wastewater circuit rider program at $32.5 million for each of FY2026 through FY2030, of which $7.5 million in each fiscal year would have been dedicated for cybersecurity technical assistance.
H.R. 2344	Water ISAC Threat Protection Act	March 25, 2025	Referred to House Transportation and Infrastructure (T&I) Committee and House Energy and Commerce (E&C) Committee	Would require EPA to establish a program to support membership, particularly of smaller water and wastewater systems, in the Water Information Sharing and Analysis Center (WaterISAC). The bill's program would require EPA to offset membership dues for water and wastewater systems, coordinate with WaterISAC for incident reporting and analysis, and "enhance" WaterISAC's monitoring tools and preparedness resources. Would authorize $10 million in appropriations for each of FY2026 and FY2027 to carry out this program.
S. 1118	Water Intelligence, Security, and Cyber Threat Protection Act of 2025	March 25, 2025	Referred to Senate Environment and Public Works (EPW) Committee	Would require EPA to establish a program to support membership, particularly of smaller water and wastewater systems, in the WaterISAC. The bill's program would require EPA to offset membership dues for water and wastewater systems, coordinate with WaterISAC for incident reporting and analysis, and "enhance" WaterISAC's monitoring tools and preparedness resources. Would authorize $10 million in appropriations for each of FY2026 and FY2027 to carry out this program.
H.R. 2594	To establish a Water Risk and Resilience Organization to develop risk and resilience requirements for the water sector	April 2, 2024	Referred to House T&I Committee and House E&C Committee	Would establish a framework for addressing cybersecurity wherein EPA would certify a "water risk and resilience organization" (WRRO), which would establish cybersecurity risk and resilience requirements, that the WRRO would enforce among water and wastewater systems, with oversight from EPA. Would authorize $10 million in appropriations to support the WRRO.

Bill	Title	Date of Introduction	Latest Action	Description of Selected Provisions
S. 1549	Water Cybersecurity Enhancement Act of 2025	May 1, 2025	Referred to Senate EPW Committee	Would reauthorize appropriations for SDWA Section 1433 technical assistance, and would have added participation in security and resilience training programs to the eligible uses of funds. Would reauthorize appropriations at $25 million for each of FY2026 through FY2031.

Source: Compiled by CRS from Congress.gov; Congress.gov, "Policy Areas—Field Values," https://www.congress.gov/help/field-values/policy-area; and Congress.gov, "Legislative Subject Terms—Field Values," https://www.congress.gov/help/field-values/legislative-subject-terms. CRS used the following search terms to identify bills in the 119th Congress: "water system," "drinking water," "wastewater," "sewage," "treatment works," "cybersecurity," "cyber security," "cyber threat," "cyber incident," "cyber attack," "hacking," "spyware," "malicious software," "malware." Note that the legislation search did not include amendments offered during the 118th Congress. Further, the bills identified with the use of search terms listed above may not necessarily be comprehensive of all such legislation, as other bills may use differing terms in reference to water system cybersecurity.

Note: This table includes legislation or provisions in which the primary focus was addressing water sector cybersecurity, based on a CRS review of the results of the legislation search. Appropriations acts providing funding for water system cybersecurity grant programs are not included.

Considerations

While many stakeholders and policymakers recognize that the water sector remains vulnerable to cyberattacks, they have offered differing approaches to improving the sector's cybersecurity. Some approaches involve authorizing additional financial or technical assistance programs to support systems' cybersecurity. Other approaches would change the existing framework (i.e., the existing federal framework under SDWA, as amended by AWIA, which requires larger water systems to assess their vulnerabilities and develop response plans) or develop a new federal framework to address water sector cybersecurity. These approaches raise a number of questions for consideration by policymakers.

The approaches discussed in this section primarily involve efforts to address the cybersecurity of the municipal water sector, specifically. Considerations associated with potential changes in the broader efforts to address CI cybersecurity, such as through E.O. 14239, "Achieving Efficiency Through State and Local Preparedness," are not discussed below.

Broadly, the range of cyberthreats may mean that improving both the cybersecurity of technologies used by the sector and individual systems' cybersecurity practices remain priorities for stakeholders and policymakers. One consideration involves the relative risk associated with each type of cyberthreat and the relative vulnerability of different water systems. For example, cyberthreats to technology widely used by water systems would pose a risk for the systems that use it. Other cyberthreats may target individual systems, where an attack could result in significant public health impacts for that one community. Accordingly, one question may be how approaches to address water system cybersecurity assess and target risks given the range of cyberthreats.

