Fact Sheet

Supporting Cybersecurity Measures with the Clean Water State Revolving Fund

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

- interrupting treatment processes by accessing the system remotely to open and close valves, override alarms, or disable pumps or other equipment;
- overriding industrial control systems (e.g., SCADA system) used for remote monitoring of automated treatment and distribution processes;
- stealing customers' personal data or credit card information from the utility's billing system;
- installing malicious programs (e.g. ransomware) that can disable operations; or
- defacing the system's website or compromising the email system.

These attacks can compromise the ability of utilities to effectively and safely treat wastewater, erode customer confidence, and result in financial and legal liabilities. A robust cybersecurity program can effectively reduce or even eliminate the vulnerabilities that cyberattacks exploit.

HOW THE CWSRFS WORK AND WHO MAY QUALIFY

Clean Water State Revolving Fund (CWSRF) programs in each state and Puerto Rico operate like banks. Federal and state contributions are used to capitalize the programs. These assets are used to make low interest loans for water quality projects. Funds are then repaid to the CWSRFs and are recycled to fund additional eligible projects. The programs may provide assistance to public, private, or non-profit entities for water infrastructure projects. Eligible recipients vary by project type. Since the program is managed by the states, the financing of projects may vary according to the priorities of each state.

USING CWSRF FUNDS TO SUPPORT CYBERSECURITY

The CWSRF may be used to develop effective cybersecurity practices and measures at publicly owned treatment works (POTWs). Each state CWSRF program has flexibility to strategically focus their program using Intended Use Plans (IUP). Required annually, a state's IUP explains the CWSRF program, goals, operations, and compliance to the public and EPA. Those interested should seek out their state's CWSRF program to determine whether these project types are eligible in their state and participate in the annual process that determines which projects are funded. The CWSRF in your state will be able to guide potential assistance recipients through the application process. Contact your state's CWSRF program for details. A list of contacts by state can be found on the CWSRF website.

ASSESSMENTS AND TRAINING

A risk and resilience assessment of a wastewater system includes assessing the security of any electronic, computer, or other automated systems utilized by the utility. States may provide CWSRF assistance to POTWs to allow them to complete vulnerability assessments and contingency and emergency response plans. The development and initial presentation of workshops, seminars, and other training events related to cybersecurity awareness and response are also eligible.

EPA provides several free tools for conducting

risk assessments, including the Vulnerability Self-Assessment Tool 2.0 (VSAT Web 2.0), and offers water sector cybersecurity training both online and at locations nationally. Please contact safewater@epa.gov for more information about this tool.

Additionally, EPA is offering free, confidential cybersecurity assessments and technical assistance to interested water and wastewater utilities. The assessment consists of a questionnaire completed with EPA contractors and the technical assistance consists of developing a cyber action plan based on the results of your utility's assessment.Register through the contractor's cybersecurity page for more information.

EQUIPMENT & INFRASTRUCTURE

The CWSRF 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 SCADA systems, providing on-site back up power generation, and installing threat detection and monitoring systems. Publicly owned treatment works may use CWSRF financing 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 POTW improvement projects or may be stand-alone projects.

ADDITIONAL RESOURCES

ASSESSMENTS AND TRAINING

America's Water Infrastructure Act of 2018 mandates all community water systems serving over 3,300 people to conduct risk and resilience assessments (RRAs) and develop or update emergency response plans (ERPs), which must address "electronic computer, or other automated systems, including the security of such systems." Below are resources for utilities to conduct and develop these assessments and plans.

- EPA's Cybersecurity Incident Action Checklist provides steps for water and wastewater systems to prepare for, respond to, and recover from a cybersecurity incident.
- The Cybersecurity and Infrastructure Security Agency (CISA) offers free scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. Services are available to federal, state, local, tribal, and territorial governments and public and private sector critical infrastructure organizations. Results are kept confidential between the customer and CISA. Email vulnerability_info@cisa.dhs.gov with questions or to get started.
- The American Water Works Association, in collaboration with the U.S. Department of Agriculture (USDA) and the Partnership for Safe Water, offers free cybersecurity workshops specifically targeted towards small systems attendees.

REPORTING INCIDENTS

Because water and wastewater systems are not required to report cyberattacks, the federal government will only be able to respond if the affected facility contacts the government and requests assistance. Below are resources on reporting cyberattacks.

- Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government explains when, what, and how to report a cyber incident to the federal government.
- The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA.

For more information, visit: epa.gov/cwsrf

EPA Publication 817F21007