United States
Environmental Protection
Agency

Office of Water
Drinking Water State Revolving Fund (DWSRF) and
Clean Water State Revolving Fund (CWSRF) Programs
in coordination with the SRF State-EPA Subworkgroup on Cybersecurity

Strengthening and Integrating Cybersecurity Measures into State Revolving Fund (SRF) Funded Projects

EPA 832-R25-001 October 2025

PREPARED BY:

U.S. Environmental Protection Agency
Office of Water
Drinking Water State Revolving Fund (DWSRF) and
Clean Water State Revolving Fund (CWSRF) Programs
in coordination with the SRF State-EPA Subworkgroup on Cybersecurity

1.0 | Overview

Cybersecurity incidents can have significant financial and operational consequences for drinking water and wastewater systems. The Environmental Protection Agency (EPA) has statutory responsibilities to decrease risks to cybersecurity threats in this sector.[1] EPA's State Revolving Funds (SRF) award federal grants to state-level SRF programs that then enter into assistance agreements with water utilities and communities. As critical infrastructure owners/operators, these assistance recipients, or sub-recipients, are all at risk for cybersecurity incidents. The SRFs understand the significant vulnerabilities for water infrastructure and the need to focus on projects that improve physical security and cybersecurity.

With the rise of cyber threats to water systems, the EPA established a subworkgroup under the State-EPA SRF workgroup specifically to discuss cybersecurity in the context of water infrastructure projects funded by the SRFs. This subworkgroup met with the goal of understanding current sub-recipient approaches to cybersecurity and share methods for encouraging SRF sub-recipients to adopt optimal cyber hygiene practices[2] to safeguard federal expenditures intended to protect public health and ensure ongoing access to clean drinking water for communities. The subworkgroup discussions explored a range of strategies to enhance cybersecurity defenses, with a focus on the role of SRFs and how SRF state programs have identified, shared, and reinforced cybersecurity best practices.

This paper provides key findings from the subworkgroup discussions and serves as a reference for SRF agencies looking to educate, encourage, or potentially require loan recipients to address cybersecurity risks and take steps to strengthen water infrastructure against threats. The Cybersecurity Toolkit below includes preventive measures that states may choose to use in their cybersecurity initiatives.

2.0 | Background

Ensuring a reliable supply of safe drinking water and effective wastewater treatment is essential for public health, environmental protection, and economic stability. In the United States the increase in cyberattacks targeting water and wastewater infrastructure poses a significant threat to the delivery of clean and safe drinking water and the disposal and treatment of wastewater.

[1] EPA is the designated Sector Risk Management Agency under Section 9002 of the National Defense Authorization Act of 2021 for the Drinking Water and Wastewater Systems Sector. In this role, EPA leads the effort to decrease risks to cybersecurity threats and other hazards. In addition, EPA is also responsible for directly implementing the requirements of the Safe Drinking Water Act Section 1433 requirements, where drinking water systems serving populations greater than 3,300 must address cybersecurity in Risk and Resilience Assessments and Emergency Response Plans.

[2] Cyber hygiene is a set of practices that individuals and organizations use to maintain the basic health and security of their systems, devices, networks, and data, aiming to protect against cyber threats and data breaches.

Malicious cyber acts by criminal entities have the capacity to cause substantial harm by disrupting vital water services, increasing vulnerability to the spread of illness, and incurring substantial financial burdens on affected communities. For example, the joint factsheet released by EPA and the Cybersecurity and Infrastructure Agency (CISA) highlighted the vulnerabilities existing at utilities using human machine interface devices. Also, one industry report found that the average ask for a ransomware attack was $2,000,000.

By offering resources, technical assistance and support, states can help ensure that SRF sub-recipients take proactive steps to increase cybersecurity. Further, fostering a culture of cybersecurity awareness at the state level will enhance the resilience of essential services like water supply and wastewater treatment, reducing the risk of costly cyber incidents and safeguarding public resources.

3.0 | Cybersecurity Toolkit

SRF state programs can take several actions to assist sub-recipients with incorporating resilient cyber practices. Examples of actions taken by different states are provided below.

I. Encourage Sub-recipients to Participate in a Cyber Assessment and Evaluation Program

Cybersecurity assessments are a valuable tool for identifying information and operational technology (IT/OT) vulnerabilities, which can be used to develop a cybersecurity risk mitigation plan. Many free resources are available to help water systems assess gaps in cyber resiliency and create plans to mitigate the risk of cyber incidents.

