EPA Cybersecurity for the Water Sector

United States
Environmental Protection
Agency

Office of Water

About the Speaker

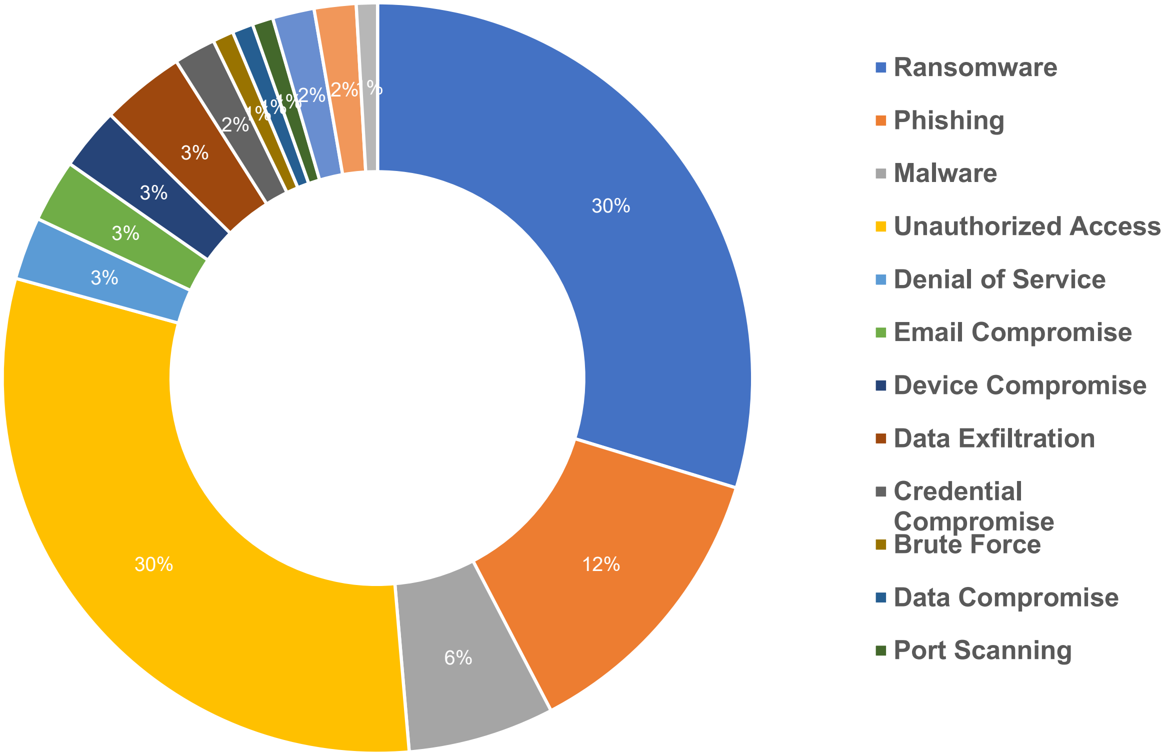
- Vijal Pancholi, Cybersecurity Analyst
- EPA's Office of Water
  - Office of Ground Water and Drinking Water
  - Water Infrastructure and Cyber Resilience
  - Cybersecurity Branch
- B.S. Computer Networks & Cybersecurity
- Email: Pancholi.Vijal@epa.gov

Water Sector Cybersecurity Threat Landscape

United States
Environmental Protection
Agency

Office of Water

Water Sector Cybersecurity Incident Statistics*



*Updated as of August 30, 2024. This chart only includes the incidents that have been voluntarily reported to EPA, CISA, or FBI.

EPA’s Cybersecurity Assessment and Technical Assistance Resources

EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems

Developed to assist owners and operators of drinking water and wastewater systems with assessing gaps in their current practices and identify actions that may reduce the risk form cyberattacks.

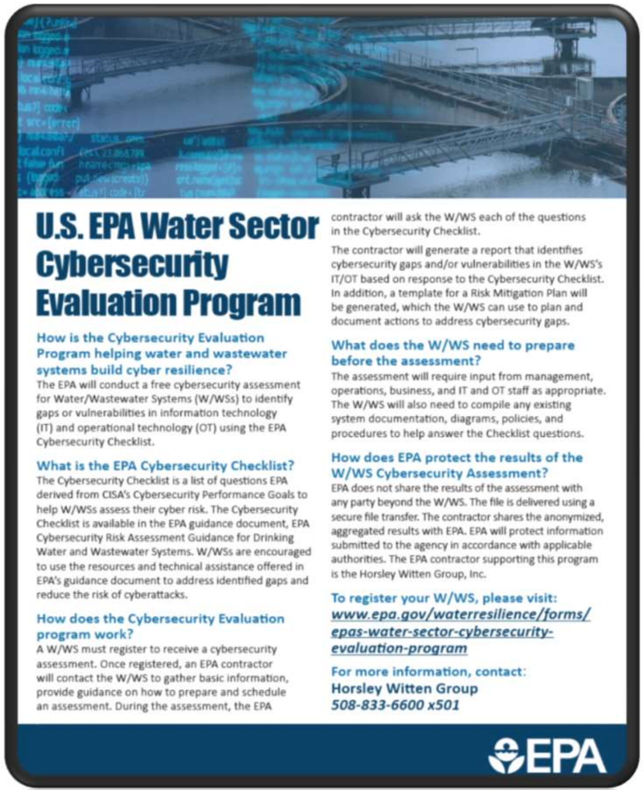
- Can be used to comply with RRA and ERP requirements for AWIA Section 1433
- EPA Cybersecurity Training
- EPA's Water Sector Cybersecurity Evaluation Program
- EPA's Cybersecurity Technical Assistance Program
- Federal Financial Resources
- EPA's Cybersecurity Checklist
- Priority Cybersecurity Practices
- Artificial Intelligence for Water and Wastewater Systems
- Fact Sheets

Cybersecurity Assessment Resources

Self-Assessment	Third-Party Assessment
Checklist and Water Cybersecurity Assessment Tool (WCAT)	Water Sector Cybersecurity Evaluation Program

EPA Water Sector Cybersecurity Evaluation Program

- EPA conducts free cybersecurity assessment for Water and Wastewater Systems to identify cybersecurity gaps.
- The program uses the EPA Cybersecurity Checklist.
- You will receive an Assessment Report and a Risk Mitigation Plan template.



U.S. EPA Water Sector Cybersecurity Evaluation Program

How is the Cybersecurity Evaluation Program helping water and wastewater systems build cyber resilience?

The EPA will conduct a free cybersecurity assessment for Water/Wastewater Systems (W/WSs) to identify gaps or vulnerabilities in information technology (IT) and operational technology (OT) using the EPA Cybersecurity Checklist.

What is the EPA Cybersecurity Checklist?

