Threat Resources and Tools for the Water and Wastewater Sector

February 27, 2024, Water and Wastewater Sector Threat Briefing

U.S. Environmental Protection Agency Resources

Top Cyber Actions for Securing Water Systems
This joint fact sheet, co-sealed by CISA, EPA, and FBI, outlines cyber actions that Water and Wastewater Systems Sector entities can take to reduce risk and improve resilience to malicious cyber activity. The fact sheet provides links to free services, resources, and tools to support these actions. Link:
https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems

EPA Water Sector Cybersecurity Evaluation Program
Water and Wastewater utilities work with a cybersecurity professional virtually to complete an assessment using the Water Cybersecurity Assessment Tool (WCAT). Following the assessment, utilities 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. Link:
https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program

EPA Water Cybersecurity Assessment Tool (WCAT)
WCAT helps water systems self-assess their cybersecurity practices. State primacy agencies and technical assistance providers can use this tool when conducting cybersecurity assessments at water systems. This tool utilizes EPA's Cybersecurity Checklist, which contains the basic cybersecurity controls needed to build a strong cybersecurity program. Link to download the tool: https://www.epa.gov/system/files/documents/2023-10/epa-water-cybersecurity-assessment-tool-2.0.-for-w_ws.xlsx

EPA 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. Link: https://www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-water-utilities

EPA Cybersecurity Checklist Fact Sheets
For each of the 33 questions on the WCAT, utilities can learn additional details about each cybersecurity control, including why it is important, recommendations, implementation tips (corrective actions), and additional resources to assist in implementing each control. Link (Fact

Sheets are in Appendix B): https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf

EPA Cybersecurity for the Water Sector Website
The site contains information, tools, and resources to assist water and wastewater utilities with cybersecurity assessments, planning, training, response, and funding opportunities. Link: https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector

America's Water Infrastructure Act (AWIA) Section 2013
EPA's AWIA resources help drinking water utilities conduct risk and resilience assessments (RRA) and develop emergency response plans (ERP). Link: https://www.epa.gov/waterresilience/awia-section-2013

- **Vulnerability Self-Assessment Tool 3.0 (VSAT Web 3.0)**
  VSAT Web 3.0 assists utilities in assessing potential impacts from man-made and natural disasters in accordance with AWIA requirements and provides suggested actions to strengthen security and resilience according to risk levels and cost-effectiveness. Link: https://www.epa.gov/waterriskassessment/vulnerability-self-assessment-tool-conduct-drinking-water-or-wastewater-utility

- **AWIA Small System Risk and Resilience Assessment Checklist**
  This checklist provides guidance for small community water systems (CWSs) serving fewer than 50,000 people to comply with requirements for risk and resilience assessments. Link: https://www.epa.gov/waterresilience/small-system-risk-and-resilience-assessment-checklist

- **Emergency Response Plan (ERP) Template and Instructions**
  The template assists drinking water and wastewater utilities in creating an ERP in accordance with AWIA requirements. It describes strategies, resources, plans, and procedures utilities can use to prepare for and respond to an incident that threatens life, property, or the environment. Separate templates and instructions for drinking water and wastewater utilities are provided. Link: https://www.epa.gov/waterutilityresponse/develop-or-update-emergency-response-plan

Incident Action Checklists for Water Utilities
Resource with twelve concise checklists with key actions to take before, during, and after an intentional incident or natural disaster. Includes checklists for drought, extreme heat and cold, tornadoes, wildfires, earthquakes, flooding, tsunami, hurricanes, volcanic activity, power outages, pandemic, cybersecurity breaches, and harmful algal blooms. Link: https://www.epa.gov/waterutilityresponse/incident-action-checklists-water-utilities

Supply Chain Resilience Guide for Water and Wastewater Utilities
The Supply Chain Resilience Guide provides actions to prepare for, or respond to, equipment and water treatment chemical supply chain challenges. The Guide provides information that utilities can use to mitigate the impacts of a future supply chain disruption. Topics include:

- Available federal and state resources
- Tips for effective supplier management and communication
- How to tap into local partnerships
- Potential operational flexibilities

Link: https://www.epa.gov/waterutilityresponse/supply-chain-resilience-guide-water-and-wastewater-utilities

Climate Resilience Evaluation and Awareness Tool (CREAT)
Interactive tool that assists water utilities in assessing climate-related risk to assets and operations in five modules:

1. **Climate Awareness**: Provide basic utility information; increase awareness of climate impacts.
2. **Scenario Development**: Understand utility risk; design scenarios of threats based on climate data.
3. **Consequences and Assets**: Outline potential consequences; catalog critical assets.
4. **Adaptation Planning**: Inventory current actions that provide resilience; design adaptation plans.
5. **Risk Assessment**: Assess risk from a changing climate; compare risk reduction of adaptation plans.