States can encourage drinking water and wastewater systems to request a free cybersecurity assessment through the US EPA Water Sector Cybersecurity Evaluation Program. An EPA third-party contractor uses the EPA Water Cybersecurity Assessment Tool to identify gaps or vulnerabilities in a water system's information and operational technologies that may compromise their ability to produce and distribute safe water. A water system may register to request a cybersecurity assessment, and the EPA contractor will contact the water system to coordinate the assessment. After the completion of the assessment, a report and a template for a Risk Mitigation Plan will be generated for the water system to document and track actions to address their cybersecurity gaps or vulnerabilities. Both the assessment and mitigation plan remain private between the water utility and contractor: EPA does not receive any utility-specific information. For additional questions and/or requests for cybersecurity consultations, water systems and primacy agencies can request EPA Cybersecurity Technical Assistance.

States can also encourage water systems to contact the Cybersecurity & Infrastructure Security Agency (CISA) for free cybersecurity assessments. CISA's "Cyber Hygiene" services include vulnerability scanning and web application scanning. Vulnerability scanning continuously monitors and assesses internet-accessible network assets, providing weekly reports of findings

and urgent reports of high-risk findings. Web application scanning assesses utilities' public-facing online systems to uncover vulnerabilities and misconfigurations that attackers could exploit. To sign up for CISA's Cyber Hygiene services, a system can email vulnerability@cisa.dhs.gov with the subject line "Requesting Vulnerability Scanning Services." The email should include the name of the utility, a point of contact with an email address, and the physical address of the utility's headquarters.

In considering options for encouraging or requiring sub-recipients to complete cyber assessments and evaluations, SRF state programs should identify and coordinate with existing cybersecurity efforts within their state. Multiple state programs have incorporated cybersecurity assessments into their work with water systems.

- The **New York** State Department of Health (NYSDOH) requires community water systems serving 3,301 or more people to submit a five-year water supply emergency plan including a cybersecurity vulnerability analysis. Using a state template, systems assess risks to critical infrastructure and outline mitigation steps. NYSDOH analysts review assessments and provide guidance. In 2025, NYSDOH proposed new cybersecurity rules requiring asset inventories and breach response protocols.
- Through its Sustainable Infrastructure Planning Projects (SIPP) program, the **Oregon** Health Authority offers up to $20,000 in forgivable loans for studies or assessments to evaluate infrastructure and information security, including cybersecurity.
- In **Indiana**, cybersecurity vulnerability assessments are a required component of each system's asset management plan under state law. Indiana state law requires all community water systems to incorporate cybersecurity risk assessments into their asset management plans, and Indiana's SRF program supports this by making periodic vulnerability assessments mandatory for systems seeking financing.

In these examples, states implemented cybersecurity assessment requirements on a wide scale, rather than as a requirement specific to the SRF state program. This approach may encourage systems to seek out the SRF state programs as a source of assistance to achieving a state requirement or incentive rather than viewing a cybersecurity initiative as an SRF-specific burden.

II. Incorporate Incentives for SRF Sub-recipients to Use Cybersecurity Practices

SRF state programs can use incentives to encourage SRF sub-recipients to strengthen critical information technology (IT) and operation technology (OT) systems and safeguard public health services. Examples of incentives for SRF sub-recipients that are currently incorporated in SRF state programs include: priority score points for funding, reduced interest rates for projects, and the use of set-asides for cybersecurity practices.

SCORING CRITERIA | Each SRF state program has its own scoring criteria, known as priority score points, which includes assigning a numerical value to a project based on its relative importance and need. The scoring criteria is used to rank projects in order of priority for funding. Points may be offered for cybersecurity project elements such as cybersecurity upgrades to existing infrastructure, projects that include an updated cybersecurity assessment plan, and projects that include cybersecurity improvements based on a cybersecurity assessment.