The Cybersecurity Checklist is a list of questions EPA derived from CISA's Cybersecurity Performance Goals to help W/WSs assess their cyber risk. The Cybersecurity Checklist is available in the EPA guidance document, EPA Cybersecurity Risk Assessment Guidance for Drinking Water and Wastewater Systems. W/WSs are encouraged to use the resources and technical assistance offered in EPA's guidance document to address identified gaps and reduce the risk of cyberattacks.

How does the Cybersecurity Evaluation program work?

A W/WS must register to receive a cybersecurity assessment. Once registered, an EPA contractor will contact the W/WS to gather basic information, provide guidance on how to prepare and schedule an assessment. During the assessment, the EPA contractor will ask the W/WS each of the questions in the Cybersecurity Checklist.

The contractor will generate a report that identifies cybersecurity gaps and/or vulnerabilities in the W/WS's IT/OT based on response to the Cybersecurity Checklist. In addition, a template for a Risk Mitigation Plan will be generated, which the W/WS can use to plan and document actions to address cybersecurity gaps.

What does the W/WS need to prepare before the assessment?

The assessment will require input from management, operations, business, and IT and OT staff as appropriate. The W/WS will also need to compile any existing system documentation, diagrams, policies, and procedures to help answer the Checklist questions.

How does EPA protect the results of the W/WS Cybersecurity Assessment?

EPA does not share the results of the assessment with any party beyond the W/WS. The file is delivered using a secure file transfer. The contractor shares the anonymized, aggregated results with EPA. EPA will protect information submitted to the agency in accordance with applicable authorities. The EPA contractor supporting this program is the Horsley Witten Group, Inc.

To register your W/WS, please visit:
www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program

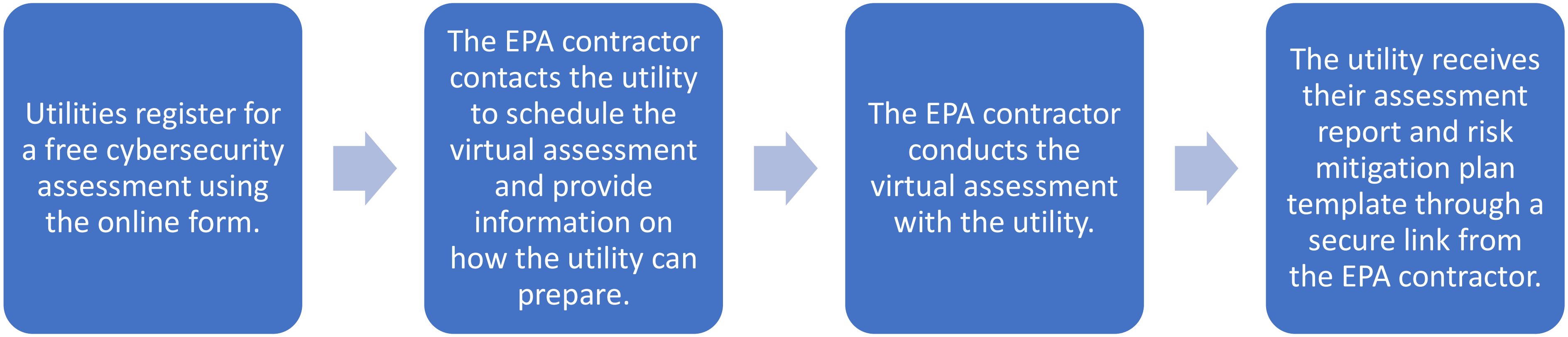
For more information, contact:
Horsley Witten Group
508-833-6600 x501

EPA

Overview of EPA's Cybersecurity Checklist

Function	# of Controls
1. Identify	7
2. Protect	24
3. Detect	1
4. Respond	1
5. Recover	1
Total:	34

EPA Water Sector Cybersecurity Evaluation Program Process



Utilities register for a free cybersecurity assessment using the online form.

The EPA contractor contacts the utility to schedule the virtual assessment and provide information on how the utility can prepare.

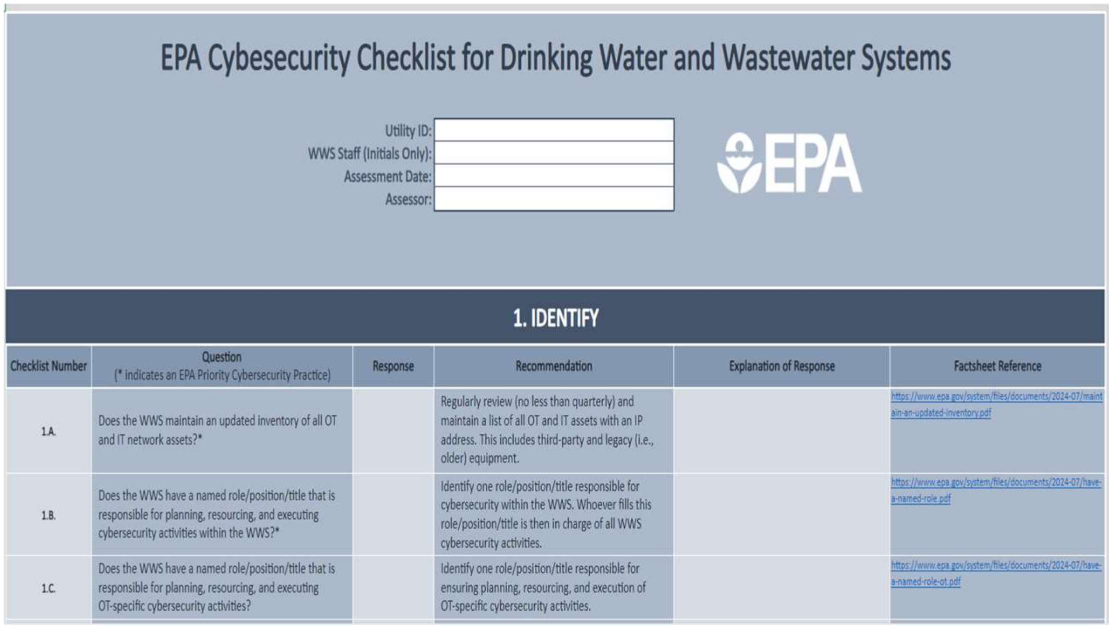
The EPA contractor conducts the virtual assessment with the utility.

The utility receives their assessment report and risk mitigation plan template through a secure link from the EPA contractor.

EPA Water Cybersecurity Assessment Tool (WCAT)

- Utilizes EPA’s Cybersecurity Checklist and provides a method to evaluate cybersecurity practices at water and wastewater utilities.

