Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

# Safe Drinking Water Act (SDWA) Cybersecurity Provisions

January 29, 2024

The disruption of a safe and reliable water supply remains a concern related to the protection of public health. Several events have increased attention to water system security, including "malicious cyber activities" affecting devices used by some systems. Water systems are one 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 lead agency responsible for water sector security, including cybersecurity.

## SDWA and Water Systems

To address intentional acts that may threaten water systems, Congress added provisions to the Safe Drinking Water Act (SDWA) to support the safety of water supplies. SDWA is the key federal law for protecting public water supplies; it applies to the nearly 144,000 privately and publicly owned water systems that provide piped water to at least 15 service connections or that regularly serve at least 25 people.

Of these systems, roughly 49,400 (34%) are *community water systems* (CWS), which serve the same residences year-round. Most CWS (81%) are relatively small, serving 3,300 or fewer individuals. These systems provide water to 7.6% of the total population served by CWS. Fewer than 9% of CWS serve 10,000 or more individuals, but these systems provide water to 83% of the population served (nearly 260 million individuals).

Due to the number of systems and range of system sizes, cybersecurity challenges faced by the sector may differ from other CI sectors (e.g., the energy sector) that have fewer providers. For example, smaller systems may lack resources to assist them with cybersecurity.

### SDWA Water System Security Provisions

Water system security provisions, which are primarily in SDWA Part D "Emergency Powers," range from risk and resilience assessment and emergency response planning to penalties against those who tamper or attempt to tamper with water systems.

**Congressional Research Service**
https://crsreports.congress.gov
IN12311

In 2002, P.L. 107-188 amended SDWA to add Section 1433 that required CWS serving 3,300 or more individuals to (1) assess the vulnerabilities of their system, including the "electronic, computer or other automated systems which are utilized by the public water system," to terrorist attacks or other intentional acts that could disrupt the provision of a safe and reliable water supply, (2) submit assessments to EPA, and (3) develop emergency response plans based on their assessments. EPA was directed to provide guidance to small systems (serving fewer than 3,300 people) on how to conduct assessments, prepare emergency response plans, and address threats. As initially added to SDWA, Section 1433 did not require CWS to update their assessments.

In 2018, P.L. 115-270 amended Section 1433 to require CWS serving more than 3,300 people to conduct risk and resilience assessments. Under the revised section, CWS are required to assess risk from natural hazards, in addition to malevolent acts. As a part of their assessment, CWS 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 financial capacity to respond to these risks.

For 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 ... a system's function, or if function is interrupted, to rapidly return to a normal operating condition." Based on their assessments, CWS must also develop emergency response plans. CWS must certify their assessments and submit the certifications to EPA by deadlines specific to their communities' size. CWS serving 3,300 or more individuals must review their risk assessments every five years and update them, if needed. Risk and resilience assessments and emergency response plans are voluntary for small CWS. EPA is required to provide guidance and technical assistance to small CWS on how to conduct assessments, prepare emergency response plans, and address threats.

## Other SDWA Provisions Related to Cybersecurity

Congress has established SDWA assistance programs that can support a range of objectives, including water system cybersecurity. Authorized by Section 1452, the Drinking Water State Revolving Fund (DWSRF) is the key federal financial assistance program to help water systems finance infrastructure projects needed to comply with drinking water regulations and to meet health protection objectives. These include projects that address the "vulnerability of a water system to disruption of safe water delivery, whether natural or of human origin, [and the] capability to recover from disruption of safe water delivery." Further, states are authorized to set aside portions of their annual funding allotment for water system capacity development, and strategy development. According to EPA guidance, these activities may include "security inspections and exercises (including physical infrastructure and cybersecurity assessments)," which could be a part of efforts to "develop cybersecurity effective practices or measures."

Other SDWA financial assistance programs are intended to address water system cybersecurity. SDWA Section 1433(g) directs EPA to establish a technical assistance and grant program to address CWS resiliency. As amended by P.L. 117-58, SDWA Section 1442(b) authorizes EPA to provide grants to states or water systems in emergencies, including from cybersecurity events, "to assist in responding to and alleviating any emergency situation." 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. SDWA Section 1459G requires EPA, subject to appropriations, to study technologies including those to address cybersecurity vulnerabilities, and requires EPA to establish a technology grant program for either water systems serving 100,000 or fewer individuals or small and disadvantaged water systems.

P.L. 117-58 also amended SDWA to add Section 1420A, which required EPA, in coordination with the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) to develop a

framework to identify water systems that, if degraded or rendered inoperable due to an incident, would lead to significant public health and safety impacts; and required EPA and CISA to develop a plan to support water systems. Pursuant to Section 1420A, EPA published a prioritization framework and a technical cybersecurity support plan.

## Author Information

Elena H. Humphreys
Analyst in Environmental Policy

## Disclaimer