Approaches to Address Systems' Cybersecurity

Federal efforts to address water system cybersecurity generally have involved requirements for systems serving more than 3,300 individuals and technical and financial assistance for systems serving 3,300 or fewer individuals. This approach recognizes the different capacities of water systems, but as noted, EPA's OIG and other stakeholders have raised concerns about its effectiveness at improving the cybersecurity of both larger and smaller systems (e.g., concerns over the quality of larger systems' vulnerability assessments and emergency response plans, and the extent to which smaller systems are benefitting from technical and financial assistance).

Legislative proposals have focused on adding programs (e.g., circuit rider programs targeted to rural systems) intended to improve cybersecurity or reauthorizing appropriations for existing technical and financial assistance programs. On one hand, options to authorize additional programs to support technical assistance could create new opportunities for systems to improve their cybersecurity. On the other hand, these options could result in the creation of additional programs that would duplicate the services of existing programs. A key question pertains to whether the existing technical and financial assistance is oversubscribed or accessed only by certain types of systems.

To answer this question, a first step involves understanding how water systems utilize existing EPA technical and financial assistance and using this information for targeted outreach. Data from GAO's cybersecurity report provide some statistics about the number of systems participating in

EPA's technical assistance trainings and programs.[81] GAO's report identifies that, from FY2022 to FY2024, representatives of around 3,000 water systems attended trainings.[82] For context, nearly 50,000 community water systems operate in the United States. EPA could compile information (e.g., demographics or other system characteristics) regarding the systems that do access trainings, which could help inform strategies to attract more water systems or to target specific systems to accept EPA's technical assistance. Requiring EPA to develop outreach plans, informed by data collected from the agency's existing efforts, may result in better targeting of specific systems that may not be utilizing existing technical and financial assistance. This approach is similar to the technical support plan that EPA and CISA developed as required by SDWA Section 1420A. Of concern is the efficacy of an outreach planning requirement that leads to the development of another plan or strategy, which may or may not affect the number or type of systems accessing available technical assistance and resources.

Other considerations pertain to technical assistance proposals that involve third-party entities (e.g., nonprofit organizations or circuit rider programs). The relative expertise of entities may be a consideration, as these entities could experience similar cybersecurity hiring or recruiting challenges as other systems do.[83] Another consideration is whether such third-party entities themselves are secure and whether they might pose a threat to participating systems because of the potential need for them to collect and evaluate data on the systems' vulnerabilities to cyberattacks. Previously, Congress has deliberated over concerns regarding potentially exposing such additional vulnerabilities due to sharing of sensitive information. SDWA Section 1433 requires systems to certify to EPA that such assessments are completed rather than requiring them to submit the assessments to EPA, given the potential risk that doing so would create a national repository of water system vulnerabilities that could be subject to a cyberattack or security breach.

Outside of authorizing new programs, another way to increase the number of systems addressing cybersecurity vulnerabilities would be to expand risk assessment and emergency planning requirements to water systems serving under 3,300 individuals. One approach to expanding such requirements would involve amending SDWA Section 1433. Expanding the SDWA framework to include small community water systems may result in similar compliance challenges for these systems as EPA identified for larger systems. Therefore, consideration involves how expanding requirements would affect the technical and financial challenges that these systems continue to face. In addition, EPA's ability to oversee the implementation of such requirements may pose difficulties, as states challenged EPA's attempt to use other SDWA authorities to review cyber practices of water systems (e.g., through expanded sanitary survey requirements for states). Further, other stakeholders have questioned whether EPA's or states' water system expertise extends to expertise in cybersecurity practices.[84] GAO has also raised questions about whether EPA's SDWA authorities "need enhancement" to address water systems cybersecurity.[85]

---

[81] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*.

[82] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*.

[83] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*, p. 21.

[84] Jay Landers, "EPA Directs States to Assess Drinking Water Cybersecurity," American Society of Civil Engineers, March 27, 2023, https://www.asce.org/publications-and-news/civil-engineering-source/civil-engineering-magazine/article/2023/03/epa-directs-states-to-assess-drinking-water-cybersecurity.