Link: https://www.epa.gov/crwu/climate-resilience-evaluation-and-awareness-tool-creat-risk-assessment-application-water

Water and Wastewater Sector Incident Response Guide (IRG)
The Water and Wastewater Sector IRG provides Sector owners and operators with information about the federal roles, resources, and responsibilities for each stage of the cyber incident response (IR) lifecycle. Sector owners and operators can use this information to augment their respective IR plans and procedures. Link: https://www.cisa.gov/sites/default/files/2024-01/WWS-Sector_Incident-Response-Guide.pdf

Water Sector Cybersecurity Program Case Studies
These case studies present approaches and lessons learned that can be applied to enhance cybersecurity planning, response and recovery, include account, device and data security, governance and training, and vulnerability management.

- **Small Wastewater System**: https://www.epa.gov/system/files/documents/2023-09/cybersecurity-program-case-study-small-wastewater-system_508c.pdf
- **Medium Drinking Water System**: https://www.epa.gov/system/files/documents/2023-09/cybersecurity-program-case-study-medium-drinking-water-system_508c.pdf
- **Medium Combined System**: https://www.epa.gov/system/files/documents/2023-12/231205-medium-combined_508c.pdf

- **Large Combined System**: https://www.epa.gov/system/files/documents/2023-10/231010-large-combined-case-study_508c.pdf

EPA Water Laboratory Alliance (WLA) Analytical Preparedness Full-Scale Exercise (AP-FSE) Toolkit

The AP-FSE Toolkit provides states, water utilities, and laboratories with tools and training to conduct exercises involving coordinating laboratory support during a contamination incident. Benefits of conducting an AP-FSE include:

- Helps states, utilities, and laboratories practice their existing response plans and standard operating procedures as well as the WLA Response Plan (WLA-RP).
- Facilitates relationship-building with other response partners prior to a water contamination incident.

The AP-FSE Toolkit is designed to be consistent with guidance in the Homeland Security Exercise and Evaluation Program (HSEEP). Link: https://www.epa.gov/waterlabnetwork/plan-laboratory-full-scale-exercise

Water Contaminant Information Tool (WCIT)

WCIT is used by the water sector to prepare for, respond to, or recover from drinking water and wastewater contamination incidents. WCIT includes comprehensive information about contaminants that could be introduced into a water system following a natural disaster, vandalism, accident or act or terrorism. There are currently over 800 priority contaminants of concern listed in WCIT. Access to this password-protected tool is limited to utilities, state primacy agencies and subsidiaries, laboratories, public health officials, state and federal emergency responders, and water associations. Link: https://www.epa.gov/waterdata/water-contaminant-information-tool-wcit

WaterISAC Resources

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

The guide contains dozens of cybersecurity best practices that water and wastewater systems can implement to reduce security risk to their IT and OT systems, broken down into 15 major categories. *Note: WaterISAC will publish an updated version of the guide in 2024 (12 Cybersecurity Fundamentals for Water and Wastewater Utilities). Three fundamentals will be released each quarter, beginning on March 27, 2024 (and then in June, July, and September 2024).* Link: https://www.waterisac.org/fundamentals

Resource Center

The Resource Center is a searchable library of articles, reports, best practices, threat analyses, and tools focused on reducing risks to water and wastewater infrastructure. Link: https://www.waterisac.org/resources

Upcoming Events
Information about upcoming WaterISAC events, including webinars and briefings. Link: https://www.waterisac.org/events

Annual Threat Analysis Report
WaterISAC's annual threat analysis report focuses on the threat environment for water and wastewater utilities. (Restricted to WaterISAC members.) Link: https://www.waterisac.org/portal/threat-analysis-water-and-wastewater-sector-may-2023

Quarterly Incident Summaries
Quarterly Incident Summaries present information on incidents and suspicious activities at water and wastewater utilities. Link: https://www.waterisac.org/waterisac-publications

Water and Wastewater Case Studies
Case studies involving cybersecurity incidents at water and wastewater utilities. (Restricted to WaterISAC members.) Link: https://www.waterisac.org/cybersecurity-incident-case-studies