- The **Georgia** Environmental Finance Authority (GEFA) has implemented a scoring enhancement program to promote cybersecurity measures in Clean Water and Drinking Water infrastructure projects. Under this initiative, communities that incorporate cybersecurity components into their project proposals will receive additional scoring points during the evaluation process. Other State Revolving Fund programs which award ranking points for projects incorporating cybersecurity initiatives include Washington (WA) Drinking Water State Revolving Fund (DWSRF), Delaware (DE) Drinking Water State Revolving Fund (DWSRF) and New Hampshire (NH) Drinking Water State Revolving Fund (DWSRF).
- The **Idaho** Department of Environmental Quality (DEQ) incentivizes cybersecurity through a Cyber Informed Engineering (CIE) approach in both the DWSRF and CWSRF. CIE includes traditional cybersecurity elements and emphasizes the design of engineered cyber controls into the infrastructure. The CIE approach provides safety and redundancy benefits in addition to cyber protection. Idaho DEQ awards additional scoring points for projects that include cyber-resilient design elements. Additional information can be found at the Idaho Department of Environmental Quality (IDEQ), including Letter of Interest ranking forms and an IDEQ CIE webinar recording.

REDUCED INTEREST RATES | Another incentive for encouraging stronger cybersecurity practices for SRF sub-recipients is offering reduced interest rates on project loans. This incentive can provide significant financial relief and motivate recipients to prioritize essential cybersecurity investments.

- The **Arkansas** Department of Agriculture SRF program provides a reduction of lending rate (up to 0.50% rate reduction) for eligible cybersecurity components of publicly owned community water system infrastructure improvement projects for DWSRF and for public owned treatment works (POTW) for CWSRF. (See section C.1.b of the 2025 AR DWSRF IUP, p. 10 and section A.2.d of the 2025 AR CWSRF IUP).

SET-ASIDES | States may use SRF set-asides to incentivize sub-recipients to develop resilience to cyber-attacks. States are eligible to use a portion of their set-asides to assist small systems to build technical, managerial, and financial capacity, including increasing cybersecurity.

- **The New Hampshire's** SRF program used SRF set-asides to provide Water System Cybersecurity "In-a-Box." The "Cybersecurity In-a-Box" program assists public water

systems in addressing cybersecurity gaps by providing a standard set of tools to improve security, including hardware updates, network redesign and enhanced protections. The state is also using set-asides to host cybersecurity workshops for utilities.

- The **Massachusetts** Department of Environmental Protection Drinking Water Program (MassDEP DWP) provides grants up to $50,000 for qualifying public water systems (PWS). This project is a partnership between the DWSRF and MassDEP DWP.
- The **Delaware** DWSRF plans to use a portion of their set-aside to develop a voluntary Cybersecurity Assessment Program to assist water systems with cybersecurity initiatives (p 29 of DE DWSRF SFY25 IUP).

III. Integrate Cybersecurity into Contractual Terms and Conditions

Terms and conditions (T&Cs) refer to the specific rules, requirements, and guidelines that govern an agreement, contract, or funding program. In the context of the SRF state program, state-level T&Cs outline the expectations and obligations for both the recipients of the funds and the granting agency. SRF state programs can choose to require cybersecurity measures by adding specific terms and conditions within SRF funded loans.

Cyber-specific T&Cs may include, but are not limited to, requiring recipients to conduct a cyber risk assessment, create a cybersecurity plan, and adhere to secure-by-design and cyber-informed engineering principles.

- The **New Mexico** Drinking Water State Revolving Fund (DWSRF) SFY25 Intended Use Plan incorporates a grant condition for all DWSRF loans that, "the Governmental Unit agrees to comply with all applicable New Mexico State cybersecurity laws and requirements..." (p.61 of DWSRF SFY25 IUP).
- Nationally, the Office of the National Cyber Director, in coordination with CISA, has issued a Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure, which was designed to integrate cyber-informed engineering and secure-by-design principles into critical infrastructure. For SRF state programs, this playbook provides template language for grant award terms and conditions which can help SRF sub-recipients prioritize cybersecurity investments and develop comprehensive strategies to mitigate risks to critical public service.

IV. Create Outreach Paths to SRF Sub-recipients

Effective outreach to SRF sub-recipients can promote the integration of cybersecurity practices throughout the life of a funded infrastructure project. By providing clear guidance, resources, and ongoing support, SRF state programs can help sub-recipients understand and enhance cybersecurity, reducing risks to critical infrastructure and improving resilience. Many states have found a website to be an effective way to share such information with SRF sub-recipients. While

it may be challenging for a state to create their own cybersecurity content, creating a landing page to connect to partner resources can be an easier first step that is helpful for water systems. A website or landing page for SRF sub-recipients focused on cybersecurity involves several key steps to ensure it is effective, accessible, and easy to navigate.