[85] GAO, *Critical Infrastructure: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems.*

Approaches to the Federal Role in Water System Cybersecurity

Some stakeholders propose that better coordination between EPA and CISA is needed to improve water sector cybersecurity,[86] while others have debated EPA's expertise, capacity, or available resources to act as a SRMA.[87] For example, GAO reported that EPA followed GAO's recommendation to develop a risk-informed cybersecurity strategic plan, completing the plan in January 2025.[88] Further, E.O. 14239 seeks to realign the federal coordination role in cybersecurity and resilience by delegating more responsibility to the states. Changing or eliminating the roles of federal agencies in water sector cybersecurity raises questions about the specific responsibilities that EPA and CISA should have. EPA's authorities under SDWA means that the agency has expertise in water systems but may lack some cybersecurity expertise, while CISA has expertise in CI cybersecurity, more broadly, rather than for water systems. Given these different areas of expertise, the existing framework relies on federal agency coordination, which has been identified by DHS OIG and other stakeholders as an area of improvement. Shifting agency roles may raise a question over how moving responsibilities away from EPA, an agency with municipal water sector expertise, to another agency, such as CISA, would affect the suitability of cybersecurity guidance developed for this sector. Expanding other agencies' roles to include cybersecurity for specific systems (e.g., the role of the U.S. Department of Agriculture with respect to rural systems) may lead to questions about each agency's specific responsibilities. The issue of agency roles and responsibilities may be pertinent, given that federal agency coordination has been identified as an area of improvement for those agencies with existing water sector cybersecurity roles.

Other proposals seek to establish a different regulatory framework to address water sector cybersecurity. These include proposals to create an industry-led organization to set standards for cybersecurity for adoption by water and wastewater systems.[89] Under this proposal, EPA would retain oversight of the standard-setting organization. This framework is similar to the division of roles between the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) in the electricity sector, as outlined in the **Appendix**.

A NERC/FERC model approach may need to consider the differences between the electricity sector and the water sector. A primary difference is the sectors' interconnectedness. In the electricity sector, local distribution systems are connected to a larger transmission network, meaning that a disruption of the network from an attack could affect several states. Water and wastewater systems generally serve local communities, such as municipalities, and are not interconnected at the state level. NERC standards apply to the interconnected transmission network, rather than the local electricity distribution systems. The decision to apply these standards to the transmission network may be due to the scale of potential disruption from an outage to the network. Similarly, Congress has applied requirements for vulnerability assessments and planning requirements to larger water systems, given the relative scale and impact that an

[86] DHS OIG, *CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector.*

[87] Microsoft and Cyberspace Solarium Commission 2.0, *Multistakeholder Insights to Advance Water and Wastewater Infrastructure Cybersecurity*, December 13, 2023, https://cybersolarium.org/csc-2-0-reports/after-action-report-multistakeholder-insights-to-advance-water-and-wastewater-infrastructure-cybersecurity/.

[88] See "Recommendations" section of GAO's website "Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems," https://www.gao.gov/products/gao-24-106744.

[89] Microsoft and Cyberspace Solarium Commission 2.0, *Multistakeholder Insights to Advance Water and Wastewater Infrastructure Cybersecurity*.

attack or disruption of service would have. Yet smaller systems, while they serve fewer individuals, may be more vulnerable to cyberattacks.

Other questions may involve the relative effectiveness of an industry-led organization in developing protective cybersecurity standards. Proponents of this approach may cite sector-led efforts to adopt voluntary standards for cybersecurity and/or efforts to use existing cybersecurity expertise to enable water systems to assist each other to improve cybersecurity practices.[90] One question is what mechanisms of enforcement would exist for oversight of both systems and the organization. Further, the costs of supporting an industry-led organization as well as complying with potential standards may contribute to stakeholder water affordability concerns.[91]

Given that water and wastewater systems are generally local, another consideration pertains to the role of the states as compared to the federal government, particularly in light of E.O. 14239. The states' authority over the water and wastewater systems operating in that state could mean that addressing water sector cybersecurity is better handled at the state level. Others may point to federal agency resources and capacity to share information, including intelligence about threat-actors, as reasons why cybersecurity is better addressed at the federal level.