- The Tool Features:
  - Assessment Workbook
  - Assessment Report
  - Risk Mitigation Plan



EPA Cybesecurity Checklist for Drinking Water and Wastewater Systems

Utility ID:
WWS Staff (Initials Only):
Assessment Date:
Assessor:

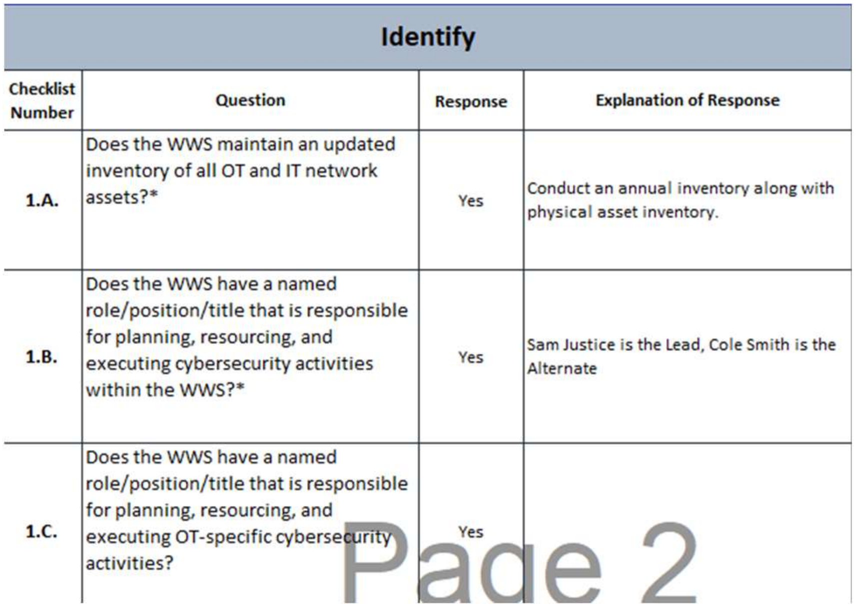
1. IDENTIFY

Checklist Number	Question (* indicates an EPA Priority Cybersecurity Practice)	Response	Recommendation	Explanation of Response	Factsheet Reference
1.A.	Does the WWS maintain an updated inventory of all OT and IT network assets?*		Regularly review (no less than quarterly) and maintain a list of all OT and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment.		https://www.epa.gov/system/files/documents/2024-07/maintain-an-updated-inventory.pdf
1.B.	Does the WWS have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the WWS?*		Identify one role/position/title responsible for cybersecurity within the WWS. Whoever fills this role/position/title is then in charge of all WWS cybersecurity activities.		https://www.epa.gov/system/files/documents/2024-07/have-a-named-role.pdf
1.C.	Does the WWS have a named role/position/title that is responsible for planning, resourcing, and executing OT-specific cybersecurity activities?		Identify one role/position/title responsible for ensuring planning, resourcing, and execution of OT-specific cybersecurity activities.		https://www.epa.gov/system/files/documents/2024-07/have-a-named-role-ot.pdf

WCAT Assessment Report Tab

- This report identifies cybersecurity gaps and/or vulnerabilities found during the cybersecurity assessment.

- The Assessment Report includes a full summary of each response and explanation of response collected during an assessment.



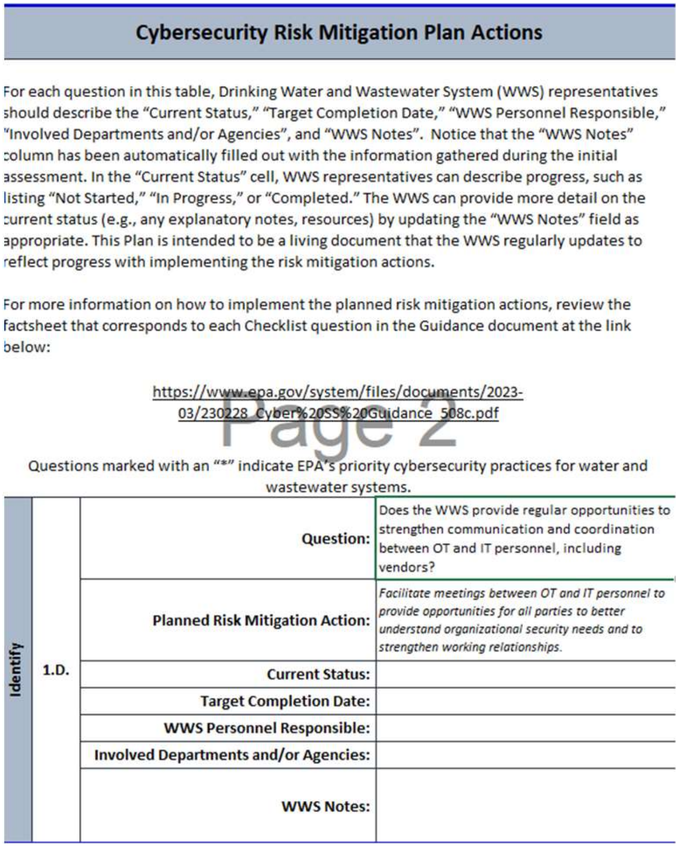
Identify

Checklist Number	Question	Response	Explanation of Response
1.A.	Does the WWS maintain an updated inventory of all OT and IT network assets?*	Yes	Conduct an annual inventory along with physical asset inventory.
1.B.	Does the WWS have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the WWS?*	Yes	Sam Justice is the Lead, Cole Smith is the Alternate
1.C.	Does the WWS have a named role/position/title that is responsible for planning, resourcing, and executing OT-specific cybersecurity activities?	Yes	

WCAT Cybersecurity Risk Mitigation Plan Template

- The Risk Mitigation Plan Template is generated for each question where you responded “No” or “In Progress.”

- You can use this template to plan and document actions to address cybersecurity gaps.



Cybersecurity Risk Mitigation Plan Actions

For each question in this table, Drinking Water and Wastewater System (WWS) representatives should describe the “Current Status,” “Target Completion Date,” “WWS Personnel Responsible,” “Involved Departments and/or Agencies”, and “WWS Notes”. Notice that the “WWS Notes” column has been automatically filled out with the information gathered during the initial assessment. In the “Current Status” cell, WWS representatives can describe progress, such as listing “Not Started,” “In Progress,” or “Completed.” The WWS can provide more detail on the current status (e.g., any explanatory notes, resources) by updating the “WWS Notes” field as appropriate. This Plan is intended to be a living document that the WWS regularly updates to reflect progress with implementing the risk mitigation actions.

For more information on how to implement the planned risk mitigation actions, review the factsheet that corresponds to each Checklist question in the Guidance document at the link below:

https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf

Questions marked with an “*” indicate EPA’s priority cybersecurity practices for water and wastewater systems.

