FACT SHEET

EPA's Cybersecurity Resources for Drinking Water and Wastewater Systems

Improving cybersecurity across the water sector remains one of EPA's highest priorities. EPA continues to underscore that adopting cybersecurity best practices at drinking water and wastewater utilities is essential to protect communities from the increasing number and severity of cyber-threats facing our nation's water systems. The Agency will continue to explore opportunities to lower cybersecurity risk for public water systems.

EPA will continue to support states, technical assistance providers, drinking water and wastewater systems by providing ongoing technical assistance in the form of cybersecurity assessments, subject-matter expert consultations, training, and funding.

Cybersecurity Assessments

EPA conducts cybersecurity assessments for utilities through the ***Cybersecurity Evaluation Program*** where utilities work with a cybersecurity professional virtually to complete an assessment using the WCAT, described below. Following the assessment, utilities will receive their comprehensive Assessment Report and Risk Mitigation Plan Template so they can begin addressing their cybersecurity gaps and track their progress as they make improvements to their cybersecurity program.

EPA's ***Water Cybersecurity Assessment Tool (WCAT)*** helps water systems self-assess their cybersecurity practices. State Primacy Agencies and Technical Assistance Providers can also use this tool when conducting a cybersecurity assessment at water systems. The tool utilizes **EPA's Cybersecurity Checklist,** which contains the basic cybersecurity controls needed to build a strong cybersecurity program.

Cybersecurity Technical Assistance

EPA offers direct technical assistance through the **Cybersecurity Technical Assistance Program for the Water Sector.** Primacy agencies, technical assistance providers, and utilities can submit cybersecurity questions and receive one-on-one remote assistance (phone or email) from a cybersecurity subject-matter expert. EPA strives to respond to each request for technical assistance within two business days. Using EPA's **Cybersecurity Checklist Fact Sheets,** for each of the 33 questions on the WCAT, utilities can learn additional details on each cybersecurity control including why it's important, recommendations, implementation tips (corrective actions), and additional resources utilities can access to assist in implementing each control.

Cybersecurity Training

EPA offers cybersecurity training and tabletop exercises free to the water sector. For example, EPA's Cybersecurity 101 Webinar introduces the basic principles of cybersecurity to Water Sector members. EPA has also conducted trainings on how to use the ***WCAT*** to conduct cybersecurity assessments at water and wastewater utilities for technical assistance providers and water systems. EPA also hosts webinars covering cybersecurity concepts and highlighting EPA's cybersecurity assessment resources for water systems supporting Defense drinking water and wastewater facilities.

Working in coordination with states, State-Level Rural Water Sections and Water/Wastewater Agency Response Networks (WARNS), EPA hosts tabletop exercises featuring scenarios that allow staff to assess their cyber response practices, identify ways to improve their cybersecurity posture, and engage with cybersecurity subject-matter experts.

Cybersecurity Planning

EPA's ***Cybersecurity Incident Action Checklist*** provides utilities with guidance for preparation, response, and recovery of a cybersecurity incident. By sharing examples from utilities of all sizes who have established successful cybersecurity programs, EPA has published the **Water Sector Cybersecurity Case Studies** to serve as a guide to similar utilities that seek to create their own cybersecurity program.

Cybersecurity Funding Opportunities

Most cyber hygiene practices can be implemented at minimal cost beyond time because they are focused on training and putting processes in place. When there are costs, there are several funding resources available to support drinking water and wastewater systems in implementing cyber projects. These include:

- Clean Water State Revolving Fund (CWSRF): Provides assistance to any public, private, or nonprofit entity for measures to increase the security of publicly owned treatment works, including cybersecurity.
- Drinking Water State Revolving Fund (DWSRF): Provides assistance with All-Hazard Risk and Resilience Assessment, Training, Equipment, and Infrastructure, including cybersecurity.
- CISA State and Local Cybersecurity Grant Program (SLCGP): Cybersecurity grant program for states, cities, counties, and towns from state administrative agency. Sub-award applications for cities, counties and towns must be submitted to the respective state administrative agency.
- Drinking Water System Infrastructure Resilience and Sustainability Program: This grant program can be used for planning, design, construction, implementation, operation, or maintenance of a program or project that increases resilience of public water systems, including cybersecurity.
- Tribal Cybersecurity Grant Program: DHS grant program for tribal governments to help address cybersecurity risks and threats to their information systems and improve their security.

Cybersecurity Workshops for Primacy Agencies

EPA hosts workshops across the country to assist primacy agencies with developing a cybersecurity assessment program plan for their public water systems, using state authorities or within a voluntary construct. These workshops provide information on the potential options primacy agencies can use to assess PWS cybersecurity, a detailed overview of cybersecurity assessments, cybersecurity assessment resources, funding, training, and technical assistance available to support cybersecurity at public water systems.

Threat Briefings and Alerts for Water and Wastewater Systems

EPA in conjunction with the Department of Homeland Security - Cybersecurity and Infrastructure Security Agency (CISA) offers Secret level in-person threat briefing sessions to water systems. These briefings provide an overview of classified information related to water and wastewater sector security threats and preparedness. EPA issues alerts designed for the water sector for certain incidents.

Partnerships to Support Cybersecurity Incident Response

EPA continues to coordinate with CISA and FBI when a water or wastewater system reports a cybersecurity incident. To assist water systems in the incident reporting process, EPA's fact sheet outlines the process, including instructions and contact information for EPA, FBI, and CISA. EPA, with our partners, will continue to leverage Cybersecurity Awareness Month each October to promote the cybersecurity tools and resources offered to the water sector through webinars, newsletters, and outreach.