Confidential Incident Reporting
Confidential reporting of cyber and physical security incidents and suspicious activity to WaterISAC. Link: https://www.waterisac.org/report-incident

Cyber Resilience – Cyber Readiness Institute (CRI) Continues Recruiting Small and Medium-sized Water and Wastewater Utilities for Free Cybersecurity Training
The Cyber Readiness Institute, in partnership with the Center on Cyber and Technology Innovation and Microsoft, is actively recruiting small and medium-sized water and wastewater utilities to participate in a free cybersecurity training program. the CRI program provides coach-supported training and resources focused on improving cybersecurity risk management and ability to respond and recover from a cybersecurity incident. Link: https://www.waterisac.org/portal/cyber-resilience-%E2%80%93-cyber-readiness-institute-cri-continues-recruiting-small-and-medium-sized

CISA Resources

CISA Regional Resources
CISA Regional offices offer a range of cyber and physical services to support the security and resilience of critical infrastructure owners and operators and state, local, tribal, and territorial partners. CISA experts collaborate with critical infrastructure partners and communities at the regional, state, county, tribal, and local levels to:

- Support preparation, response, and recovery efforts for hazards impacting critical infrastructure.
- Conduct and integrate infrastructure assessments and analysis, including dependencies and cascading effects, on critical infrastructure to influence decision-making at all phases of emergency management.

- Facilitate information sharing between public and private sector critical infrastructure partners.
- Improve situational awareness of cybersecurity risks and incidents.

Link: https://www.cisa.gov/about/regions

Cybersecurity Resources

CISA provides tools, information, and resources to help the water sector protect itself against attacks by malicious actors to reduce the likelihood of successful cyber incursions (Link: https://www.cisa.gov/water):

- **CISA's Free Cyber Vulnerability Scanning for Water Utilities**
  CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet, developed in coordination with the Environmental Protection Agency (EPA), Water Sector Coordinating Council (WSCC) and the Association of State Drinking Water Administrators (ASDWA), explains the process and benefits of signing up for CISA's free vulnerability scanning program. Link: https://www.cisa.gov/resources-tools/resources/cisas-free-cyber-vulnerability-scanning-water-utilities
- **4 Things You Can Do To Keep Yourself Cyber Safe**
  Information on the basics of "cyber hygiene," easy and common-sense ways to protect yourself online. Link: https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe
- **Report to CISA**
  A secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. Link: https://www.cisa.gov/report
- **Cybersecurity Alerts & Advisories**
  Cybersecurity advisories, alerts, and reports. Link: https://www.cisa.gov/news-events/cybersecurity-advisories
    - IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
- **Cyber Risks & Resources for the Water and Wastewater Systems Sector Infographics**
  CISA developed two infographics on Cyber Risks and Resources for the Supply Water and Manage Wastewater National Critical Functions to provide water and wastewater systems managers and state, local, tribal, and territorial partners with an overview of the cyber risks they may face and to highlight resources available to help them enhance their cybersecurity. Link: https://www.cisa.gov/national-critical-functions-supply-water-and-manage-wastewater
- **Critical ICS Cybersecurity Performance Goals and Objectives**
  CISA's Cybersecurity Performance Goals (CPGs) are a subset of cybersecurity practices,

selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. These voluntary CPGs strive to help small- and medium-sized organizations kickstart their cybersecurity efforts by prioritizing investment in a limited number of essential actions with high-impact security outcomes.
Link: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

- **Known Exploited Vulnerabilities Catalog**
  CISA's Known Exploited Vulnerabilities (KEV) Catalog is a compilation of documented security vulnerabilities that have been successfully exploited, as well as vulnerabilities associated with ransomware campaigns. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors. Link: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **CyberSentry Program**
  CyberSentry is a CISA-managed threat detection and monitoring capability that provides operational visibility into information technology and operational technology (IT/OT) networks within participating critical infrastructure entities. CyberSentry monitors for malicious activity affecting critical infrastructure participants' IT/OT networks, in many cases using sensitive information derived from government or international partners. Link: https://www.cisa.gov/resources-tools/programs/cybersentry-program

- **Logging Made Easy (LME)**
  Logs give an administrator insight into their system and network performance. More specifically, logs pinpoint exactly who is connected to a device and how they are using it. Coupled with the practice of protective monitoring – actively reviewing logs either manually or through automation – these system records can play an integral part in mitigating risk and identifying vulnerabilities before they grow too unruly. LME is a free and open log management toolset for Windows-based equipment. Link: https://www.cisa.gov/resources-tools/services/logging-made-easy