Identify	1.D.	**Question:**	Does the WWS provide regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?
		Planned Risk Mitigation Action:	*Facilitate meetings between OT and IT personnel to provide opportunities for all parties to better understand organizational security needs and to strengthen working relationships.*
		Current Status:	
		Target Completion Date:	
		WWS Personnel Responsible:	
		Involved Departments and/or Agencies:	
		WWS Notes:	

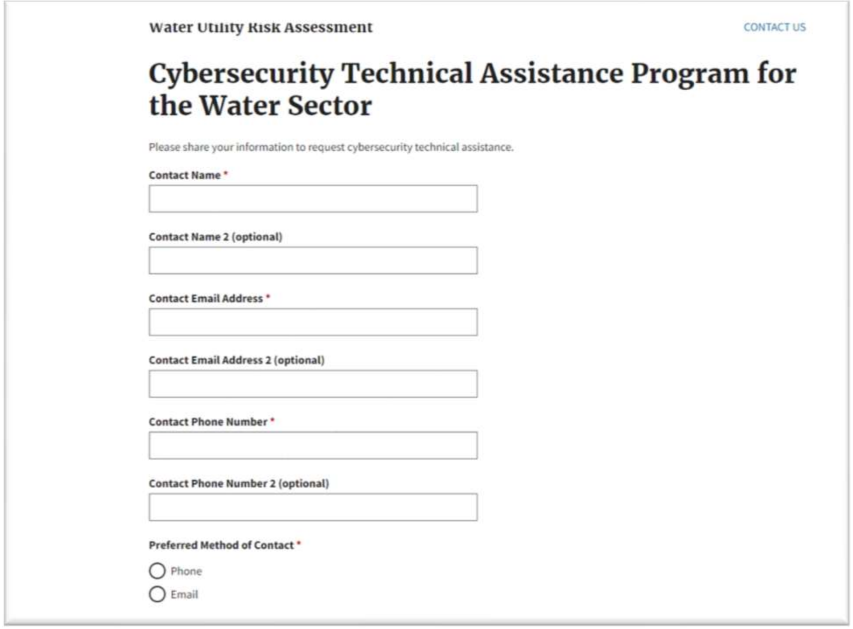
Cybersecurity Technical Assistance

Cybersecurity Technical Assistance Program for the Water Sector

- Under this program, water and wastewater systems, state primacy agencies, and technical assistance providers can submit questions or request to consult with a subject matter expert (SME) regarding cybersecurity.

- EPA will strive to have an SME respond within two business days.

- All assistance will be remote.



Water Utility Risk Assessment

CONTACT US

Cybersecurity Technical Assistance Program for the Water Sector

Please share your information to request cybersecurity technical assistance.

Contact Name *

Contact Name 2 (optional)

Contact Email Address *

Contact Email Address 2 (optional)

Contact Phone Number *

Contact Phone Number 2 (optional)

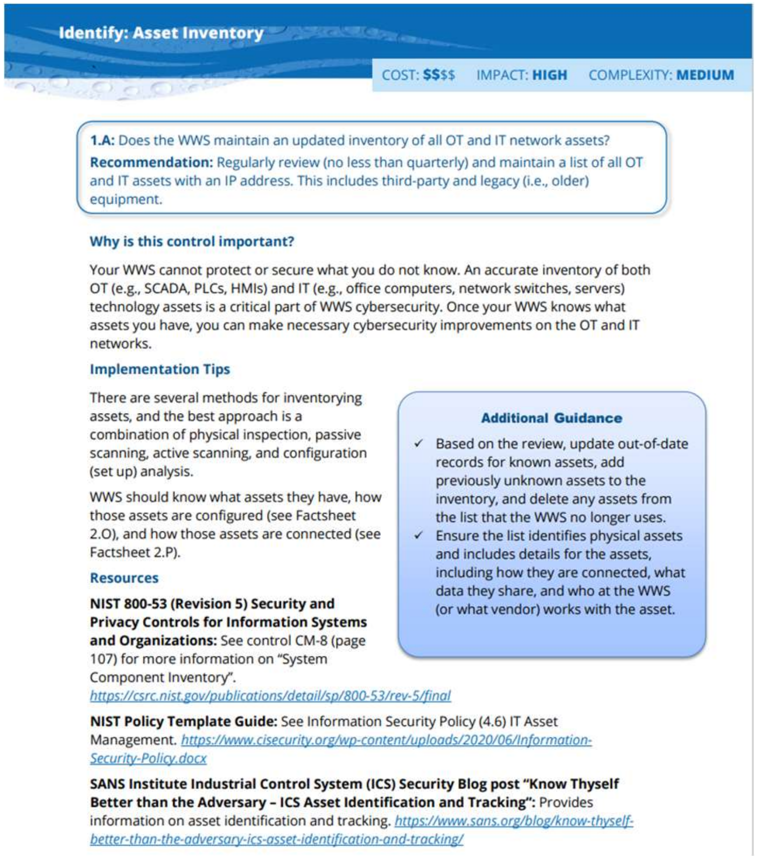
Preferred Method of Contact *

○ Phone

○ Email

EPA Cybersecurity Checklist Fact Sheets

- Fact Sheets are available for each question on the EPA Checklist and include:
  - Recommendations
  - Overview of why the control is important
  - Additional Guidance
  - Implementation Tips
  - Additional Resources
  - Estimate for Cost, Impact, and Complexity



Identify: Asset Inventory

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

1.A: Does the WWS maintain an updated inventory of all OT and IT network assets?

Recommendation: Regularly review (no less than quarterly) and maintain a list of all OT and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment.

Why is this control important?

Your WWS cannot protect or secure what you do not know. An accurate inventory of both OT (e.g., SCADA, PLCs, HMIs) and IT (e.g., office computers, network switches, servers) technology assets is a critical part of WWS cybersecurity. Once your WWS knows what assets you have, you can make necessary cybersecurity improvements on the OT and IT networks.

Implementation Tips

There are several methods for inventorying assets, and the best approach is a combination of physical inspection, passive scanning, active scanning, and configuration (set up) analysis.

WWS should know what assets they have, how those assets are configured (see Factsheet 2.O), and how those assets are connected (see Factsheet 2.P).

Additional Guidance

✓ Based on the review, update out-of-date records for known assets, add previously unknown assets to the inventory, and delete any assets from the list that the WWS no longer uses.

