Summary of Water Cyber Shield Act of 2026

The Water Cyber Shield Act of 2026 is comprehensive legislation to reform how EPA addresses the vulnerability of water and wastewater systems to cyberattack. Through amendments to the Safe Drinking Water Act and the Clean Water Act, this bill empowers EPA with the authorities it needs as the Sector Risk Management Agency for the water and wastewater sector—a job EPA is statutorily tasked with but lacks the necessary authorities to carry out.

According to GAO, "a cyberattack could override the systems that monitor and control automated treatment processes, leading to unsafe levels of bacteria, parasites, or chemicals in drinking water." Cyber incidents also impose costs on water systems, including through ransom payments, expenses to get damaged systems back online, and the upfront costs of investing in proper cybersecurity infrastructure and response plans. These costs are being shifted to ratepayers. Therefore, this legislation is simultaneously about water quality, water affordability, and national security.

During the development of this draft, the Senator's office engaged extensively with water sector stakeholders, state regulators, cybersecurity experts, and federal agencies. Senator Schiff believes it is important for the federal government to take a greater role in oversight of the vulnerability of the water and wastewater sector to cyberattack, but that water systems need greater resources to build capacity. This legislation reflects that comprehensive approach.

There is increased urgency to address this issue given EPA's April advisory on increasing cyber incidents and the updated July 2026 warning from CISA, EPA, FBI, and others concerning Iranian cyberattacks.

The bill also directly addresses several points raised by the water sector:

- It embraces a tiered approach, not a one-size-fits-all approach. It recognizes that there needs to be different standards for systems of different sizes and capacities.
- It is not an unfunded mandate. It includes resources that would help water stakeholders get up to speed on cybersecurity.
- It is flexible on who is in the driver's seat when it comes to enforcement. By default, EPA would hold primary enforcement responsibility. But the bill offers states a path to assume primary enforcement responsibility. States with capacity can take on the responsibility, but states that need more time can rely on EPA.
- It specifically prioritizes funding support for smaller systems and those at greater risk.
- It requires strong participation of the water sector in setting any cybersecurity standards. EPA must work with the sector, and the bill would establish an advisory committee of water stakeholders of differently sized systems.
- It requires strong protections of any data or information shared with EPA.

The bill outline is below.

Bill Outline

Drinking water systems

- Amends the Safe Drinking Water Act (SDWA) to require the inclusion in risk and resilience assessments (RRA) of risks to electronic, computer, or other automated systems for the purpose of identifying significant cybersecurity risks.
- Adds requirement to include countermeasures the system maintains or intends to use to guard against cyber threats in a water system's emergency response plan (ERP).
- Directs EPA to conduct cybersecurity assessments (including inspections) of a representative sample of public water systems each year. These would be checked against cybersecurity standards.
- Requires public water systems to provide the relevant cybersecurity portions of the RRA and ERP during a cybersecurity assessment for review by EPA or the State.
- Protects cyber documentation provided by a water system to EPA from disclosure or dissemination.
- EPA can require corrective action if the system fails to sufficiently provide for cybersecurity resilience by using tools in the SDWA.
- Directs EPA to provide technical assistance to public water systems to comply with any new requirements or to address significant cybersecurity issues.
- Lays out a pathway for state assumption of primary enforcement responsibility for cybersecurity requirements for those states who have capacity and wish to hold primary responsibility.
- Directs EPA to establish baseline cybersecurity standards for drinking water systems.
- EPA must consult with the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and the states on these metrics. The bill would also establish a technical advisory committee of water sector experts to advise EPA on the development of these metrics.
- Directs EPA to establish cybersecurity metrics to analyze the progress of the entire sector and publish regular reports.
- Directs EPA to use a tiered approach, not a one-size-fits-all approach: the bill directs the EPA to establish baseline cybersecurity standards for all systems of various sizes and risks and gives EPA the ability to establish different standards for different categories of systems based on risk and capacity.
- Authorizes an additional $300 million for the Drinking Water State Revolving Fund that is solely dedicated to helping water systems address cybersecurity needs.

Wastewater systems

- Amends the Clean Water Act (CWA) to include new requirements for large treatment works that treat domestic sewage. Exempts smaller systems.
- Applies requirement to complete RRA and ERP to wastewater systems.
- Directs EPA to conduct cybersecurity assessments (including inspections) of a representative sample of treatment works each year. These would be checked against cybersecurity standards.
- Requires applicable wastewater systems to provide the relevant cybersecurity portions of the RRA and ERP during a cybersecurity assessment for review by EPA or the State.

- Protects cyber documentation provided by a covered treatment works to EPA from disclosure or dissemination.
- EPA can require corrective action if the treatment works fails to provide for cybersecurity resilience by using the tools in the CWA.
- Directs EPA to provide technical assistance to covered treatment works to comply with any new requirements or to address significant cybersecurity issues.
- Lays out a pathway for state assumption of primary enforcement responsibility for cybersecurity requirements for those states who have capacity.
- Directs EPA to establish baseline cybersecurity standards for wastewater systems.
- EPA must consult with the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and the states on the development of these standards. The bill would also establish a technical advisory committee of wastewater sector experts to advise EPA on the standards.
- Directs EPA to establish cybersecurity metrics to analyze the progress of the entire sector and publish regular reports.
- Directs EPA to use a tiered approach, not a one-size-fits-all approach: the bill directs the EPA to establish baseline cybersecurity standards for all treatment works of various sizes and risks and gives EPA the ability to establish different standards for different categories of treatment works based on risk and capacity.
- Authorizes an additional $300 million for the Clean Water State Revolving Fund that is solely dedicated to helping wastewater systems address cybersecurity needs for treatment works.

Cyber incident reporting

- Amends 6 U.S.C. 681 to ensure that applicable water systems and wastewater systems must comply with cyber incident reporting requirements established by the Cyber Incident Reporting for Critical Infrastructure Act, which exempted state and locally owned systems (the vast majority of the water and wastewater sector).
- Requires information sharing between CISA and EPA.