Physical Security Resources

Physical security resources include training and resources on active shooter, bombing, unmanned aircraft, vehicle ramming, and insider threat attacks. CISA also has tools and resources on non-confrontational techniques to empower and educate employees, citizens, and others with skills and support needed to identify and report suspicious behavior. Link: https://www.cisa.gov/topics/physical-security

- **Assist Visits and the Infrastructure Survey Tool Fact Sheet**
  An Assist Visit, conducted by Protective Security Advisors (PSAs) alongside critical infrastructure facility representatives, establishes and enhances the U.S. Department of Homeland Security's (DHS) relationship with critical infrastructure owners and operators, informs them of the importance of their facility, and explains how their facility or service fits

into its specific critical infrastructure sector. Link: https://www.cisa.gov/resources-tools/resources/assist-visits-and-infrastructure-survey-tool-fact-sheet

- **Personal Security Considerations Action Guide**
  This action guide helps critical infrastructure workers assess their security posture and provide options to consider whether they are on or off the job. The guide provides actionable recommendations and resources intended to prevent and mitigate threats to a critical infrastructure worker's personal safety. Link: https://www.cisa.gov/resources-tools/resources/personal-security-considerations-action-guide

- **Insider Threat Mitigation Resources**
  Resources, videos, and training courses to assist organizations in preparing for and mitigating insider threats to their employees, information, and infrastructure. Link: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/resources-and-tools

Emergency Communications Resources

The CISA Emergency Communications Division (ECD) promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient (Link: https://www.cisa.gov/topics/emergency-communications/priority-services). Services include:

- **Water Fact Sheet for Priority Telecommunications Services (PTS)**
  Priority in communications is crucial to continuity of operations at water and wastewater utilities facing adverse conditions, such as natural disasters, biohazards, cyber-attacks, or events arising from human error. CISA offers three PTSs that enable essential personnel to communicate when networks are degraded or congested, including:
    - **Government Emergency Telecommunications Service (GETS):** Prioritizes landline voice communications; no special equipment is needed and provided at no cost.
    - **Wireless Priority Service (WPS):** Prioritizes wireless calls; available on all nationwide networks and provided at no cost.
    - **Telecommunications Service Priority (TSP):** Prioritizes repair and installation of organizations' critical voice and data circuits; minimal enrollment charges and monthly fees.

  Link: https://www.cisa.gov/resources-tools/resources/water-fact-sheet-priority-telecommunications-services-pts

To apply for or receive more information on the three Priority Telecommunications Services, please visit: https://www.cisa.gov/apply-pcs

Secure Our World

Simple ways to protect yourself, your family, and business from online threats. Link: https://www.cisa.gov/secure-our-world

Other Resources

Cybersecurity Guide and Assessment Tool (AWWA)
Cyber resilience planning resources for water utilities to assess their exposure to cyber risks, set priorities, and implement a proactive cybersecurity strategy. Link: https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance

Joint Ransomware Guide (CISA-MS-ISAC)
Ransomware best practices and recommendations based on operational insight from CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response. Link: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware Guide_S508C_.pdf

Stop Malicious Cyber Activity Against Connected Operational Technology (OT) (NSA)
The National Security Agency (NSA) created this evaluation methodology and basic cybersecurity improvement approach for NSS, DoD, and DIB network owners. Link: https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF

Nationwide SAR Initiative (DHS)
The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by DHS, the FBI, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. Link: https://www.dhs.gov/nationwide-sar-initiative-nsi

Ongoing Cyber Threats to U.S. Water and Wastewater Systems (FBI-CISA-EPA-NSA)
Joint advisory detailing ongoing malicious cyber activity, by known and unknown actors, that are targeting U.S. Water and Wastewater Systems Sector facilities. Link: https://www.cisa.gov/sites/default/files/publications/AA21-287A-Ongoing_Cyber_Threats_to_U.S._Water_and_Wastewater_Systems.pdf

Tribal Information Sharing and Analysis Center (Tribal-ISAC)
Tribal-ISAC provides a platform to the nation's tribal governments, and their operations and enterprises, for cyber threat information sharing, threat prevention, protection, community response, and collaboration with other government agencies and industry ISACs. Link: https://tribalisac.org/