✓ Ensure the list identifies physical assets and includes details for the assets, including how they are connected, what data they share, and who at the WWS (or what vendor) works with the asset.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control CM-8 (page 107) for more information on "System Component Inventory". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Information Security Policy (4.6) IT Asset Management. *https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Policy.docx*

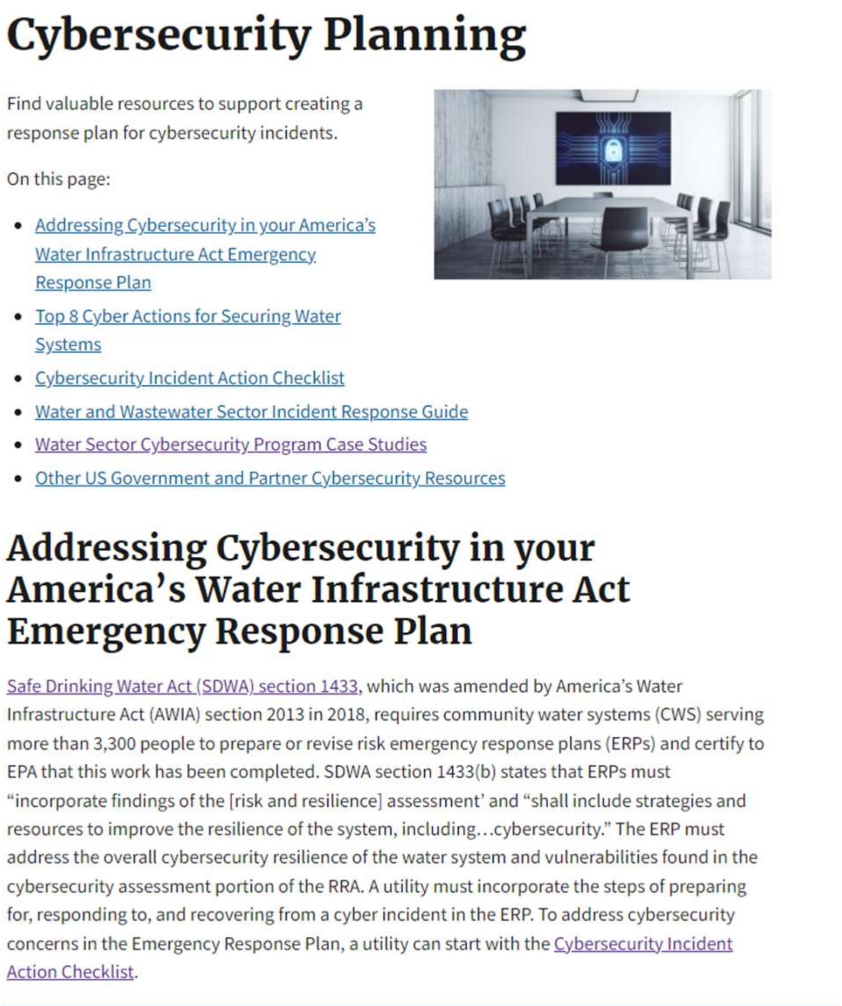
SANS Institute Industrial Control System (ICS) Security Blog post "Know Thyself Better than the Adversary – ICS Asset Identification and Tracking": Provides information on asset identification and tracking. *https://www.sans.org/blog/know-thyself-better-than-the-adversary-ics-asset-identification-and-tracking/*

Cybersecurity Planning

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home
SHARE:
CISA
UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
Water and Wastewater Cybersecurity

- CISA and EPA's Water and Wastewater Cybersecurity Toolkit consolidates key resources for water and wastewater systems at every level of cybersecurity maturity.

- The toolkit provides resources to enable sector stakeholders to proactively assess vulnerabilities and implement solutions to reduce risk and increase resilience.



Cybersecurity Planning

Find valuable resources to support creating a response plan for cybersecurity incidents.

On this page:

- Addressing Cybersecurity in your America's Water Infrastructure Act Emergency Response Plan
- Top 8 Cyber Actions for Securing Water Systems
- Cybersecurity Incident Action Checklist
- Water and Wastewater Sector Incident Response Guide
- Water Sector Cybersecurity Program Case Studies
- Other US Government and Partner Cybersecurity Resources

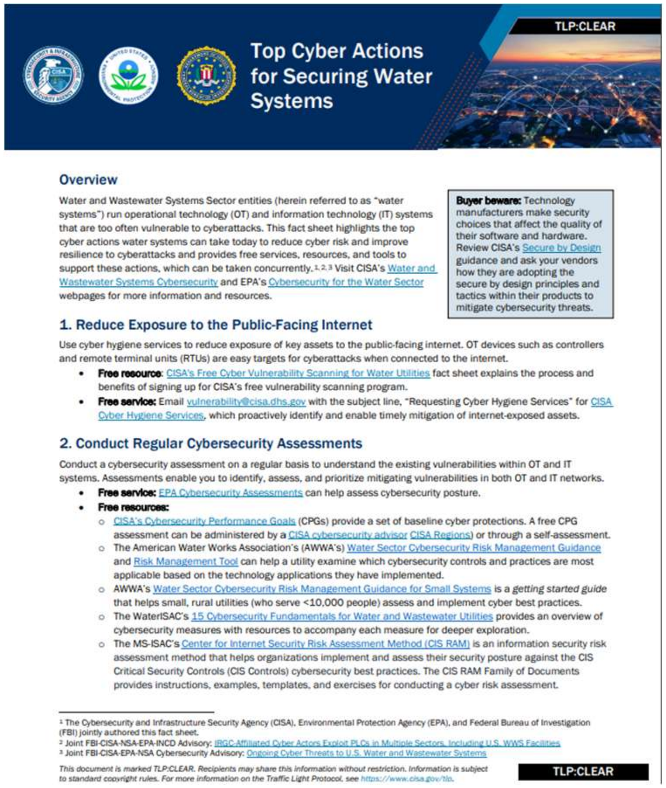
Addressing Cybersecurity in your America's Water Infrastructure Act Emergency Response Plan

Safe Drinking Water Act (SDWA) section 1433, which was amended by America's Water Infrastructure Act (AWIA) section 2013 in 2018, requires community water systems (CWS) serving more than 3,300 people to prepare or revise risk emergency response plans (ERPs) and certify to EPA that this work has been completed. SDWA section 1433(b) states that ERPs must "incorporate findings of the [risk and resilience] assessment' and "shall include strategies and resources to improve the resilience of the system, including…cybersecurity." The ERP must address the overall cybersecurity resilience of the water system and vulnerabilities found in the cybersecurity assessment portion of the RRA. A utility must incorporate the steps of preparing for, responding to, and recovering from a cyber incident in the ERP. To address cybersecurity concerns in the Emergency Response Plan, a utility can start with the Cybersecurity Incident Action Checklist.

Top Cyber Actions for Securing Water Systems

- **Fact sheet that highlights the top cyber actions for water systems to reduce cyber risk.**

- **Includes resources to assist water systems in implementing each cyber action.**



TLP:CLEAR

Top Cyber Actions for Securing Water Systems

Overview

Water and Wastewater Systems Sector entities (herein referred to as "water systems") run operational technology (OT) and information technology (IT) systems that are too often vulnerable to cyberattacks. This fact sheet highlights the top cyber actions water systems can take today to reduce cyber risk and improve resilience to cyberattacks and provides free services, resources, and tools to support these actions, which can be taken concurrently.[1, 2, 3] Visit CISA's Water and Wastewater Systems Cybersecurity and EPA's Cybersecurity for the Water Sector webpages for more information and resources.