[90] Microsoft and Cyberspace Solarium Commission 2.0, *Multistakeholder Insights to Advance Water and Wastewater Infrastructure Cybersecurity*, p. 10.

[91] For more information on these issues, see CRS Report R48271, *Paying for Drinking Water: Background and Issues for Congress*, by Elena H. Humphreys.

Appendix. Case Study from the Electricity Sector[92]

One model for addressing water sector cybersecurity is based on an existing framework used in the electricity sector. This appendix describes this framework and the background for the framework's establishment.

The electricity sector in the much of the contiguous United States operates in many ways as a single, interconnected system (the grid). The grid allows electricity to "flow" between neighboring states and across regions. Electricity disruptions in one state can affect electricity service in another state, giving rise to the federal interest in electric reliability. This interconnectedness is one reason why blackouts in 1965 and 2003 resulted in cascading failures affecting extensive areas of the United States. The electricity sector developed its own industry-wide practices for enhancing reliability on a voluntary basis over several decades prior to being subjected to mandatory federal standards. This experience allowed electric utilities and others time to develop their capacity for identifying reliability needs and developing technical standards for meeting those needs. Background and context on the existing framework to address electricity reliability is provided below.

The North American Electric Reliability Corporation (NERC) plays a key role in developing federally mandated reliability standards for the U.S. electricity sector. The nonprofit entity was originally founded in 1968 as the National Electric Reliability Council in response to a blackout in 1965. The 1965 blackout was caused by a single point of failure in the electricity transmission system in Ontario, Canada, that ultimately affected 30 million people in Ontario and eight U.S. states. Initially, NERC was a utility-led organization focused on knowledge sharing and improving coordination of reliability activities among different regions.

Electric reliability was not regulated at the federal level until Congress passed the Energy Policy Act of 2005. This congressional action followed a blackout in 2003 caused by a single point of failure in the transmission system in Ohio that ultimately affected 50 million people in four states and parts of Canada.[93] Congress directed NERC and the Federal Energy Regulatory Commission (FERC) to use much of the existing institutional capacity to develop and enforce mandatory electric reliability standards. Pursuant to the 2005 law, NERC develops standards to ensure the reliable operation of the "bulk-power system" defined in statute to include "facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof) and electric energy from generation facilities needed to maintain transmission

[92] Ashley J. Lawson, Specialist in Energy Policy, wrote this section.

[93] Other, smaller blackouts in earlier years had prompted some Members of Congress to call for mandatory electric reliability standards prior to 2005. For example, on January 21, 2004, Sen. Cantwell introduced legislation that would have required mandatory electric reliability standards, remarking the following:

> While the August 2003 blackout was certainly a potent reminder, the call for reliability legislation dates back at least another five years. In 1997, both a Task Force established by the Clinton Administration's Department of Energy and a blue ribbon panel formed by the North American Electric Reliability Council (NERC) determined that reliability rules for our nation's electric system had to be made mandatory and enforceable. These conclusions resulted, in part, from an August 1996 blackout in the Western Interconnection, where the short-circuit of two overloaded transmission lines near Portland, Oregon, caused a sweeping outage that knocked out power for up to 16 hours in ten states. The blackout affected 7.5 million consumers from Idaho to California, resulting in the automatic shutdown of 15 large thermal nuclear generating plants in California and the southwest—compromising the West's energy supply for several days, even after power had mostly been restored to end-users.

Sen. Cantwell, *Congressional Record*, vol. 150, part 2 (January 21, 2004), p. S119, https://www.govinfo.gov/content/pkg/CREC-2004-01-21/pdf/CREC-2004-01-21-pt1-PgS118-3.pdf.

system reliability."[94] Federal electric reliability standards do not apply to local electricity distribution systems, nor do they apply in Alaska or Hawaii, where electricity systems do not connect with those of other states. NERC, in close collaboration with FERC, currently enforces over 100 reliability standards covering a number of areas, including cybersecurity.

For additional information about how NERC and FERC regulate electric reliability, see CRS Report R45764, *Maintaining Electric Reliability with Wind and Solar Sources: Background and Issues for Congress*, by Ashley J. Lawson. For additional information about the history of NERC, see *The History of the North American Electric Reliability Corporation*, published by NERC in 2020.

Author Information

Elena H. Humphreys, Coordinator
Analyst in Environmental Policy

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer

[94] 16 U.S.C. §824o.