- The **Massachusetts** Clean Water State Revolving Fund (CWSRF) website has a paragraph promoting cybersecurity stating, "The SRF program encourages cybersecurity assessments through its Asset Management Planning Grant activities, as well as offers financing for cybersecurity related equipment and software. Public water suppliers and wastewater utilities are encouraged to participate in the SRF program by submitting a proposal during the annual project solicitation". Another example is a Cybersecurity Resource Hub for Public Water Systems (PWS) established by the Massachusetts Department of Environmental Protection (MassDEP). This page includes a section for news flashes and alerts, information on free cybersecurity assessments, cyber incident plans, and additional resources.
- The **Michigan** Department of Environment, Great Lakes, and Energy (EGLE) Cybersecurity for the Water Sector website provides contact information for cyber emergency response for critical cyber incidents, cybersecurity best practices, upcoming and pre-recorded trainings and webinars, advisory and alert messages. The website also includes resources from established partners, including CISA, EPA, Internet Crime Compliant Center (IC3), Michigan Cyber Command Center (MC3), Michigan Cyber Partners and Water Information Sharing and Analysis Center (WaterISAC). The EGLE website serves to collect and link to cybersecurity material provided from their partners.
- Another example which has similar components to the EGLE website is **Georgia** GEFA's cybersecurity for water systems landing page.

4.0 | Conclusion

Incorporating cybersecurity elements and information into SRF state programs is an important way to improve cyber resilience at drinking water and wastewater utilities. SRF state programs that continue to coordinate with other state-level cyber efforts, such as in state Drinking Water, Clean Water, and Information Technology agencies, can ensure a cohesive approach to cybersecurity across their state. SRF state programs can leverage other state programs and requirements to improve cyber resilience. Sub-recipient cybersecurity assessments can help to identify whether cybersecurity vulnerabilities exist. States may also leverage federal assistance in their efforts. CISA can support organizations to defend against cyber threats by offering services that proactively monitor systems and reduce vulnerabilities.

EPA can help SRF state programs and sub-recipients address cybersecurity via the EPA Cybersecurity Evaluation Program by conducting assessments and providing individualized aid

with the Cybersecurity Technical Assistance Helpdesk. EPA also provides technical assistance courses, exercises and easy-to-use tools to help water systems reduce their risk to cybersecurity incidents. SRF state programs can choose to require cybersecurity initiatives by adding specific terms and conditions to loans. The emphasis on cybersecurity practices that SRF state programs can create through these various approaches can have significant downstream benefits. For example, SRF incentives can encourage sub-recipients to strengthen IT and OT systems, and safeguard public health services. By strategically selecting the approaches that can best support SRF sub-recipients in their states and conducting strategic outreach on integrating cybersecurity practices, state SRF programs can be instrumental in providing guidance, resources, and support to reduce risks and enhance long-term reliability of the water sector.

5.0 | Resources

EPA Cybersecurity for the Water Sector
EPA's Cybersecurity Resources for Drinking Water and Wastewater Systems.

Fact Sheet: U.S. EPA Water Sector Cybersecurity Evaluation Program
Free cybersecurity assessment program that identifies cybersecurity gaps and vulnerabilities conducted by EPA's third-party contractor.

Fact Sheet: Supporting Cybersecurity Measures with the Drinking Water State Revolving Fund
Resource for SRF state programs to strengthen cybersecurity in critical drinking water infrastructure projects.

Fact Sheet: Supporting Cybersecurity Measures with the Clean Water State Revolving Fund
Resource for SRF state programs to strengthen cybersecurity in critical clean water infrastructure projects.

Cybersecurity Technical Assistance Program for the Water Sector
Registration link to receive cybersecurity technical assistance from cybersecurity subject matter experts.

Water Sector Cybersecurity Program Case Studies
Provides examples of how water utilities are improving their cybersecurity resilience.

Fact Sheet: EPA's Cybersecurity Resources for Drinking Water and Wastewater Systems
Technical assistance resources for states, technical assistance providers, drinking water and wastewater systems.

CISA Water Toolkit
This toolkit consolidates key resources for water and wastewater systems at every level of cybersecurity maturity.

AWWA's Cybersecurity & Guidance

Comprehensive set of guidance to assist water utilities to understand policies, how to comply with requirements and implements best practices.

MS-ISACs Center for Internet Security

The Center for Internet Security Risk Assessment Method provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Outlines essential cybersecurity practices for water and wastewater utilities.