Buyer beware: Technology manufacturers make security choices that affect the quality of their software and hardware. Review CISA's Secure by Design guidance and ask your vendors how they are adopting the secure by design principles and tactics within their products to mitigate cybersecurity threats.

1. Reduce Exposure to the Public-Facing Internet

Use cyber hygiene services to reduce exposure of key assets to the public-facing internet. OT devices such as controllers and remote terminal units (RTUs) are easy targets for cyberattacks when connected to the internet.

- **Free resource**: CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.
- **Free service:** Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services" for CISA Cyber Hygiene Services, which proactively identify and enable timely mitigation of internet-exposed assets.

2. Conduct Regular Cybersecurity Assessments

Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.

- **Free service:** EPA Cybersecurity Assessments can help assess cybersecurity posture.
- **Free resources:**
  - CISA's Cybersecurity Performance Goals (CPGs) provide a set of baseline cyber protections. A free CPG assessment can be administered by a CISA cybersecurity advisor CISA Regions) or through a self-assessment.
  - The American Water Works Association's (AWWA's) Water Sector Cybersecurity Risk Management Guidance and Risk Management Tool can help a utility examine which cybersecurity controls and practices are most applicable based on the technology applications they have implemented.
  - AWWA's Water Sector Cybersecurity Risk Management Guidance for Small Systems is a *getting started guide* that helps small, rural utilities (who serve <10,000 people) assess and implement cyber best practices.
  - The WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities provides an overview of cybersecurity measures with resources to accompany each measure for deeper exploration.
  - The MS-ISAC's Center for Internet Security Risk Assessment Method (CIS RAM) is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Critical Security Controls (CIS Controls) cybersecurity best practices. The CIS RAM Family of Documents provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.

[1] The Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and Federal Bureau of Investigation (FBI) jointly authored this fact sheet.
[2] Joint FBI-CISA-NSA-EPA-INCD Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. WWS Facilities
[3] Joint FBI-CISA-EPA-NSA Cybersecurity Advisory: Ongoing Cyber Threats to U.S. Water and Wastewater Systems

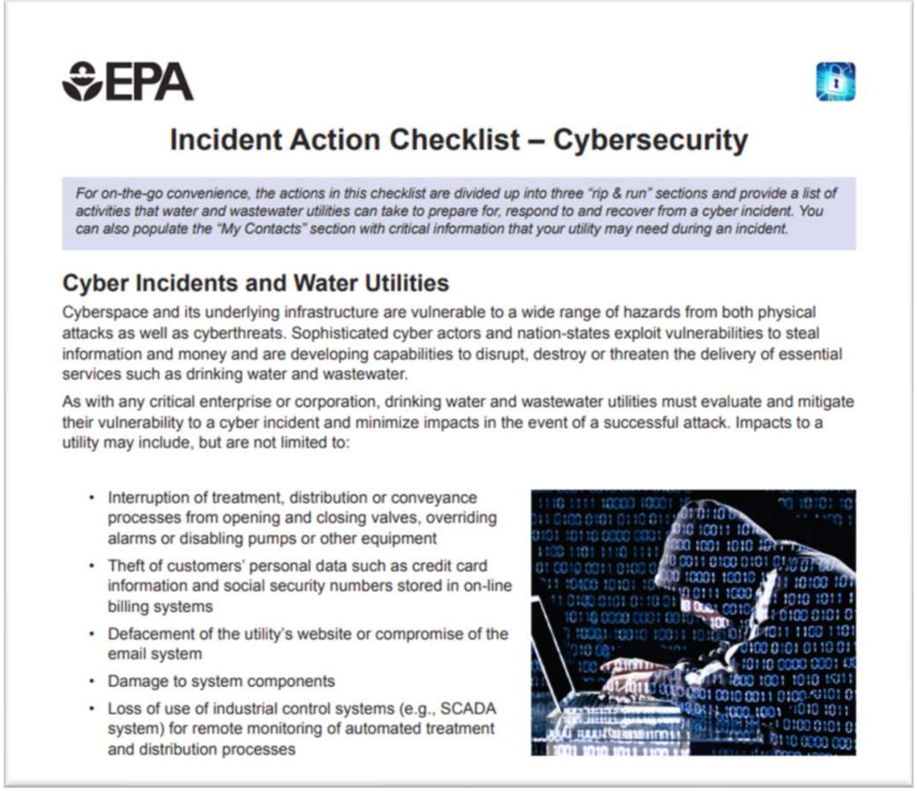
This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

TLP:CLEAR

EPA Water Sector Incident Action Checklist - Cybersecurity

- An actionable list of activities you can take during all phases of a cyber incident, including:
  - Preparation
  - Response
  - Recovery

- This Checklist can be included in your Incident Response Plans for quick access.



EPA

Incident Action Checklist – Cybersecurity

For on-the-go convenience, the actions in this checklist are divided up into three "rip & run" sections and provide a list of activities that water and wastewater utilities can take to prepare for, respond to and recover from a cyber incident. You can also populate the "My Contacts" section with critical information that your utility may need during an incident.

Cyber Incidents and Water Utilities

Cyberspace and its underlying infrastructure are vulnerable to a wide range of hazards from both physical attacks as well as cyberthreats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services such as drinking water and wastewater.

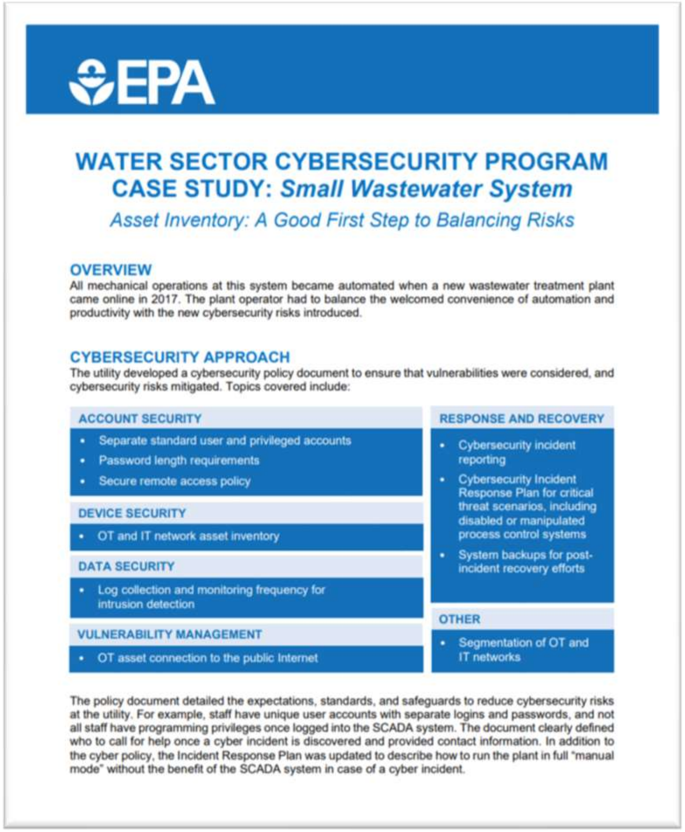
As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to:

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment
- Theft of customers' personal data such as credit card information and social security numbers stored in on-line billing systems
- Defacement of the utility's website or compromise of the email system
- Damage to system components
- Loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes

Water Sector Cybersecurity Program Case Studies

Case Studies highlighting the cybersecurity success stories at water and wastewater utilities.

