Supporting Cybersecurity Measures with the Drinking Water State Revolving Fund

The Drinking Water State Revolving Fund (DWSRF) loan fund and set-asides may be used to support state programs and communities with cybersecurity measures.

BACKGROUND

Cyber-attacks are a growing threat to critical infrastructure sectors, including water systems. Many critical infrastructure facilities have experienced cybersecurity incidents that led to the disruption of a business process or critical operation. Cyber-attacks on water utilities can cause significant harm, such as:

- upsetting treatment processes by accessing the system remotely to open and close valves, override alarms, or disable pumps or other equipment;
- defacing the system's website or compromising the email system;
- stealing customers' personal data or credit card information from the utility's billing system; and
- installing malicious programs (e.g. ransomware) that can disable operations.

These attacks can compromise the ability of drinking water systems to provide safe water to customers, erode customer confidence, and result in financial and legal liabilities. A robust cybersecurity program can effectively reduce or even eliminate the vulnerabilities that cyber-attacks exploit.

DWSRF ASSISTANCE

The Drinking Water State Revolving Fund (DWSRF) can provide financial assistance to publicly-owned and privately-owned community water systems, as well as non-profit non-community water systems, for drinking water infrastructure projects including cybersecurity measures. Projects must either facilitate the system's compliance with national primary drinking water regulations or significantly further the health protection objectives of the Safe Drinking Water Act.

Each of the 50 states and Puerto Rico operates its own DWSRF program. They receive annual capitalization grants from the EPA, which in turn provide low-interest loans and other types of assistance to water systems. Repayments of DWSRF loans begin one year after project completion, with loan terms up to 30 years for most communities, or up to 40 years for disadvantaged communities.

Additionally, states may use a portion of their capitalization grant from the EPA as "set-asides" to help communities build the technical, managerial, and financial capacities of their systems. With an emphasis on small systems, these funds help ensure sustainable infrastructure and public health investments.

CYBERSECURITY MEASURES

The DWSRF may be used to develop effective cybersecurity practices and measures at drinking water systems. The set-asides can be used to conduct assessments and to develop improvement plans and emergency response strategies. The loan fund can be used to fund the installation of cyber-related infrastructure, which may include upgrading information technology and operational technology.

Risk and Resilience Assessment

The Safe Drinking Water Act (SDWA), as amended, requires community water systems serving more than 3,300 persons to conduct a risk and resilience assessment of their water systems. This includes assessing the security of any electronic, computer, or other automated systems utilized by the community water system. The SDWA also requires these community water systems to certify to the EPA that they have completed the required assessments. Following the completion of the assessment, water systems must develop or update their emergency response plans (ERPs). DWSRF set-asides may be used to assist water systems in establishing a cybersecurity program, including developing assessments and ERPs. Eligible infrastructure improvements identified by the assessments may be funded through the loan fund. More information on the SDWA risk and resilience assessment requirements can be found on the EPA's Water Resilience website.

Training

Training and education of operators and other water system staff is an eligible set-aside activity. States or their third-party contractors may develop and present workshops, seminars and other training events related to cybersecurity awareness and response. Other set-aside activities include assisting water systems with the creation of cybersecurity policies and procedures, the development of cyber incident response plans, and conducting table top exercises and full-scale emergency exercises.

Equipment & Infrastructure

The DWSRF loan fund may be used to finance equipment and upgrade technologies. Examples include upgrading outdated computers and software, creating secure network backups, enhancing the security of information technology and operational technology systems, installing or updating Supervisory Control and Data Acquisition (SCADA) systems, providing on-site back up power generation, and installing threat detection and monitoring systems. Water systems may use DWSRF loan funding to construct physical barriers and access control systems to protect information technology (IT) systems from unauthorized physical access. These may include locking doors/cabinets, cabinet intrusion alarms or conduit to protect network cables. These are eligible components of larger drinking water system improvement projects or may be stand-alone projects.

APPLY FOR FUNDING

Water systems receive DWSRF assistance directly from state agencies. Each state has its own application procedure. Contact information for each state is posted at https://www.epa.gov/dwsrf/state-dwsrf-website-and-contacts.

EPA's Water Sector Cybersecurity Brief for States:
https://www.epa.gov/sites/production/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf

DWSRF Eligibility Handbook
https://www.epa.gov/dwsrf/dwsrf-eligibilities