- Small Combined System
- Small Wastewater System
- Medium Drinking Water System
- Medium Drinking Water System #2
- Medium Combined System
- Large Combined System



EPA

WATER SECTOR CYBERSECURITY PROGRAM
CASE STUDY: *Small Wastewater System*

Asset Inventory: A Good First Step to Balancing Risks

OVERVIEW

All mechanical operations at this system became automated when a new wastewater treatment plant came online in 2017. The plant operator had to balance the welcomed convenience of automation and productivity with the new cybersecurity risks introduced.

CYBERSECURITY APPROACH

The utility developed a cybersecurity policy document to ensure that vulnerabilities were considered, and cybersecurity risks mitigated. Topics covered include:

ACCOUNT SECURITY
- Separate standard user and privileged accounts
- Password length requirements
- Secure remote access policy

DEVICE SECURITY
- OT and IT network asset inventory

DATA SECURITY
- Log collection and monitoring frequency for intrusion detection

VULNERABILITY MANAGEMENT
- OT asset connection to the public Internet

RESPONSE AND RECOVERY
- Cybersecurity incident reporting
- Cybersecurity Incident Response Plan for critical threat scenarios, including disabled or manipulated process control systems
- System backups for post-incident recovery efforts

OTHER
- Segmentation of OT and IT networks

The policy document detailed the expectations, standards, and safeguards to reduce cybersecurity risks at the utility. For example, staff have unique user accounts with separate logins and passwords, and not all staff have programming privileges once logged into the SCADA system. The document clearly defined who to call for help once a cyber incident is discovered and provided contact information. In addition to the cyber policy, the Incident Response Plan was updated to describe how to run the plant in full "manual mode" without the benefit of the SCADA system in case of a cyber incident.

Cybersecurity Training

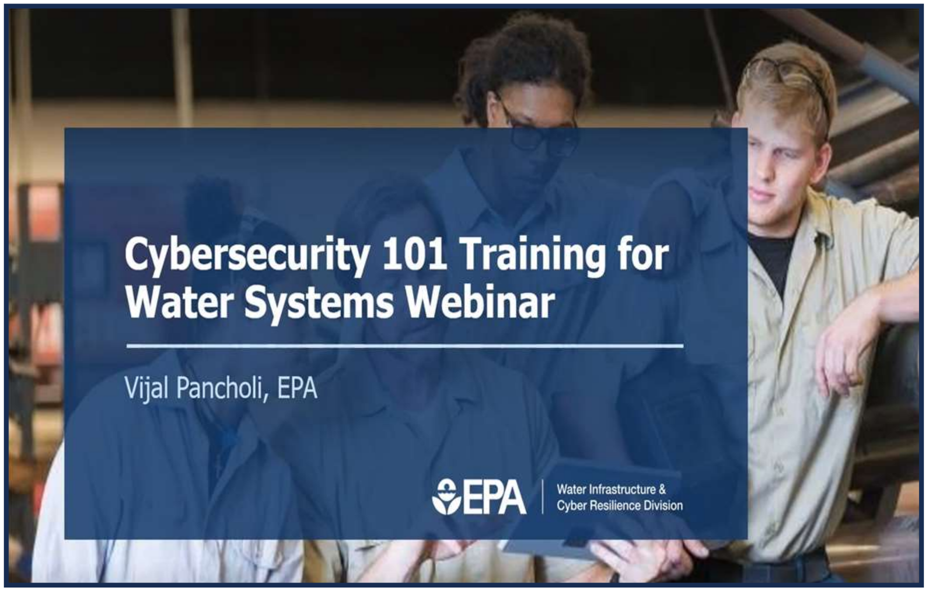
United States
Environmental Protection
Agency

Office of Water

Cybersecurity 101 Webinar for Water Systems

- This webinar reviews basic cybersecurity topics including:
  - Account security
  - Device security
  - Data security
  - Training, and more.

- You can use this webinar during your annual cybersecurity training!



Cybersecurity 101 Training for Water Systems Webinar

Vijal Pancholi, EPA

EPA | Water Infrastructure & Cyber Resilience Division

Link: https://www.youtube.com/watch?v=e2QDbgrojb0

Cybersecurity 102 Webinar for Water Systems

- This webinar reviews basic cybersecurity topics focusing on Operational Technology:
  - IT vs OT
  - Common OT threats
  - Protecting OT systems
  - Incident Response, and more

RECORDING TO BE RELEASED IN OCTOBER

- EPA plans to release quarterly trainings in FY25
  - Cyber 101
  - Cyber 102
  - WCAT training

EPA Cybersecurity Assessment Training for Water and Wastewater Systems

This webinar will demonstrate how to use EPA’s WCAT to conduct a cybersecurity assessment at a water or wastewater system, including:

- Explanation of each Cybersecurity Question
- Potential Documentation to Review
- Questions to Ask
- How to Generate the Assessment Report and Risk Mitigation Plan

Cybersecurity Tabletop Exercises

- EPA offers free cybersecurity tabletop exercises for water and wastewater utilities to test incident response procedures and to provide resources to develop and improve incident response plans.

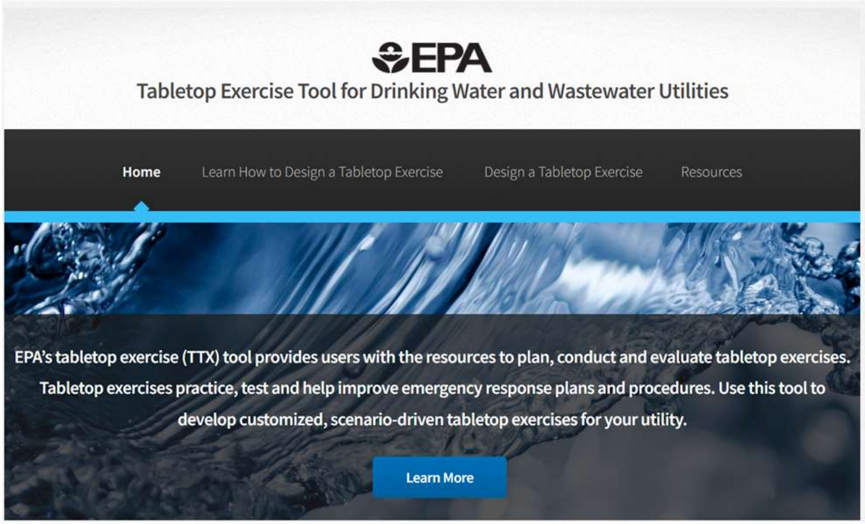
- EPA partners with primacy agencies, state agencies, water sector associations, WARNs, CISA, and FBI.

- Email watercyberta@epa.gov to request a tabletop exercise.

EPA Tabletop Exercise Tool for Utilities

Download this tool to plan and conduct your own Tabletop Exercise. There are many scenarios available including:

- Cybersecurity
- Natural Disasters
- Vandalism
- Contamination



EPA

Tabletop Exercise Tool for Drinking Water and Wastewater Utilities

Home
Learn How to Design a Tabletop Exercise
Design a Tabletop Exercise
Resources

EPA's tabletop exercise (TTX) tool provides users with the resources to plan, conduct and evaluate tabletop exercises. Tabletop exercises practice, test and help improve emergency response plans and procedures. Use this tool to develop customized, scenario-driven tabletop exercises for your utility.

Link: https://www.epa.gov/waterresiliencetraining/develop-and-conduct-water-resilience-tabletop-exercise-water-utilities

Cybersecurity Response

United States
Environmental Protection
Agency

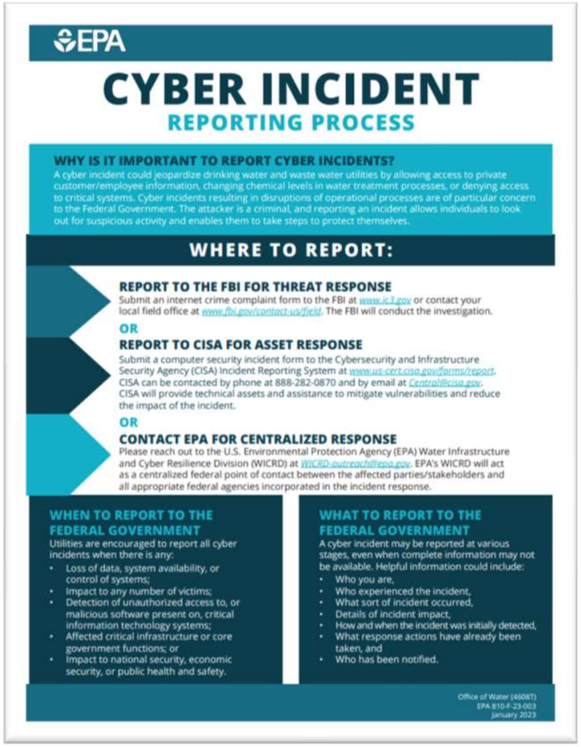
Office of Water

EPA’s Cybersecurity Incident Reporting Fact Sheet

Provides clear guidance on:

- Why it’s important to report
- Where to report
- When to report
- What to report

- It’s encouraged to include this fact sheet in your Cybersecurity Incident Response Plans.



EPA

CYBER INCIDENT

REPORTING PROCESS

WHY IS IT IMPORTANT TO REPORT CYBER INCIDENTS?

A cyber incident could jeopardize drinking water and waste water utilities by allowing access to private customer/employee information, changing chemical levels in water treatment processes, or denying access to critical systems. Cyber incidents resulting in disruptions of operational processes are of particular concern to the Federal Government. The attacker is a criminal, and reporting an incident allows individuals to look out for suspicious activity and enables them to take steps to protect themselves.

WHERE TO REPORT:

REPORT TO THE FBI FOR THREAT RESPONSE

Submit an internet crime complaint form to the FBI at www.ic3.gov or contact your local field office at www.fbi.gov/contact-us/field. The FBI will conduct the investigation.

OR

REPORT TO CISA FOR ASSET RESPONSE

Submit a computer security incident form to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at www.us-cert.cisa.gov/forms/report. CISA can be contacted by phone at 888-282-0870 and by email at Central@cisa.gov. CISA will provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident.

OR

CONTACT EPA FOR CENTRALIZED RESPONSE

Please reach out to the U.S. Environmental Protection Agency (EPA) Water Infrastructure and Cyber Resilience Division (WICRD) at WICRD-outreach@epa.gov. EPA’s WICRD will act as a centralized federal point of contact between the affected parties/stakeholders and all appropriate federal agencies incorporated in the incident response.

WHEN TO REPORT TO THE FEDERAL GOVERNMENT

Utilities are encouraged to report all cyber incidents when there is any:

- Loss of data, system availability, or control of systems;
- Impact to any number of victims;
- Detection of unauthorized access to, or malicious software present on, critical information technology systems;
- Affected critical infrastructure or core government functions; or
- Impact to national security, economic security, or public health and safety.

WHAT TO REPORT TO THE FEDERAL GOVERNMENT

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include:

- Who you are,
- Who experienced the incident,
- What sort of incident occurred,
- Details of incident impact,
- How and when the incident was initially detected,
- What response actions have already been taken, and
- Who has been notified.

Office of Water (4608T)
EPA 810-F-23-003
January 2023

When to Report?

Utilities are encouraged to report all cyber incidents when there is any of the following:

- Loss of data, system availability, or control of systems.
- Impact to any number of victims.
- Detection of unauthorized access to, or malicious software present on, critical information technology systems.
- Affected critical infrastructure or core government functions.
- Impact to national security, economic security, or public health or safety

Where to Report?

Threat Response (FBI)	Asset Response (CISA)	Centralized Response (EPA)
Submit an internet crime complaint form to the FBI at www.ic3.gov or contact your local field office at www.fbi.gov/contact-us/field. The FBI will conduct the investigation.	Submit a computer security incident form to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at www.uscert.cisa.gov/forms/report. CISA can be contacted by phone at 888-282-0870 and by email at Central@cisa.gov. CISA will provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident.	Please reach out to the U.S. Environmental Protection Agency (EPA) Water Infrastructure and Cyber Resilience Division (WICRD) at watercyberta@epa.gov. EPA's WICRD will act as a centralized federal point of contact between the affected parties/stakeholders and all appropriate federal agencies incorporated in the incident response.

What to Report?

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include:

- Who you are.
- Who experiences the incident.
- What sort of incident occurred.
- Details of incident impact.
- How and when the incident was initially detected.
- What response actions have already bene taken.
- Who has been notified.

EPA’s Cybersecurity for the Water Sector Website

https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector