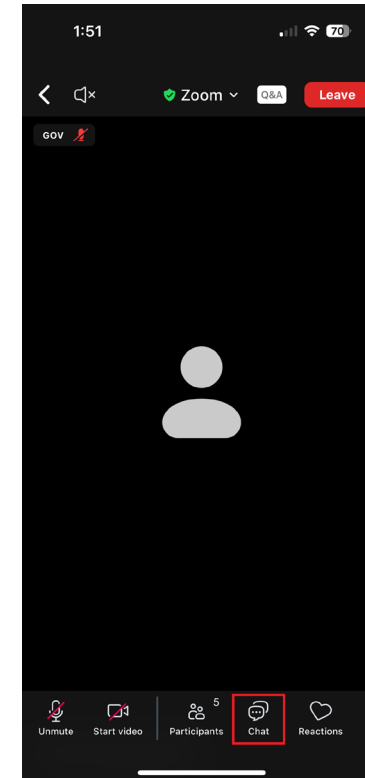
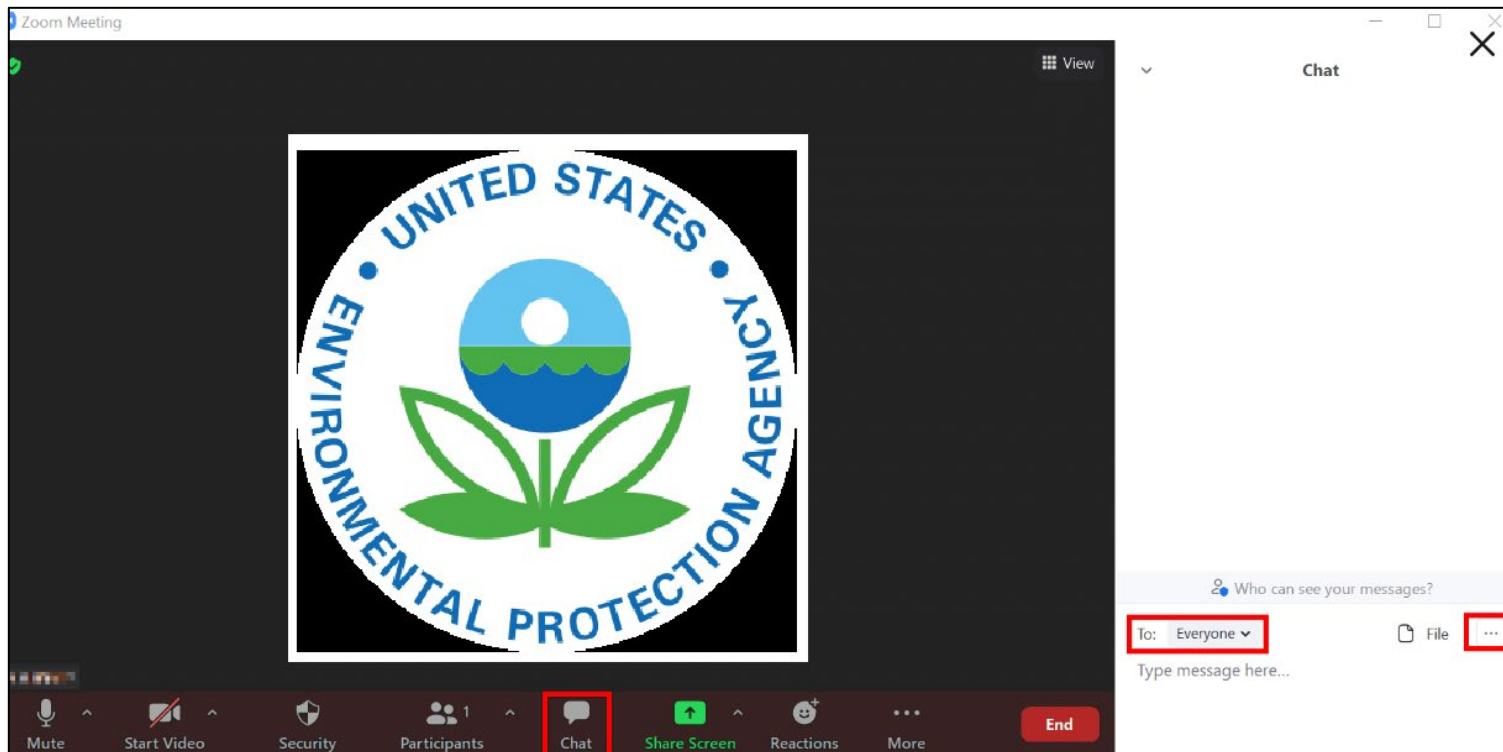


# Webinar Logistics

- Will use chat feature throughout webinar
- Attendees will be sent a post workshop email with presentation slides, Continuing Education Unit (CEU) quiz, and webinar recording





# Updating Your AWIA RRA and ERP

Charlene Kormondy, Cameron Burden, Parker Allen  
EPA Water Infrastructure and Cyber Resilience Division  
February 12, 2025

# Agenda

- Overview of AWIA section 2013/SDWA section 1433
- Creating or Revising an RRA using EPA's VSAT
- Creating or Revising an RRA using EPA's Small System RRA Checklist
- Break
- Checklist of Priority Cybersecurity Practices for Water Systems
- Creating or Revising an ERP using EPA's ERP Template

# Overview of AWIA 2013/SDWA 1433(a) – (f)

- On October 23, 2018, America's Water Infrastructure Act (AWIA) was signed into law. AWIA section 2013 revised Safe Drinking Water Act (SDWA) section 1433.
- Community drinking water systems (CWSs) serving more than 3,300 people shall:
  - Create or update Risk and Resilience Assessments (RRAs) and Emergency Response Plans (ERPs)
  - Submit certifications to EPA by specified deadlines
  - Review and revise RRAs and ERPs and re-certify to EPA every 5 years
  - Coordinate with local emergency planning committees (LEPCs), to the extent possible, when preparing or revising an RRA or ERP
  - Maintain records at the water system for 5 years



# 2025-2026 Certification Deadlines

Population Served	RRA Deadline	ERP Deadline
Over 100,000	March 31, 2025	September 30, 2025
50,000 – 99,999	December 31, 2025	June 30, 2026
3,301 – 49,999	June 30, 2026	December 31, 2026

Check if your PWSID is expected to certify a SDWA section 1433 RRA and ERP in 2025-2026 [here on EPA's website](#).

# RRA Requirements

CWSs serving over 3,300 people must prepare or revise their assessment of the risks to and resilience of the following **specified assets** to **malevolent acts** and **natural hazards**:

1. physical barriers;
2. source water;
3. pipes and constructed conveyances, water collection and intake;
4. pretreatment and treatment;
5. storage and distribution facilities;
6. electronic, computer, or other automated systems (including security of such systems);
7. monitoring practices;
8. financial infrastructure;
9. the use, storage, or handling of chemicals;
10. operation and maintenance of the system;

RRAs include an evaluation of capital and operational needs for risk and resilience management.

# ERP Requirements

CWSs serving over 3,300 people must prepare or revise an ERP that incorporates findings from the RRA. ERPs must include:

1. Strategies and resources to improve resilience, including physical security and cybersecurity;
2. Plans, procedures, and equipment for responding to a malevolent act or natural hazard;
3. Actions, procedures, and equipment to lessen the impact of a malevolent act or natural hazard, including alternative source water, relocation of intakes, and flood protection barriers;
4. Strategies to detect malevolent acts or natural hazards.

# Use of Standards and Tools

- SDWA section 1433 does not require the use of any standards or tools to develop an RRA or ERP
- EPA recommends the use of standards and tools from EPA or other reputable water sector organizations to facilitate development of sound RRAs and ERPs
- No method or tool “guarantees” compliance with SDWA section 1433 - the CWS is responsible for ensuring it complies with all SDWA section 1433 requirements

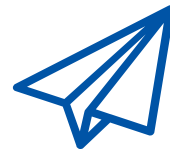


# Three Ways to Certify

1. Electronic submission through secure online portal **\*preferred method\***
2. Email
3. Regular mail

For information on how to certify, visit [www.epa.gov/waterresilience/how-certify-your-risk-and-resilience-assessment-or-emergency-response-plan](http://www.epa.gov/waterresilience/how-certify-your-risk-and-resilience-assessment-or-emergency-response-plan)

**Note: Do NOT send in your actual RRA or ERP to EPA**



# Reviewing and Revising your RRA and ERP

- Update your RRA and ERP to include emerging as well as ongoing threats
- EPA's website, [www.epa.gov/waterresilience](http://www.epa.gov/waterresilience), has resources on many threats of concern to water systems, including cyber threats, supply chain disruptions, and more



# Creating or Revising a Risk and Resilience Assessment (RRA) using EPA's Vulnerability Self Assessment Tool (VSAT)

Charlene Kormondy, EPA Water Infrastructure and Cyber Resilience Division

# VSAT

- VSAT is an e-tool that water utilities may use to develop a SDWA 1433 RRA
- Access VSAT here <https://www.epa.gov/waterresilience/vulnerability-self-assessment-tool-conduct-drinking-water-or-wastewater-utility> (overview webpage) or here <https://vsat.epa.gov/vsat/> (tool webpage)




# VSAT: Required vs. Optional Sections

VSAT Page	Requirements for SDWA section 1433-Compliant Risk and Resilience Assessment
Utility Type	Required
Utility Information	Required
Utility Resilience Index	Required
Qualitative Risk Assessment	Required
Quantitative Risk Assessment	Optional, but recommended
Countermeasure Analysis	
Report	Required
SDWA Section 1433 Certification	Self-Certification Instructions Provided

# VSAT Terminology

- **Threat**
  - Malevolent Acts (See [Baseline Information on Malevolent Acts for Community Water Systems Version 3.0](#) for more information)
  - Natural Hazards
  - Dependency/Proximity Threats
- **Asset**
- **Asset-threat pair**
- **Countermeasures**





# Training Scenario: Example VSAT RRA

VSAT analysis file available upon request to [dwresilience@epa.gov](mailto:dwresilience@epa.gov)

# Training Scenario Utility Overview

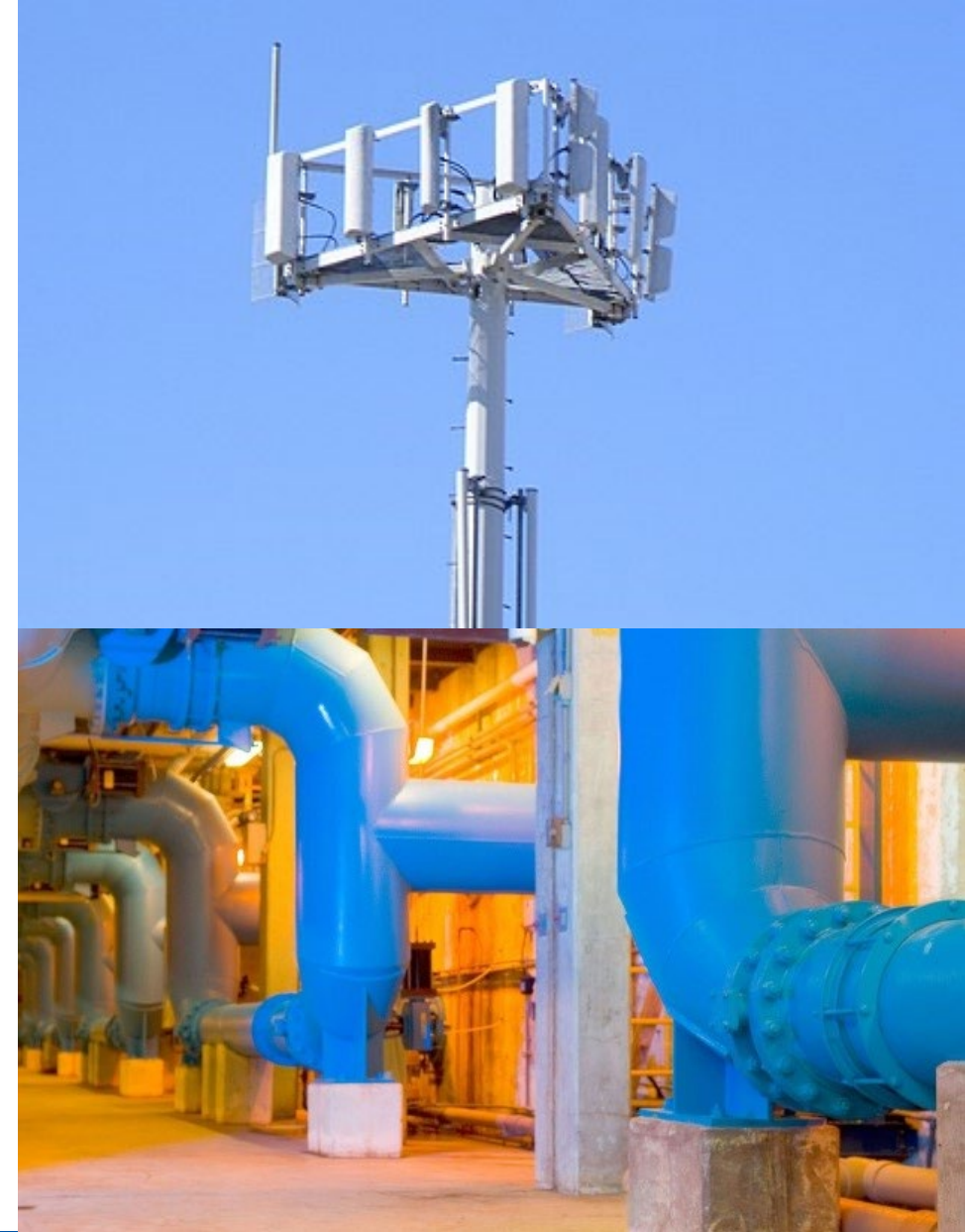
- **Utility Name:** Spring View Water District
- **Size and Location:** Medium-sized (75,000 people served) drinking water utility the far south suburbs of Chicago, Illinois.
- **Critical assets:**
  - 14 pumping stations
  - SCADA system
  - Water treatment plant
  - IT business and financial systems





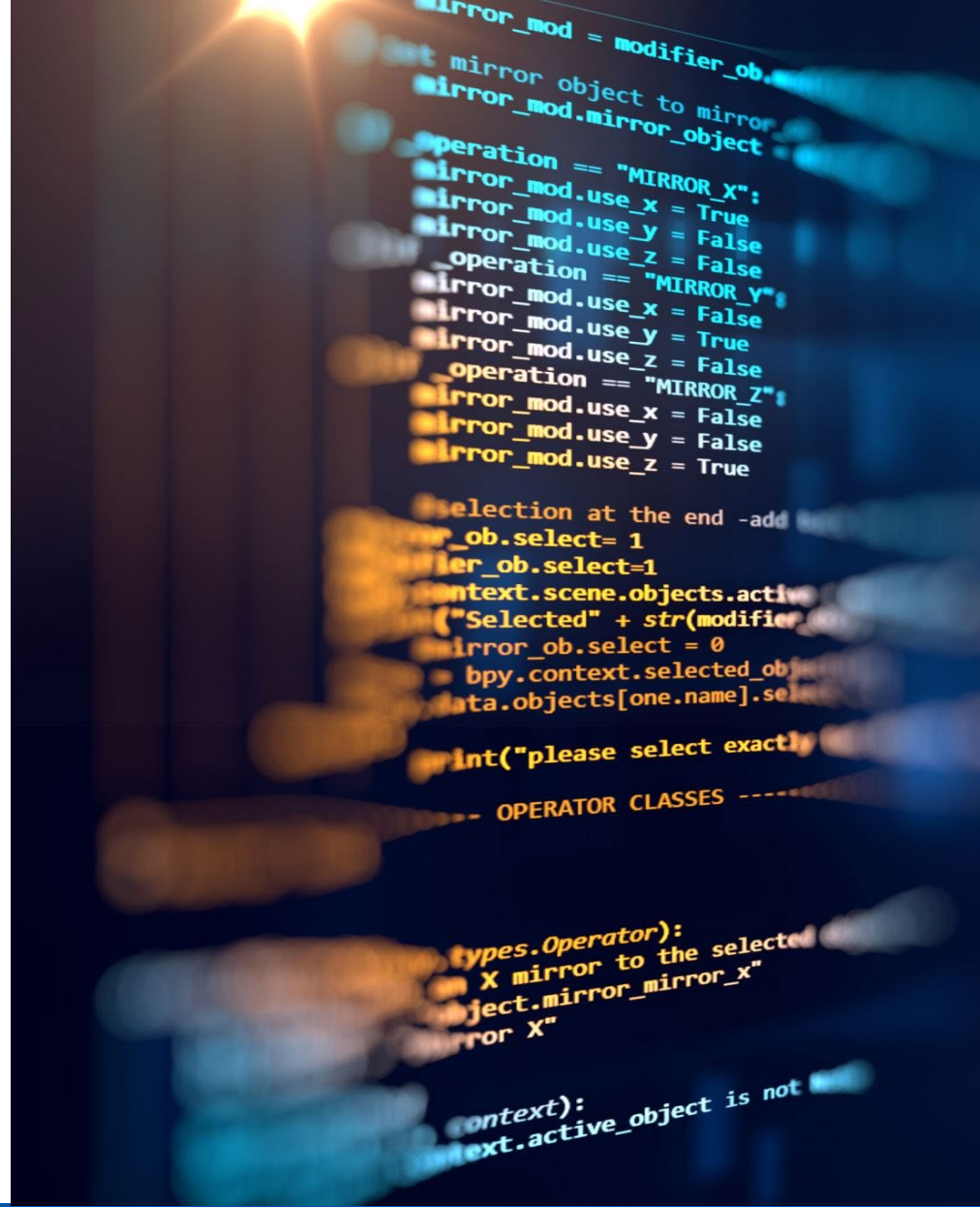
# Hypothetical Threat: Cell Tower Cyberattack

- Spring View Water District relies on cellular provider to remotely operate its pumping stations
- Cell tower attack by malicious actor could prevent remote (cellular) operation of a critical pumping station



# Hypothetical Threat: Ransomware Cyberattack

- Ransomware attack propagates through Spring View Water District's entire local area network
- Ransomware attack prevents Spring View Water District's communications with customers and the access to financial systems
- Utility systems connected to the network are also impacted (e.g., laboratory equipment, work order systems)



# Hypothetical Threat: Flooding

- Spring View Water District is located near and draws its source water from the Winding River
- 100-year flooding event occurs
- Electrical components of the utility's online water quality monitoring equipment (not elevated) could be damaged
- This could disable continuous monitoring of the finished water leaving the treatment plant

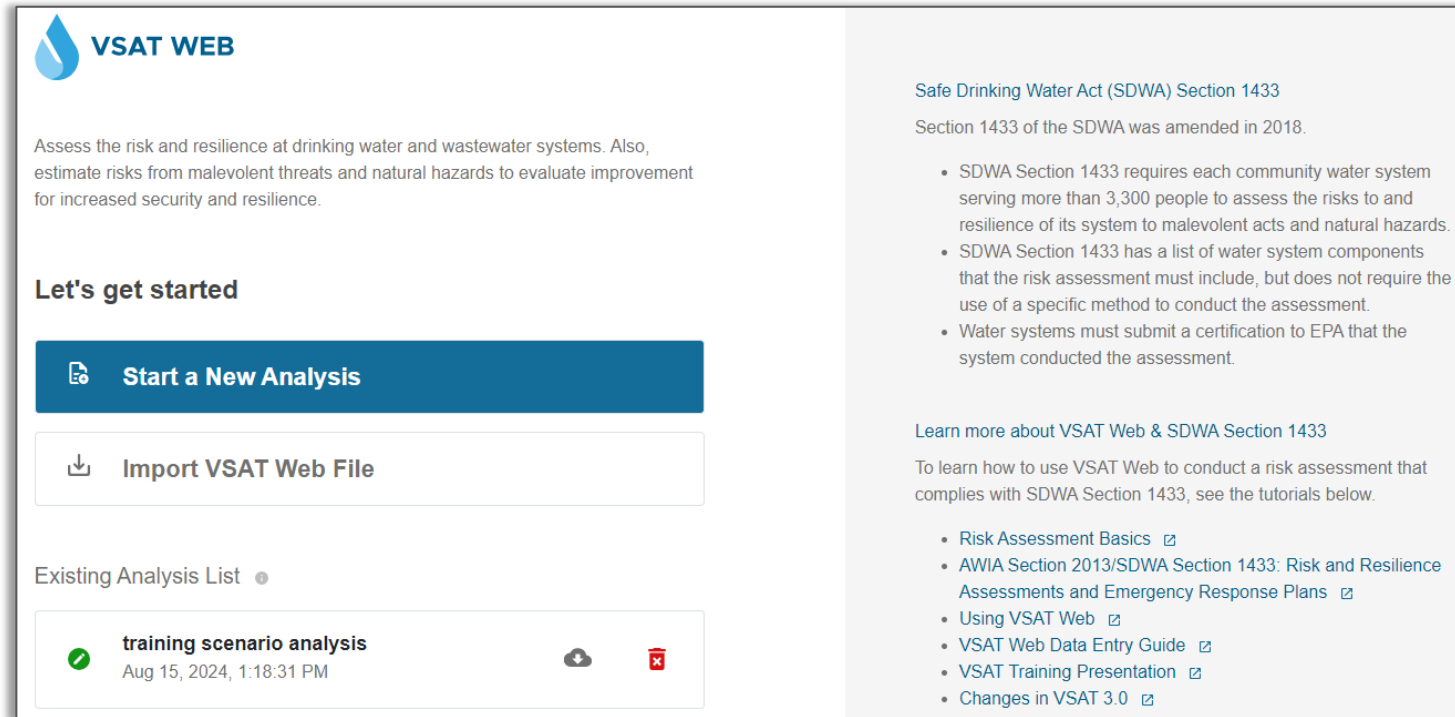


# VSAT Web Home Screen

- <https://vsat.epa.gov/vsat/>
- Start a new analysis or import a VSAT Web file
- Save locally (download or email)

## CAUTION Regarding Encryption Password:

EPA is unable to recover or reset a forgotten encryption password. Store password in a secure location. Save PDF report so you have a record of data input into VSAT in case you lose your password.




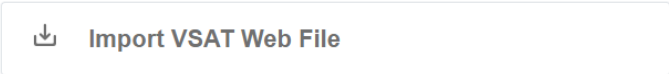
The screenshot shows the VSAT Web interface. At the top left is the VSAT WEB logo. Below it is a paragraph: "Assess the risk and resilience at drinking water and wastewater systems. Also, estimate risks from malevolent threats and natural hazards to evaluate improvement for increased security and resilience." Underneath is the heading "Let's get started" followed by two buttons: "Start a New Analysis" (with a document icon) and "Import VSAT Web File" (with a download icon). Below these is an "Existing Analysis List" section with a dropdown arrow. It contains one entry: "training scenario analysis" with a green checkmark icon, the date "Aug 15, 2024, 1:18:31 PM", and icons for download and delete. On the right side of the screen, there is a section titled "Safe Drinking Water Act (SDWA) Section 1433" with a sub-heading "Section 1433 of the SDWA was amended in 2018." followed by a bulleted list of three points. Below this is a link "Learn more about VSAT Web & SDWA Section 1433" and a paragraph: "To learn how to use VSAT Web to conduct a risk assessment that complies with SDWA Section 1433, see the tutorials below." followed by a bulleted list of six links with external icons.

**VSAT WEB**




Assess the risk and resilience at drinking water and wastewater systems. Also, estimate risks from malevolent threats and natural hazards to evaluate improvement for increased security and resilience.

**Let's get started**

 **Start a New Analysis**

 **Import VSAT Web File**

Existing Analysis List ▾

 **training scenario analysis**    
Aug 15, 2024, 1:18:31 PM







**Safe Drinking Water Act (SDWA) Section 1433**

Section 1433 of the SDWA was amended in 2018.

- SDWA Section 1433 requires each community water system serving more than 3,300 people to assess the risks to and resilience of its system to malevolent acts and natural hazards.
- SDWA Section 1433 has a list of water system components that the risk assessment must include, but does not require the use of a specific method to conduct the assessment.
- Water systems must submit a certification to EPA that the system conducted the assessment.

[Learn more about VSAT Web & SDWA Section 1433](#)

To learn how to use VSAT Web to conduct a risk assessment that complies with SDWA Section 1433, see the tutorials below.

- [Risk Assessment Basics](#) 
- [AWIA Section 2013/SDWA Section 1433: Risk and Resilience Assessments and Emergency Response Plans](#) 
- [Using VSAT Web](#) 
- [VSAT Web Data Entry Guide](#) 
- [VSAT Training Presentation](#) 
- [Changes in VSAT 3.0](#) 

# Dialog Box: Changes in VSAT Web 3.0

- Value of Statistical Life default updated to \$11.2 million (2024 dollars)
- Malevolent act changes:
  - Default threat likelihood ranges
  - Threat type changes
    - Accidental water contamination removed
    - A single cyberattack threat type

### Changes in VSAT Web 3.0

The default value of statistical life (VSL) for a newly created VSAT analysis has been updated to \$11.2 million (2024 dollars). This value may be viewed and modified in the Settings dialog after creating or opening an existing analysis.

The following changes to malevolent act threat types and default threat likelihood values displayed in VSAT have been made based on revisions to the Baseline Information on Malevolent Acts for Community Water Systems document version 3.0 released in May 2024.

- Most estimates of default threat likelihood were replaced with order of magnitude ranges.
- While EPA developed the new default threat likelihood ranges for drinking water, EPA views them as generally applicable to wastewater systems as well and provides the same ranges for analysts to consider for these systems.
- Accidental contamination of source and finished water were eliminated as malevolent act threat categories.
- Cyberattacks on business enterprise systems and process control systems were combined into a single category of cyberattack.

#### Cyberattack Threats

As part of the baseline risk assessment, VSAT Web now provides a cybersecurity vulnerability likelihood assessment for assets assigned the malevolent threat type "Cyberattack". For this threat type, the utility

# Dialog Box: Malevolent Acts Threat Changes

- Displays if existing VSAT analysis is impacted by threat type changes
- Impacted threats are displayed
- May 'Keep Existing' or 'Delete' prior Cyber Attack threats

Malevolent Acts Threat Changes

Your VSAT analysis is impacted by changes to malevolent act threat types. Please review the following information.

- Accidental contamination of source and finished water were eliminated as malevolent act threat categories.
- Cyberattacks on business enterprise systems and process control systems were combined into a single category of cyberattack.

Accidental Water Contamination Threats

Your VSAT analysis contains previously existing accidental water contamination threat assessments.

- Chollas Lake --- Contamination of Source Water - Accidental
- Water main lines --- Contamination of Finished Water - Accidental

Accidental water contamination threats and associated data will be deleted from you VSAT analysis.

Cyberattack Threats

Your VSAT analysis contains previously existing cyberattack threat assessments. If you would like to utilize the new cybersecurity vulnerability likelihood assessment to estimate how vulnerable your utility network is to cybersecurity attacks, you will need to delete the existing cyberattack assessments. If you choose to keep the existing cyberattack assessments, the risk assessment results and countermeasure information associated with these asset-threat pairs will be preserved, but they cannot be modified.

Your VSAT analysis file contains the following asset/threat pairs with existing cyberattack threat assessments:

- Billing system --- Cyber Attack on Business Enterprise Systems
- Desalination System --- Cyber Attack on Process Control Systems

**CAUTION: If you are unsure whether you want to delete your existing cyberattack threats and associated data, click the Keep Existing button.** You may then review and download your Risk Results Report to maintain a copy of your prior cyberattack threat data. The above cyberattack threats may then be deleted on the Quantitative Risk Assessment screen, allowing you to utilize the new Cyberattack threat type.

Would you like to keep the existing cyberattack assessments, or delete them and utilize the cybersecurity vulnerability likelihood assessment?

Keep Existing Delete

# Utility Overview

Identify the utility type and input utility details.

**VSAT WEB** August 15, 2024 training scenario analysis

## Utility Overview

### Type of Utility

Please identify whether the risk assessment will be conducted on a drinking water or a wastewater utility. Combined utilities must conduct separate analyses for drinking water and wastewater operations.

**Drinking Water Utility**  
A drinking water utility provides water for human consumption through pipes or other constructed conveyances to at least 15 service connections or serves an average of at least 25 people for at least 60 days a year.

**Wastewater Utility**  
A wastewater utility conveys wastewater in a combined sewer or sanitary sewer, treats the water at a wastewater treatment plant, and discharges the treated wastewater into receiving water via an effluent pipe.

### Utility Information

Please enter the utility's information below. VSAT uses this information to determine the frequency of certain natural hazards and economic impact values.

Utility Name: Spring View Water District

State: Illinois Zip Code: 60417

Population Served: 75,000 Ownership:  Public  Private

Avg. Daily Water Service (MGD): 25 Avg. Rate (\$/1000 Gallons): \$4.00

Comments and notes: Risk assessment for SDWA section 1433 certification.

# Utility Resiliency Index (URI)

Assesses capability to respond to and recover from an incident impacting critical operations

The screenshot shows the VSAT WEB interface for the Utility Resilience Index. The left sidebar contains a navigation menu with the following items: Utility Overview, Utility Resilience Index (highlighted), Qualitative Risk Assessment, Quantitative Risk Assessment, Countermeasure Risk Assessments, Risk Results Report, SDWA Section 1433 Certification, and Tutorials & Guides. The main content area is titled "Utility Resilience Index" and includes a descriptive paragraph, a footnote, a "Show more" link, and a section for "1. Emergency Response Plan (ERP)" with a radio button selection form.

**VSAT WEB** August 15, 2024 training scenario analysis

## Utility Resilience Index

The Utility Resilience Index (URI) is a risk management tool that can assess a utility's capability to respond to and recover from an incident that impacts critical operations.<sup>1</sup> Completing the URI involves selecting statements that best match the utility's current capabilities with respect to 12 indicators. Indicators represent attributes that help to calculate a utility's ability to absorb and/or cope with an incident and return to normal operations as quickly as possible. VSAT then calculates an overall value for the URI, and the results are included in the VSAT Assessment Report.

<sup>1</sup> Adapted from Morley, K. M. (2012). *Evaluating resilience in the water sector: Application of the Utility Resilience Index (URI)*. ([www.worldcat.org/oclc/801849602](http://www.worldcat.org/oclc/801849602)) and used with permission.

**How to complete the Utility Resilience Index (URI) risk assessment?** Show more

### 1. Emergency Response Plan (ERP)

An ERP provides a tactical level plan for immediate response to incidents of all types.

Select the statement below that best describes the utility's ERP:

- No ERP or ERP status unknown
- An ERP has been developed**
- Staff have been trained on the ERP (e.g., Table Top Exercises)
- Resource typed assets/teams defined and inventoried
- Functional exercises on the ERP have been conducted



# Spring View Water District URI Selections

1. **Emergency Response Plan (ERP):** An ERP has been developed
2. **National Incident Management System (NIMS) Compliance:** ICS 200/300 provided to key staff
3. **Mutual Aid and Assistance (MAA):** Intrastate (e.g., WARN)
4. **Emergency Power for Critical Operations (EPCO):** Up to 24 hours of backup power
5. **Minimum Daily Demand/Treatment (MDDT):** 25 hours to 48 hours
6. **Critical Parts and Equipment (CPE):** 1 week to less than 3 weeks
7. **Critical Staff Resilience (CSR):** Greater than 50 to 75%
8. **Business Continuity Plan (BCP):** BCP completed
9. **Utility Bond Rating (UBR):** AA
10. **Government Accounting Standards Board (GASB) Assessment:** 41 to 60% assessed
11. **Unemployment:** > +/- 2 National Average
12. **Median Household Income (MHI):** +/- 5% State Median

# Qualitative Risk Assessment

## Asset categories

1. Physical barriers
2. Source water
3. Pipes and Constructed Conveyances, Water Collection, and Intake
4. Pretreatment and Treatment
5. Storage and Distribution Facilities
6. Electronic, Computer, or other Automated Systems (including security)
7. Monitoring Practices
8. Financial Infrastructure
9. The Use, Storage, or Handling of Chemicals
10. The Operation and Maintenance of the Utility

# Spring View Water District Qualitative Risk Assessment

Asset Category	Malevolent Act?	Natural Hazards?	Describe Potential Impact, or Reason for No Selection
Physical Barriers	<input type="checkbox"/>	<input type="checkbox"/>	This was not selected as a high risk asset because the utility recently underwent a thorough update to its physical security system (updated alarm system, locks, card readers, etc.). Thus, the utility is confident that malevolent acts are natural hazards pose a relatively low threat to physical barriers.
Source Water	<input type="checkbox"/>	<input type="checkbox"/>	Enter reason... Enter reason for no threat selection.
Pipes and Constructed Conveyances, Water Collection, and Intake	<input type="checkbox"/>	<input type="checkbox"/>	Enter reason... Enter reason for no threat selection.
Pretreatment and Treatment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter assets, threats posing significant risk, and potential consequences... Describe potential impacts including assets, threats, and potential consequences.
Storage and Distribution Facilities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A cell tower experiences a cyberattack that impairs pumping station operation resulting in significant utility and regional economic consequences.
Electronic, Computer, or other Automated Systems (including the security of such systems)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The local area network (LAN) suffers a ransomware attack which propagates throughout the entire LAN, impacting laboratory equipment and taking the work order system offline. The outages result in significant expenses to the utility.
Monitoring Practices	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The OWQM system is damaged by flooding resulting in significant utility and regional economic consequences.
Financial Infrastructure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Ransomware attack on the LAN takes the billing system offline impacting customer communications and bill payments. The outages result in significant expenses to the utility.

# Quantitative Assessment: Perform Baseline Risk Assessment for Each Asset/Threat Pair

1. Estimate Public Health and Economic **Consequences**
  - VSAT's *WHEAT Calculator* can help you estimate this
2. Estimate **Threat** Likelihood
  - VSAT provides a range of threat likelihoods for you to consider as a starting point
3. Estimate **Vulnerability** Likelihood
  - VSAT's *Cybersecurity Vulnerability Assessment Calculator* can help you estimate this for cyber threats
  - VSAT's *Vulnerability Likelihood Calculator* can help you estimate this for non-cyber threats

**Risk = Threat x Vulnerability x Consequence**

# Assign Threats (Quantitative Risk Assessment)

Enter assets and assign threats

The screenshot displays the 'High Risk Asset Categories' interface. At the top, there is a table with columns for 'Category Name', 'Status', and 'Delete'. Below this, the 'Storage and Distribution Facilities' category is expanded, showing a 'Pump station' asset with a status of 'In Progress' and a risk of '\$0.00'. An arrow points from the 'Add Threat' button for the 'Pump station' to a 'Threat Assignment' modal window.

The 'Threat Assignment' modal window contains the following fields and options:

- Threat Category:** Select a threat category for this asset. Radio buttons are provided for:
  - Malevolent Acts
  - Natural Hazards
  - Dependency/Proximity Threats
- Threat Type:** Select the type of threat within the category. A dropdown menu is shown with 'Select Threat Type' and a downward arrow. An arrow points from this dropdown to a list of threat types.
- Description:** Provide a brief description of the threat. (200 characters). A text input field contains 'Loss of cellular communication to pump station' with '154 characters left' remaining.

The dropdown menu for 'Threat Type' lists the following options:

- Assault on Utility - Physical
- Intentional Contamination of Finished Water
- Intentional Contamination of Source Water
- Theft or Diversion - Physical
- Cyberattack** (highlighted)
- Directed/Sabotage - Physical
- Custom Threat

# Estimate Public Health and Economic Consequences (Baseline Quantitative Risk Assessment)

Baseline Risk Assessment

Consequences  
Estimate the public health and economic consequences

Fatalities	Injuries
<input type="text" value="0"/>	<input type="text" value="0"/>
Utility Financial Consequences	Regional Economic Consequences
<input type="text" value="\$100,000"/>	<input type="text" value="\$400,000"/>

The WHEAT calculator is a simplified version of the Water Health and Economic Analysis Tool (WHEAT), developed by EPA to assist with estimating fatalities, injuries, and utility financial and regional economic consequences. [The full tool, including documentation, is available here.](#)

**Help Information**  
Fatalities and significant injuries that are directly attributed to the utility assets, such as from contaminated water or a release of a hazardous gas.  
VSAT converts fatalities and significant injuries to monetary risk values. [Described here.](#)  
Utility financial and regional economic losses due to service interruptions and emergency response and recovery activities.

Public health consequence is calculated by multiplying fatalities and injuries by Value of a Statistical Life (VSL) and Value of a Statistical Injury (VSI) values.

Settings

Consequence Determination

Value of Statistical Life (VSL)\*

Value of a Statistical Injury

\*A default VSL value of \$11.2 million (2024 dollars) is provided based on converting a central estimate of VSL of \$7.4 million (2006 dollars) using the GDP deflator index per [EPA's Guidelines for Preparing Economic Analyses](#), Appendix B: Mortality Risk Valuation Estimates.

# Estimate Cybersecurity Threat and Vulnerability Likelihood (Baseline Quantitative Risk Assessment)

- 1. Select cybersecurity controls and practices already implemented
- 2. Click Calculator (VSAT calculates likelihood value based on selections)

**Threat Likelihood**  
Estimate the likelihood of the risk occurring

Annual Threat Likelihood Estimate

For assistance with a site-specific estimate for a malevolent act, you may consult U.S. EPA's Baseline Information on Malevolent Acts for Community Water Systems.

**Vulnerability Likelihood**  
Estimate the vulnerability likelihood percentage, which is the probability (from 20 to 99 percent) that if a malevolent actor carried out a cyberattack on the utility, then the utility would experience the consequences you projected earlier.

**Cybersecurity Vulnerability Assessment Calculator**

The Cybersecurity Vulnerability Assessment Calculator helps assess a utility's vulnerability to cyberattacks. Completing the assessment involves identifying cybersecurity controls and practices already implemented by the utility to protect IT and OT assets or aid in responding to a cybersecurity incident.

**Select Controls**

**Calculator**

Estimate (%)

**Baseline Cybersecurity Controls**

Select the cybersecurity controls and practices that are currently implemented at the water utility.

Note: Priority cybersecurity best practices for Water and Wastewater Systems (WWSs) are denoted with an asterisk\*.

**1. IDENTIFY**

- Maintain an updated inventory of all OT and IT network assets\*
- Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the WWS\*
- Have a named role/position/title that is responsible for planning, resourcing, and executing OT-specific cybersecurity activities
- Provide regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors
- Patch or otherwise mitigate known vulnerabilities within the recommended timeframe\*
- Require that all OT vendors and service providers notify the WWS of any security incidents or vulnerabilities in a risk-informed timeframe
- Include cybersecurity as an evaluation criterion for the procurement of OT and IT assets and services

**2. PROTECT**

- Change default passwords\*
- Require a minimum length for passwords\*
- Require unique and separate credentials for users to access OT and IT networks\*
- Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors\*

# Estimate Non-Cyber Threat and Vulnerability Likelihood (Baseline Quantitative Risk Assessment)

- **Threat likelihood:** Probability that the threat will occur in a one-year period, considering the capabilities of existing countermeasures
- **Vulnerability likelihood:** Estimated percentage (%) that the threat would result in the consequences projected earlier, if the threat occurred, given effectiveness of existing countermeasures

### Threat Likelihood

Estimate the likelihood of the risk occurring


Annual Threat Likelihood Estimate

Default Threat Likelihood Range: 0.01 – 0.1 ?

For assistance with a site-specific estimate for a malevolent act, you may consult U.S. EPA's Baseline Information on Malevolent Acts for Community Water Systems.

### Vulnerability Likelihood

Estimate the vulnerability likelihood percentage

 **Calculator**

Estimate (%)

The Calculator helps assessing the capabilities of any existing countermeasures your utility may have to detect, delay, and respond to malevolent acts, or prepare for, respond to, and recover from natural hazards and dependency or proximity threats.



# Quantitative Risk Assessment: Cyber Attack Scenarios

Asset-Threat Pair		Baseline consequences and likelihood of threat and vulnerability			
Asset	Threat	Public Health Consequences	Economic Consequences	Threat Likelihood	Vulnerability Likelihood
<b>Pump Station</b>	Cyberattack – Loss of cellular communication to pump station	Fatalities: 0 Injuries: 0	Utility Financial: \$100,000 Regional Economic: \$400,000	Annual Baseline Estimate: 1	Baseline Estimate: 90%
<b>Business enterprise systems (i.e., email, lab equipment, work order system)</b>	Cyberattack – Ransomware attack	Fatalities: 0 Injuries: 0	Utility Financial: \$300,000 Regional Economic: \$0	Annual Baseline Estimate: 1	Baseline Estimate: 99%
<b>Billing System</b>	Cyberattack – Ransomware attack	Fatalities: 0 Injuries: 0	Utility Financial: \$200,000 Regional Economic: \$0	Annual Baseline Estimate: 1	Baseline Estimate: 99%

# Quantitative Risk Assessment: Flood Scenario

Asset-Threat Pair		Baseline consequences and likelihood of threat and vulnerability			
Asset	Threat	Public Health Consequences	Economic Consequences	Threat Likelihood	Vulnerability Likelihood
Online Water Quality Monitoring Sensors	Flood – F1 – Flood – 100 Year	Fatalities: 0 Injuries: 0	Utility Financial: \$76,000 Regional Economic: \$80,944,600	Annual Baseline Estimate: 0.01	Baseline Estimate: 72%

# Perform Countermeasure Analysis (Optional)

The countermeasure analysis is a two-step process.

1. Select potential countermeasures.
2. Perform improvement risk assessment for each asset/threat pair.

Assess improvement with potential countermeasures in place:

- Enter Public Health and Economic Consequences
  - *WHEAT Calculator*
- Estimate Threat Likelihood
- Estimate Vulnerability Likelihood
  - *Vulnerability Likelihood Calculator*
  - *Cybersecurity Vulnerability Assessment Calculator*

# Potential Countermeasure Costs

Countermeasure costs may be specified.

- Utility Overview
- Utility Resilience Index
- Qualitative Risk Assessment
- Quantitative Risk Assessment
- Countermeasure Risk Assessments
- Potential Countermeasure Costs
- Countermeasure Packages
- Risk Results Report
- SDWA Section 1433 Certification
- Tutorials & Guides

### Potential Countermeasure Costs

To perform cost-benefit analyses for the selected potential countermeasures, please click on the edit icon to the left of the countermeasure name and enter below both the capital and the annual operations and maintenance (O&M) costs associated with the potential countermeasures. VSAT will then calculate an annualized cost from the entered values, using a 4% finance rate over 10 years to determine the annualized capital cost. For any potential cybersecurity countermeasures being assessed, only the annual operations and maintenance (O&M) cost is required.

#### Potential Countermeasure

Edit	Countermeasure Name	Capital Cost	Annualized Cost	
	Elevated OWQM sensors	\$5,000.00	\$616.45	▼
	Flood wall	\$21,000.00	\$2,589.11	▼
	Water/Wastewater Agency Response Network (WARN)	\$0	\$0	▼
	Waterproof boxes for OWQM equipment	\$1,500.00	\$184.94	▼

#### Potential Cybersecurity Countermeasure

Edit	Countermeasure Name	Annualized Cost	
	Change default passwords	\$0	▼
	Collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation	\$2,500.00	▼

# Countermeasure Packages

Countermeasure packages save time by grouping potential countermeasures. Can be applied to multiple asset-threat pairs.

The screenshot displays a web interface for managing countermeasure packages. On the left is a navigation sidebar with options like 'Utility Overview', 'Countermeasure Risk Assessments', and 'Countermeasure Packages'. The main content area is titled 'Countermeasure Packages' and includes an explanatory paragraph. Below this is a table of packages, with one package selected: 'Flood Threat Mitigation'. A sub-table lists 'Potential Countermeasures' with columns for 'Risk Reduction' and 'Total Annualized Cost'.

Package Name	Risk Reduction	Total Annualized Cost	Delete
<b>Flood Threat Mitigation</b> Assessing the potential countermeasures that require less capital expenditure.	\$233,339.33	\$801.39	

Potential Countermeasures	Risk Reduction	Total Annualized Cost
Elevated OWQM sensors	\$58,334.83	\$616.45
Water/Wastewater Agency Response Network (WARN)	\$58,334.83	\$0.00
Waterproof boxes for OWQM equipment	\$116,669.66	\$184.94

# Perform Countermeasure Analysis

## Cyberattack – Improvement risk data entered for training scenario

Asset-Threat Pair		Improved consequences and improved likelihood of threat and vulnerability			
Asset	Threat	Public Health Consequences	Economic Consequences	Threat Likelihood	Vulnerability Likelihood
<b>A/T Pair #1 Pump Station</b>	Cyberattack – Loss of cellular communication to pump station	YES Fatalities: 0 Injuries: 0	YES Utility Financial: \$50,000 Regional: \$200,000	YES Annual Improvement Estimate: 0.08	YES Improvement Estimate: 80%
<b>A/T Pair #2 Business enterprise systems (i.e., email, lab equipment, work order system)</b>	Cyberattack – Ransomware attack	YES Fatalities: 0 Injuries: 0	YES Utility Financial: \$75,000 Regional Economic: \$0	YES Annual Improvement Estimate: 0.1	YES Improvement Estimate: 50%
<b>A/T Pair #3 Billing System</b>	Cyberattack – Ransomware attack	YES Fatalities: 0 Injuries: 0	YES Utility Financial: \$50,000 Regional Economic: \$0	YES Annual Improvement Estimate: 0.1	YES Improvement Estimate: 50%

# Perform Countermeasure Analysis

**Flood – Improvement risk data entered for training scenario**

Asset-Threat Pair		Improved consequences and improved likelihood of threat and vulnerability			
Asset	Threat	Public Health Consequences	Economic Consequences	Threat Likelihood	Vulnerability Likelihood
<b>A/T Pair #4 Online Water Quality Monitoring Sensors</b>	Flood – F1 – Flood – 100 Year	YES Fatalities: 0 Injuries: 0	YES Utility Financial: \$0 Regional Economic: \$0	YES Annual Improvement Estimate: 0.01	YES Improvement Estimate: 3%

# Risk and Resilience Summary Report

[Go to Final Report](#) →

- Report summarizes all data entered for the assessment.
- Provides analysis of quantitative risk, qualitative risk, and countermeasures.
- May be downloaded or emailed to retain a record of data and results.

The screenshot displays a web application interface for a Risk and Resilience Summary Report. On the left is a sidebar menu with the following items: Utility Overview, Utility Resilience Index, Qualitative Risk Assessment, Quantitative Risk Assessment, Countermeasure Risk Assessments, Risk Results Report (highlighted), SDWA Section 1433 Certification, and Tutorials & Guides. The main content area is titled 'Risk And Resilience Summary Report' and includes two buttons: 'Download Report' and 'Email Report'. Below the title, it states 'Requires Adobe Acrobat Reader'. A PDF viewer is embedded, showing a document titled 'Risk Assessment Summary Report' with a page indicator '1 / 17' and a zoom level of '100%'. The PDF content visible includes the title 'Risk Assessment Summary Report for Spring View Water District'.





# Creating or Revising an RRA using EPA's Small System Checklist

Charlene Kormondy

# EPA's RRA Tools

## Small System RRA Checklist



- **Qualitative** risk assessment – **identifies** threats, vulnerabilities, and consequences but does not estimate risk value
- **Countermeasures** may be **identified**, and the benefits described but not estimated
- **“Paper” analysis** that requires minimal resources to complete
- Recommended for **smaller** water systems (serving under 50,000 people)

## Vulnerability Self Assessment Tool (VSAT)



- **Quantitative** risk assessment – **estimates** threats, vulnerabilities, consequences and monetized risk
- **Countermeasures** may be **quantified** for cost, risk reduction, and cost-benefit analysis
- **E-tool analysis** can require significant time and information resources to complete
- Recommended for **larger** water systems (serving over 50,000 people)

# Small Systems RRA Checklist

- Qualitative risk assessment
- PDF and Microsoft Word versions available
- [Download English Version Here](#)
- [Download Spanish Version Here](#)

Enter CWS Name  
Risk and Resilience Assessment

**Community Water System  
Risk and Resilience Assessment Checklist**

Enter CWS Name  
Risk and Resilience Assessment

**Please fill in the information below.**

Facility Name (if applicable): Enter text here.

PWSID: Enter text here.

Description of System: Enter text here.

Analyst Name(s): Enter text here.

Date of Analysis: Date

Analysis Notes: Enter text here.

This document and associated electronic files may contain sensitive or confidential information. Please maintain the document/electronic files in a manner that will help safeguard the information.

# Small System RRA Checklist July 2024 Updates

- Combined cyberattacks on business enterprise systems and process control systems into a single category of cyberattack.
- Eliminated accidental contamination of source and finished water as malevolent act threat categories.
- Updated the definition of “Electronic, Computer, or Other Automated Systems” to align with terminology commonly used in the cybersecurity field.
- Added *Table 11: Checklist of Priority Cybersecurity Practices for Water Systems* to provide a further method to evaluate cybersecurity at a CWS.

# Identifying Critical Assets within the SDWA 1433 Categories

CWSs serving over 3,300 people must assess the risks to and resilience of specified assets to malevolent acts and natural hazards:

Example: Pick your utility's physical barrier critical assets, e.g., fencing, walls, gates and facility entrances, intrusion detection alarms.

1. physical barriers;
2. source water;
3. pipes and constructed conveyances, water collection and intake;
4. pretreatment and treatment;
5. storage and distribution facilities;
6. electronic, computer, or other automated systems (including the security of such systems);
7. monitoring practices;
8. financial infrastructure;
9. the use, storage, or handling of chemicals;
10. operation and maintenance of the system.

*\*May include an evaluation of capital and operational needs for risk and resilience management.*

# Cover Page

## Community Water System Risk and Resilience Assessment Checklist

Enter CWS Name Below:

Spring View Water District

### Risk and Resilience Assessment

Please fill in the information below.

Facility Name (if applicable): Spring View Water District

PWSID: TX1234567

Description of System: Community Drinking Water System

Analyst Name(s): Piper Leak, Phil Terr

Date of Analysis: 2/6/2025

Analysis Notes:

# Example of a Malevolent Acts Table (Tables 1a-10a)

**Table 1a: Physical Barriers (Malevolent Acts)<sup>6</sup>**

Asset Category: <i>Physical Barriers</i>	
Examples of Assets in this Category: Encompasses physical security in place at the CWS. Possible examples include fencing, bollards, and perimeter walls; gates and facility entrances; intrusion detection sensors and alarms; access control systems (e.g., locks, card reader systems); and hardened doors, security grilles, and equipment cages.	
Malevolent Acts <sup>7</sup>	Brief Description of Impacts
<p>Select the malevolent acts in this column that pose a <u>significant risk</u> to this asset category at the CWS.</p> <p><input type="checkbox"/> Cyberattack<sup>8</sup></p>	<p>If you select a malevolent act in the left column as a significant risk to the <i>Physical Barriers</i> asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.</p>
<input type="checkbox"/> Assault on Utility – Physical	
<input type="checkbox"/> Theft or Diversion – Physical	
<input type="checkbox"/> Sabotage – Physical	
<input type="checkbox"/> Other(s), enter below:	

# Example of a Natural Hazards Table (Tables 1b-10b)

**Table 1b: Physical Barriers (Natural Hazards)<sup>9</sup>**

Asset Category: <i>Physical Barriers</i>	
Examples of Assets in this Category: Encompasses physical security in place at the CWS. Possible examples include fencing, bollards, and perimeter walls; gates and facility entrances; intrusion detection sensors and alarms; access control systems (e.g., locks, card reader systems); and hardened doors, security grilles, and equipment cages.	
Natural Hazards <sup>10</sup>	Brief Description of Impacts
<input type="checkbox"/> Hurricane Select the natural hazards in this column that pose a <u>significant risk</u> to this asset category at the CWS.	If you select a natural hazard in the left column as a significant risk to the <i>Physical Barriers</i> asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
<input type="checkbox"/> Hurricane	
<input type="checkbox"/> Flood	
<input type="checkbox"/> Earthquake	
<input type="checkbox"/> Tornado	
<input type="checkbox"/> Ice storm	
<input type="checkbox"/> Fire	
<input type="checkbox"/> Other(s), enter below:	



# Example Scenario

- Utility Name: Spring View Water District
- Size: Small utility that serves 35,000 people
- Critical assets:
  - 8 pumping stations
  - Supervisory control and data acquisition (SCADA) system
  - Water treatment plant
  - IT business and financial systems
- Example threats:
  - Flooding
  - Cyberattack
  - Viral Pandemic

# Hypothetical Threat: Cell Tower Cyberattack



**Table 5a: Storage and Distribution Facilities (Malevolent Acts)**

**Asset Category:** *Storage and Distribution Facilities*  
**Examples of Assets in this Category:** Encompasses all infrastructure used to store water after treatment, maintain water quality, and distribute water to customers. Possible examples include residual disinfection, pumps, tanks, reservoirs, valves, pipes, and meters.

<b>Malevolent Acts<sup>19</sup></b> Select the malevolent acts in this column that pose a <u>significant risk</u> to this asset category at the CWS.	<b>Brief Description of Impacts</b> If you select a malevolent act in the left column as a significant risk to the <i>Storage and Distribution Facilities</i> asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
<input checked="" type="checkbox"/> Cyberattack <sup>20</sup>	Spring View Water District relies on a cellular provider to remotely operate its pumping stations. A cell tower attack by a malicious actor could prevent remote (cellular) operation of a critical pumping station.

<input checked="" type="checkbox"/> Cyberattack <sup>20</sup>	Spring View Water District relies on a cellular provider to remotely operate its pumping stations. A cell tower attack by a malicious actor could prevent remote (cellular) operation of a critical pumping station.
---	--

<input type="checkbox"/> Sabotage – Physical	
<input type="checkbox"/> Intentional Contamination of Finished Water	
<input type="checkbox"/> Intentional Contamination of Source Water	
<input type="checkbox"/> Other(s), enter below: <div style="background-color: #e0e0e0; height: 20px; width: 100%;"></div>	

# Hypothetical Threat: Ransomware Cyberattack



**Table 6a: Electronic, Computer, or Other Automated Systems (including the security of such systems) (Malevolent Acts)**

**Asset Category:** *Electronic, Computer, or Other Automated Systems (including the security of such systems)*  
**Examples of Assets in this Category:** Encompasses all treatment and distribution operational technology (OT) or process control systems, business enterprise information technology (IT) and communications systems (other than financial), and the processes used to secure such systems. Possible examples include the controls, monitors and other interfaces, plus related IT hardware and software and communications, used to control water collection, treatment, and distribution. Also includes IT hardware, software, and communications used in business enterprise operations. The assessment must account for the security of these systems (e.g., cybersecurity, information security).

**Note:** This table focuses on how specific malevolent acts may impact the cybersecurity and information security of electronic, computer, or other automated systems. In addition, CWSs should complete Table 11, the "Checklist of Priority Cybersecurity Practices," to identify gaps in essential cybersecurity best practices.

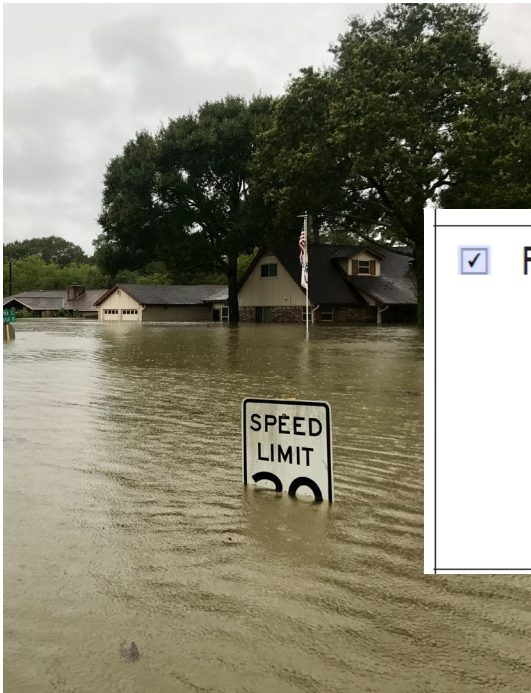
Malevolent Acts <sup>22</sup>	Brief Description of Impacts
Select the malevolent acts in this column that pose a <u>significant risk</u> to this asset category at the CWS.	If you select a malevolent act in the left column as a significant risk to the <i>Electronic, Computer, or Other Automated Systems (including the security of such systems)</i> asset category, briefly describe in the right column how the malevolent act could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.

Cyberattack<sup>23</sup>

Spring View Water District is concerned about a ransomware attack propagating through the entire local area network. The ransomware attack could prevent the District's communications with customers and access to financial systems. Utility systems connected to the network could also be impacted (e.g., laboratory equipment, work order systems).

<input type="checkbox"/> Theft or Diversion – Physical	
<input type="checkbox"/> Sabotage – Physical	
<input type="checkbox"/> Other(s), enter below:	

# Hypothetical Threat: Flooding



Flood

Spring View Water District is located near the Winding River and draws its source water from the river. The utility is concerned that a 100-year flooding event could occur. Electrical components of the utility's online water quality monitoring equipment (not elevated) could be damaged. This could disable continuous monitoring of the finished water leaving the treatment plant.

Table 7b: Monitoring Practices (Natural Hazards)<sup>28</sup>

**Asset Category:** *Monitoring Practices*  
**Examples of Assets in this Category:** Encompasses the processes and practices used to monitor source water and finished water quality, along with any monitoring systems not captured in other asset categories. Possible examples include sensors, laboratory resources, sampling capabilities, and data management equipment and systems that are implemented as part of a contamination warning system for a source water or distribution system.

Natural Hazards <sup>29</sup>	Brief Description of Impacts
Select the natural hazards in this column that pose a <u>significant risk</u> to this asset category at the CWS.	If you select a natural hazard in the left column as a significant risk to the <i>Monitoring Practices</i> asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.

<input type="checkbox"/> Hurricane	
------------------------------------	--

<input checked="" type="checkbox"/> Flood	Spring View Water District is located near the Winding River and draws its source
---	---

<input type="checkbox"/> Tornado	
----------------------------------	--

<input type="checkbox"/> Ice storm	
------------------------------------	--

# Hypothetical Threat: Viral Pandemic

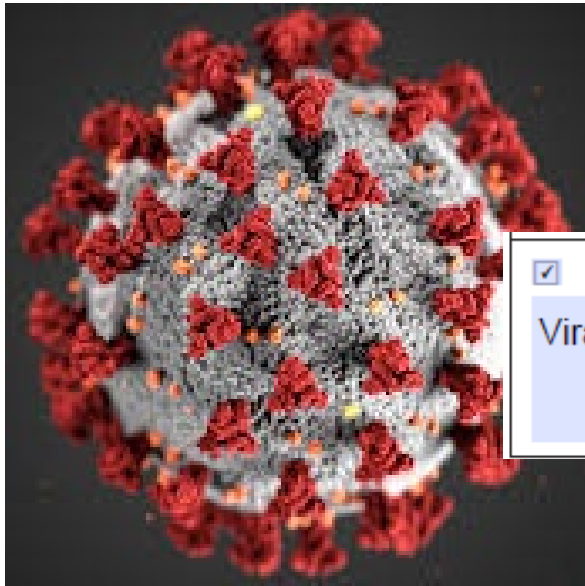


Table 10b: The Operation and Maintenance of the System (Natural Hazards)

<b>Asset Category:</b> <i>The Operation and Maintenance of the System</i> <b>Examples of Assets in this Category:</b> Encompasses critical processes required for operation and maintenance of the CWS that are not captured under other asset categories. Possible examples include equipment, supplies, and key personnel. Assessments may focus on the risk to operations associated with dependency threats like loss of utilities (e.g., power outages), loss of suppliers (e.g., interruption in chemical deliveries), and loss of key employees (e.g., disease outbreak or employee displacement).	
Natural Hazards <sup>38</sup>	Brief Description of Impacts
Select the natural hazards in this column that pose a <u>significant risk</u> to this asset category at the CWS.	If you select a natural hazard in the left column as a significant risk to the <i>Operation and Maintenance of the System</i> asset category, briefly describe in the right column how the natural hazard could impact this asset category at the CWS, especially as the impact relates to existing vulnerabilities at the CWS. Include effects on major assets, water service, and public health as applicable.
<input type="checkbox"/> Hurricane	
<input type="checkbox"/> Flood	
<input checked="" type="checkbox"/> Other(s), enter below: Viral pandemic	The District stores a three week supply of chlorine on-site. Disruptions to the supply chain during a viral pandemic could cause difficulties obtaining chlorine from suppliers. The District has 11 employees. Absenteeism during a viral pandemic could create issues with staffing and loss of key personnel.
<input type="checkbox"/> Ice storm	
<input type="checkbox"/> Fire	
<input checked="" type="checkbox"/> Other(s), enter below: Viral pandemic	The District stores a three week supply of chlorine on-site. Disruptions to the supply chain during a viral pandemic could cause difficulties obtaining chlorine from suppliers. The District has 11 employees. Absenteeism during a viral pandemic could create issues with staffing and loss of key personnel.

<sup>38</sup> Examples of natural hazards are provided, as well as the field "Other(s), enter below:" for you to write in any additional natural hazards of concern.

# NEW Cybersecurity Checklist (Table 11 in latest version)

- Includes 15 cybersecurity controls and their recommendations
- The questions are derived from the [Top 8 Cyber Actions for Securing Water Systems](#) + 7 Priority Controls from EPA’s [Cybersecurity Risk Assessment Guidance](#) (full list of 33 questions available here in the [WCAT Tool](#))

Table 11: Checklist of Priority Cybersecurity Practices for Water Systems

	Question Does the CWS...	Answer Mark the appropriate check box ("Yes", "No", "In progress", "Not applicable") to answer each cybersecurity assessment question.
<b>Reduce Exposure to Public-Facing Internet</b>		
1.	Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between OT assets and the Internet?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Eliminate unnecessary exposed ports and services on public-facing assets with regular review and eliminate OT asset connections to the public Internet unless explicitly required for operations.</i>
<b>Conduct Regular Cybersecurity Assessments</b>		
2.	Conduct regular cybersecurity assessments?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: 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.</i>
3.	Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the CWS?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Identify one role/position/title responsible for cybersecurity within the CWS. Whoever fills this role/position/title is then in charge of all CWS cybersecurity activities.</i>
<b>Change Default Passwords Immediately</b>		
4.	Change default passwords and require a minimum length for passwords?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Change all default manufacturer or vendor passwords before equipment or software is put into service and implement a minimum length requirement for passwords through a policy and/or administrative controls set in the system.</i>

# OPTIONAL Countermeasures Table (Table 12 in latest version)

**Table 12: Countermeasures (Optional)<sup>39</sup>**

Countermeasures (optional) List countermeasures in the left column the CWS could potentially implement to reduce risk from the malevolent acts and natural hazards that were selected.	Brief Description of Risk Reduction or Increased Resilience For each countermeasure, in the right column, describe how the countermeasure could reduce risk or increase resilience for CWS assets from malevolent acts or natural hazards that were selected in the analysis. A countermeasure may reduce risk across multiple malevolent acts, natural hazards, and asset categories.
1. Cyber consultant	A cyber consultant may help to identify weaknesses and vulnerabilities in Spring View Water District's software, computer systems, and networks. This may reduce risk from cyberattacks and ransomware. Update: In January 2025, the District participated in EPA's Water Sector Cybersecurity Evaluation Program and developed a plan to reduce cyber vulnerabilities with the help of a cybersecurity professional.
2. Cybersecurity awareness training	Cybersecurity awareness training may reduce risks from cyberattacks and ransomware to process control systems; storage and distribution facilities; electronic or other automatic systems; and financial infrastructure. Cybersecurity training may help employees identify attacks before they are fully enacted.
3. Elevated OWQM sensors and waterproof boxes for OWQM equipment	Elevated online water quality monitoring (OWQM) sensors and waterproof boxes for OWQM equipment may help to protect the CWS's monitoring practices during a flood. Update: in June 2023, the District implemented this countermeasure, improving resilience to future floods.
4. Water/Wastewater Agency Response Network (WARN)	WARN could provide Spring View Water District with the means to quickly obtain help in the form of personnel, equipment, materials, and associated services from other utilities to restore critical operations impacted during any type of emergency.
5. Update standard operating procedures (SOPs)	Updating SOPs for checking the system after a connective disruption and for plant operations and other essential functions will help to reduce consequences and improve response time during cyberattacks and natural hazards.



# BREAK





# ***EPA's Checklist of Priority Cybersecurity Practices for Water Systems***

Cameron Burden, EPA Water Infrastructure and Cyber Resilience Division

# NEW Cybersecurity Checklist

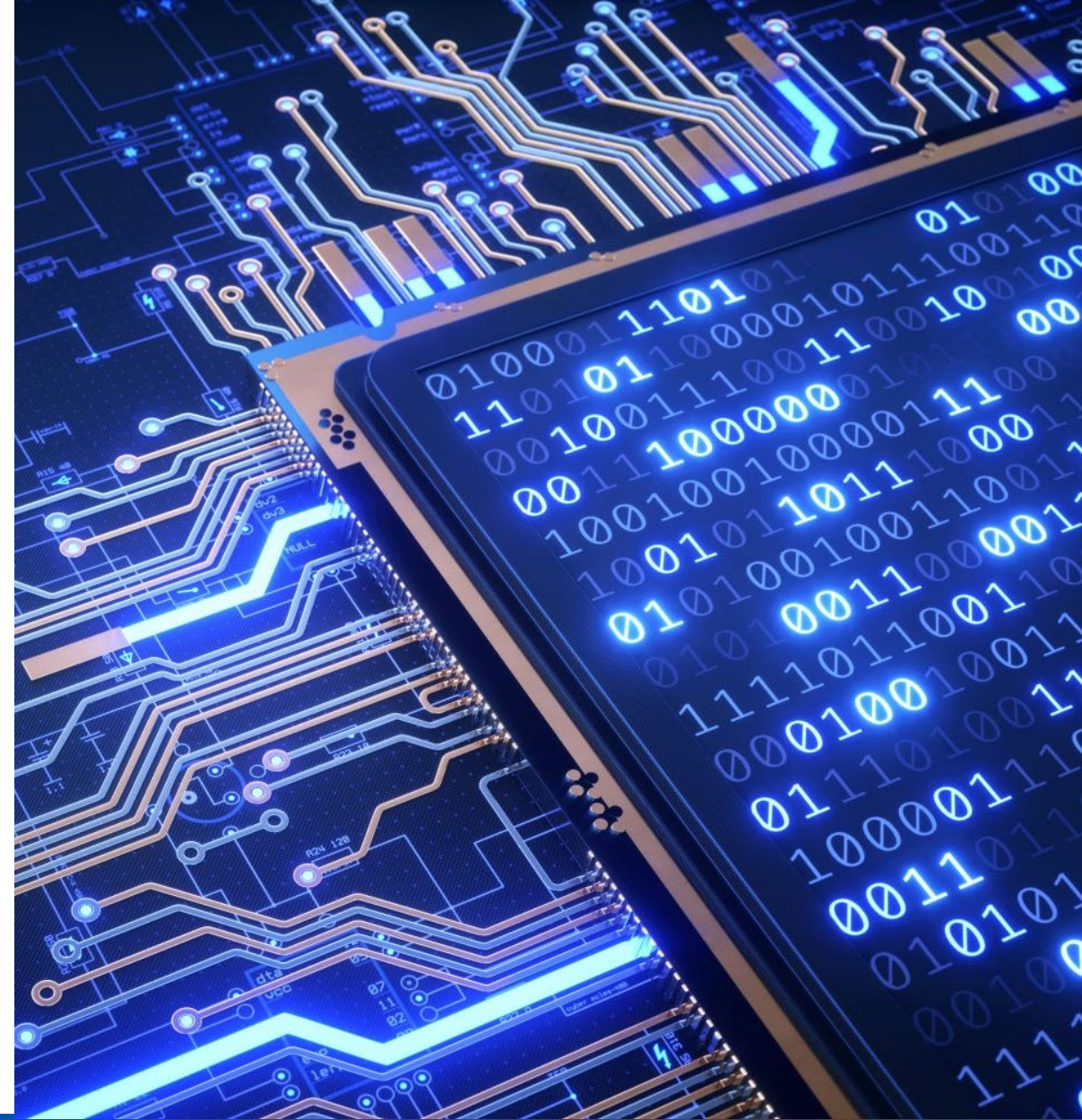
- Includes 15 cybersecurity controls and their recommendations
- The questions are derived from the [Top 8 Cyber Actions for Securing Water Systems](#) + 7 Priority Controls from EPA's [Cybersecurity Risk Assessment Guidance](#) (full list of 33 questions [available here in the WCAT Tool](#))
- Includes cybersecurity resources to assist utilities in implementing each cybersecurity control

Table 11: Checklist of Priority Cybersecurity Practices for Water Systems

	Question Does the CWS...	Answer Mark the appropriate check box ("Yes", "No", "In progress", "Not applicable") to answer each cybersecurity assessment question.
<b>Reduce Exposure to Public-Facing Internet</b>		
1.	Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between OT assets and the Internet?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Eliminate unnecessary exposed ports and services on public-facing assets with regular review and eliminate OT asset connections to the public Internet unless explicitly required for operations.</i>
<b>Conduct Regular Cybersecurity Assessments</b>		
2.	Conduct regular cybersecurity assessments?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: 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.</i>
3.	Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the CWS?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Identify one role/position/title responsible for cybersecurity within the CWS. Whoever fills this role/position/title is then in charge of all CWS cybersecurity activities.</i>
<b>Change Default Passwords Immediately</b>		
4.	Change default passwords and require a minimum length for passwords?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Change all default manufacturer or vendor passwords before equipment or software is put into service and implement a minimum length requirement for passwords through a policy and/or administrative controls set in the system.</i>

# Key Points to Remember

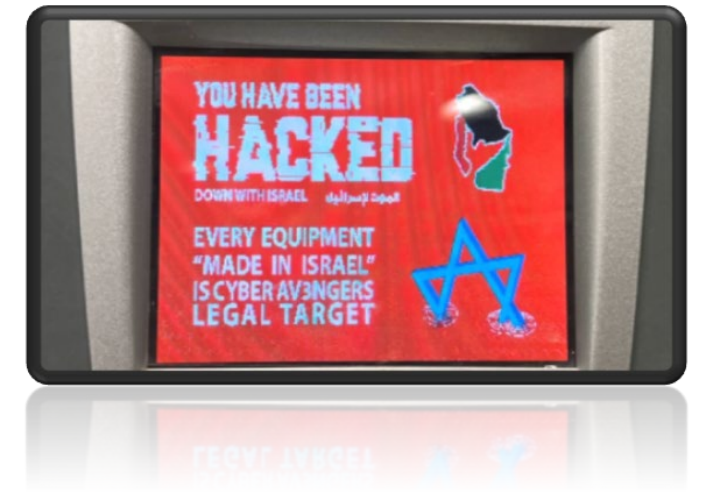
1. We understand you are not cybersecurity experts.
2. There is no “one size fits all” approach to cybersecurity.
3. Implementation of the 15 cybersecurity controls may vary between utilities.
4. Some cybersecurity controls may be overseen and implemented by third-parties.
5. If in doubt, submit cybersecurity-related questions to [EPA’s Cybersecurity Technical Assistance Program for the Water Sector.](#)



# ***1. Ensure that assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminate connections between OT assets and the Internet?***

Why is this control important?

- Ports are how computers communicate and provide services with other computers.
- Attackers can use these ports as “entrances” to a utility’s network if they are left unsecured.
- Internet-facing devices can be easily found by cyber criminals and exploited.



## *2. Conduct regular cybersecurity assessments? \*\**

Why is this important?

- Cybersecurity assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.
- Utilities should conduct an assessment on a regular basis to understand existing and new vulnerabilities within OT and IT systems.

### ***3. Have a named role/position/title that is responsible and accountable for planning, resourcing, and execution of cybersecurity activities within the utility?***

Why is this control important?

- A top-down strategy is essential for a utility's cybersecurity program.
- The cybersecurity lead can plan awareness training and exercises, request budget resources, meet with potential service providers, etc.
- This individual does not need to be a cybersecurity expert.

## 4. Change default passwords and require a minimum length for passwords?

Why is this control important?

- Factory default settings often include simple passwords that appear in the product's user manual.
- Weak and simple passwords can be cracked almost instantly.
- It is estimated to take 898,000 years to crack a 15-character password that uses upper and lowercase letters.



## ***5. Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access the OT network?***

Why is this control important?

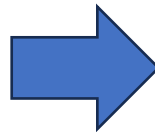
- Provides additional layer of security for accounts. Without MFA, attackers only need to obtain the password to access an account.
- Example: Something you know + something you have.
- The FBI Cyber Division has reported that 99.9% of hacked accounts don't use MFA.



## 6. Maintain an updated inventory of all OT and IT network assets?

Why is this control important?

- “You can’t protect what you don’t know you have.”
- Cybersecurity improvements can’t begin without a plan.
- An accurate inventory will assist in identifying and mitigating vulnerabilities.



### WATER SECTOR CYBERSECURITY PROGRAM CASE STUDY: *Small Wastewater System* *Asset Inventory: A Good First Step to Balancing Risks*

#### LESSONS LEARNED

- Take advantage of free cybersecurity assessments. The utility took advantage of the U.S. Environmental Protection Agency’s free cybersecurity vulnerability assessment which laid the groundwork for their cybersecurity improvements.
- Take action on all of the no-cost implementation measures. The cybersecurity measures implemented by the utility were essentially free, other than requiring some technical input from existing vendors and the operator’s time (e.g., drafting the policy document, overseeing implementation of the identified actions) over an eight-month period.
- Maintain a cybersecurity asset inventory. In retrospect, one item the utility realized as fundamental to their success was the cyber asset inventory. This inventory served as the springboard for all other cyber improvements, as it gave them a clear snapshot of what they owned and how it was connected. In the operator’s words, “It’s really hard to know how to protect what you don’t know you have.” The inventory has also assisted in ongoing maintenance for cyber assets, as it listed all the assets in one place and contained information such as model and serial number, age, how the asset is used within the network, and vendor contact information for the asset.

## *7. Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?*

Why is this control important?

- Attackers often exploit vulnerabilities that only exist in certain versions or settings.
- “You can’t protect what you don’t know you have.”
- Allows a utility to stay-up-to date on latest threats.

## ***8. Have a written cybersecurity Incident Response (IR) Plan for critical threat scenarios which is regularly practiced and updated?***

Why is this control important?

- Describes the strategies, resources, and procedures to prepare for, respond to, and recover from a cyber incident.
- The IR plan is essential in helping a utility recover quickly from cybersecurity incidents.
- Being prepared is half the battle.

# 9. Have a written procedure for reporting cybersecurity incidents, including how and to whom?

Why is this control important?

- Supports incident response procedures and allows a utility to receive support if they are experiencing a cyberattack.
- Reported information may also help stop cybercrime from occurring at other utilities.



**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](http://www.ic3.gov) or contact your local field office at [www.fbi.gov/contact-us/field](mailto: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](http://www.us-cert.cisa.gov/forms/report). CISA can be contacted by phone at 888-282-0870 and by email at [Central@cisa.gov](mailto: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](mailto: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

## ***10. Backup systems necessary for operations on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?***

Why is this control important?

- Backups are a critical element of a utility's restoration and recovery activities.
- Backups are important for cyber incidents, hardware malfunctions, or physical destruction of equipment.
- First line of defense for ransomware and similar attacks.

# ***11. Patch or otherwise mitigate known vulnerabilities within the recommended timeframe?***

Why is this control important?

- Vulnerabilities are weaknesses in software or hardware.
- Cyber criminals will actively research vulnerabilities to exploit.
- The 2023 attacks on Unitronics PLCs is an example of a known vulnerability being exploited.

## ***12. Require unique and separate credentials for users to access OT and IT networks and separate user and privileged (e.g., System Administrator) accounts?***

Why is this control important?

- Attackers use compromised credentials to access other accounts and it may not raise alarms
- This can lead to a utility not recognizing it as a security incident
- Administrator accounts have full control over a system
- Improper handling of administrator accounts makes an attacker's job easier

## ***13. Prohibit the connection of unauthorized hardware (e.g., USB drives) to OT and IT assets?***

Why is this control important?

- Inserting unauthorized hardware can lead to system breaches, disruptions, or damage.
- Cyber criminals can “drop” malicious USBs in or around buildings.
- Employees can unknowingly cause system breaches by connecting unauthorized hardware.



# 14. Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?

Why is this control important?

- Inactive accounts may appear harmless.
- Attackers can use these accounts and go undetected.
- This control protects against insider threats.



## ***15. Provide at least annual training for all utility personnel that covers basic cybersecurity concepts?***

Why is this control important?

- Regular cybersecurity training builds a culture of cybersecurity awareness.
- Utilities staff that receive regular training are more likely to identify cyber-attacks.
- Regular training is critical as cybersecurity threats evolve.

# Additional Cybersecurity Assessment Resources

- **Self-Assessment:** 33 Question Checklist and Water Cybersecurity Assessment Tool ([WCAT](#)) available at [epa.gov/waterresilience/cybersecurity-assessments](https://epa.gov/waterresilience/cybersecurity-assessments)
- **Third-Party Assessment:** Water Sector Cybersecurity Evaluation Program available at [epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program](https://epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program)





# Creating or Revising an Emergency Response Plan (ERP) using EPA's ERP Template

Parker Allen, EPA Water Infrastructure and Cyber Resilience Division

# Emergency Response Plan Guidance and Template

- [Download English Template Here](#)
- [Download Spanish Template Here](#)

## TABLE OF CONTENTS

<b>UTILITY INFORMATION</b> .....	<b>1</b>
i Utility Overview .....	1
ii Personnel Information .....	2
iii Primary Utility Components .....	3
iv Industry Chemical Handling and Storage Facilities .....	4
v Safety .....	5
vi Response Resources .....	6
vii Key Local Services .....	6
<b>1 RESILIENCE STRATEGIES</b> .....	<b>7</b>
1.1 Emergency Response Roles and Responsibilities .....	7
1.2 Incident Command System (ICS) Roles .....	8
1.3 Communication Contact Lists .....	9
1.4 Media Outreach Contact List .....	12
1.5 Public Notification Templates .....	12
<b>2 EMERGENCY PLANS AND PROCEDURES</b> .....	<b>13</b>
2.1 Core Response Procedures .....	13
2.2 Incident-Specific Response Procedures .....	16
<b>3 MITIGATION ACTIONS</b> .....	<b>17</b>
3.1 Alternative Source Water Options and Interconnected Utilities .....	17
3.2 Cybersecurity Mitigation Actions .....	17
3.3 Other Mitigation Actions .....	21
<b>4 DETECTION STRATEGIES</b> .....	<b>22</b>

# ERP Template September 2024 Updates

- Added additional cybersecurity materials and corresponding practical mitigation options for utilities
- Updated ERP Template to be easier to use and more customizable

Question		Answer
Does the CWS...		Mark the appropriate check box ("Yes", "No", "In progress", "Not applicable") to answer each cybersecurity assessment question.
<b>Reduce Exposure to Public-Facing Internet</b>		
1.	Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between OT assets and the Internet?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Eliminate unnecessary exposed ports and services on public-facing assets with regular review and eliminate OT asset connections to the public Internet unless explicitly required for operations.</i>
<b>Conduct Regular Cybersecurity Assessments</b>		
2.	Conduct regular cybersecurity assessments?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: 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.</i>
3.	Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the CWS?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Identify one role/position/title responsible for cybersecurity within the CWS. Whoever fills this role/position/title is then in charge of all CWS cybersecurity activities.</i>
<b>Change Default Passwords Immediately</b>		
4.	Change default passwords and require a minimum length for passwords?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> In progress <input type="checkbox"/> Not applicable  <i>If "No", EPA recommends that the CWS take the following action: Change all default manufacturer or vendor passwords before equipment or software is put into service and implement a minimum length requirement for passwords through a policy and/or administrative controls set in the system.</i>

# ERP Guidance – How to Access

Visit [www.epa.gov/waterresilience](https://www.epa.gov/waterresilience)  
OR search “EPA ERP” in a search engine of your choice

## ERP Template and Instructions for Drinking Water Utilities

This template and instructions will assist water utilities with developing an Emergency Response Plan (ERP) in accordance with America’s Water Infrastructure Act of 2018 (AWIA) section 2013(b), which amended Safe Drinking Water Act (SDWA) section 1433(b). SDWA 1433(b) requires community water systems serving populations greater than 3,300 to develop or update an ERP that incorporates findings of their risk assessment. **Please note that the instructions and template were updated in September 2024 to include new cybersecurity materials and corresponding practical mitigation options for utilities along with an easier to use customizable template.**

## SDWA Section 1433 Certification Requirements

Community water systems serving populations greater than 3,300 must certify to U.S. EPA that they have completed an ERP that incorporates findings of the risk and resilience assessment conducted under SDWA section 1433(a) and meets the criteria outlined under SDWA section 1433(b). U.S. EPA strongly recommends you electronically submit your community water system’s ERP certification statement by clicking the link below.

- [Submit Emergency Response Plan Certification Online](#)

Alternate certification statement submittal options are accessible by clicking the link below.

- [Email, Regular Mail or Alternate Submittal Options for Emergency Response Plan Certification](#)

AWIA requires you to submit only a certification of completion of a risk and resilience assessment and an ERP; therefore, do not submit the risk and resilience assessment and ERP documents to U.S. EPA.

**NOTE:** The PDF files use Javascript. In order to access the Word template that is imbedded within the PDF, please download the PDF file to your computer and open the PDF file with a PDF reader. If you are still having problems with accessing the Word template, email [dwresilience@epa.gov](mailto:dwresilience@epa.gov)

- [Drinking Water Utility ERP Template and Instructions \(pdf\)](#) (489.26 KB, September 2024, 816-B-24-001)

# ERP Guidance – Two Components

- A single PDF document provides guidance on what information should be provided in each section of the ERP template. Includes useful links for additional information and guidance
- A blank ERP template in Word format is embedded in the PDF document and can be easily accessed and modified to meet your own utility's needs.





# ERP Template Outline

## Sections

- Utility Information
- Resilience Strategies
- Emergency Plans and Procedures
- Mitigation Actions
- Detection Strategies

Modify the template to meet individual utility needs!

## TABLE OF CONTENTS

<b>UTILITY INFORMATION</b> .....	<b>1</b>
i Utility Overview .....	1
ii Personnel Information .....	2
iii Primary Utility Components .....	3
iv Industry Chemical Handling and Storage Facilities .....	4
v Safety .....	5
vi Response Resources .....	6
vii Key Local Services .....	6
<b>1 RESILIENCE STRATEGIES</b> .....	<b>7</b>
1.1 Emergency Response Roles and Responsibilities .....	7
1.2 Incident Command System (ICS) Roles .....	8
1.3 Communication Contact Lists .....	9
1.4 Media Outreach Contact List .....	12
1.5 Public Notification Templates .....	12
<b>2 EMERGENCY PLANS AND PROCEDURES</b> .....	<b>13</b>
2.1 Core Response Procedures .....	13
2.2 Incident-Specific Response Procedures .....	16
<b>3 MITIGATION ACTIONS</b> .....	<b>17</b>
3.1 Alternative Source Water Options and Interconnected Utilities .....	17
3.2 Cybersecurity Mitigation Actions .....	17
3.3 Other Mitigation Actions .....	21
<b>4 DETECTION STRATEGIES</b> .....	<b>22</b>

# Utility Information

During an incident, you should have information about your water utility readily available for your personnel and response partners.

- i. Utility Overview
- ii. Personnel Information
- iii. Primary Utility Components
- iv. Industry Chemical Handling & Storage Facilities
- v. Safety
- vi. Response Resources
- vii. Key Local Services



# 1.3 Primary Utility Components

List components necessary to maintain effective operation of your utility.

### Wells

Well Name	Depth/Location	Available Yield	Treatment Requirements/Associated Treatment Plant
#1	80 ft below ground surface/end of Water Rd	200 gpm	pH adjustment and chlorination/treated in well house.
Other			

### Intakes

Intake Name	Depth/Location	Capacity	Treatment Requirements/Associated Treatment Plant
Clear River	30 ft below surface/center of river at Larry's Landing	800 gpm	Coagulation, flocculation, sedimentation, filtration and disinfection/Anytown Water Treatment Plant.
Other			

### Treatment Plants

Treatment Plant Name	Location	Capacity	Treatment Train
Anytown Water Treatment Plant	1 Water Utility Drive	1.2 MGD	Pre-treatment, primary treatment, post-treatment
Other			

# Section 1: Resilience Strategies

This section of your ERP contains strategies and resources to improve the resilience of your system.

- 1.1 - Emergency Response Roles and Responsibilities
- 1.2 - Incident Command System (ICS) Roles
- 1.3 - Communication Contact List
- 1.4 - Media Outreach Contact List
- 1.5 - Public Notification Templates



# 1.1 Emergency Response Roles & Responsibilities

Describe the roles and responsibilities for key utility and external response partner personnel. You can add, edit, or delete rows as necessary.

## *Water Utility and Partner Roles*

<b>Name/Title</b>	<b>Emergency Response Role</b>	<b>Responsibilities</b>
<i>Wendy Smith/ Superintendent</i>	<i>Emergency Response Lead</i>	<i>Responsible for all incident response activities, including developing strategies and tactics and ordering and releasing resources.</i>
<i>John Doe/Operations Chief</i>	<i>Alternate Emergency Response Lead</i>	<i>Perform duties as assigned by ER Lead; assumes duties listed above when ER Lead is not available.</i>
<i>Jim Rogers/County Public Affairs Officer</i>	<i>Public Information</i>	<i>Responsible for leading the public information effort based on information supplied by either the ER or Alternate ER Lead.</i>
<i>Jane Kelly/Chief of Police</i>	<i>Security</i>	<i>Will provide incident security as needed once notified by ER Lead.</i>
Other		

# 1.3 Communication Contact Lists

List all utility emergency response team members, their response role, title and contact information.

List all external response partners, their response role or position as well as contact information.

## Internal Contact List

Name	Role/Title	Phone	Alternate Phone	Email
<i>Joe Jones, ERP Lead</i>	<i>Leads incident response and serves as Deputy Operator</i>	<i>555-555-5555</i>	<i>555-555-7777</i>	<i>jjones@anytownwater.org</i>
Other				

## External Response Partner Contact List

Organization or Department	Point Person Name or Position	Phone	Alternate Phone	Email or Website
Document last modified: 11/25/2024				
<i>County Emergency Management/EOC</i>	<i>Anita Johnson, EMD Director</i>	<i>555-555-9999</i>	<i>555-555-2222</i>	<i>ajohnson@county.org</i>
911				
Police				
Fire/HazMat				
LEPC				
Elected officials				
Wastewater utility				
Water utility				
Power utility				
Health department				
Contractor/vendor				
Industry rep.				
Mutual aid				
Other				

## Section 2: Emergency Plans & Procedures

This section of your ERP should contain plans, procedures, and equipment that can be used during an event that threatens your utility's ability to treat and distribute drinking water.

Two types of emergency response plans and procedures should be included as part of your ERP:

- 2.1 - Core Response Procedures
  - 2.2 - Incident-Specific Response Procedures (ISRPs)
- 

# Core Procedures

Core procedures are the “building blocks” for incident response, since they apply across a broad variety of incidents (e.g., hurricane, earthquake, flood).

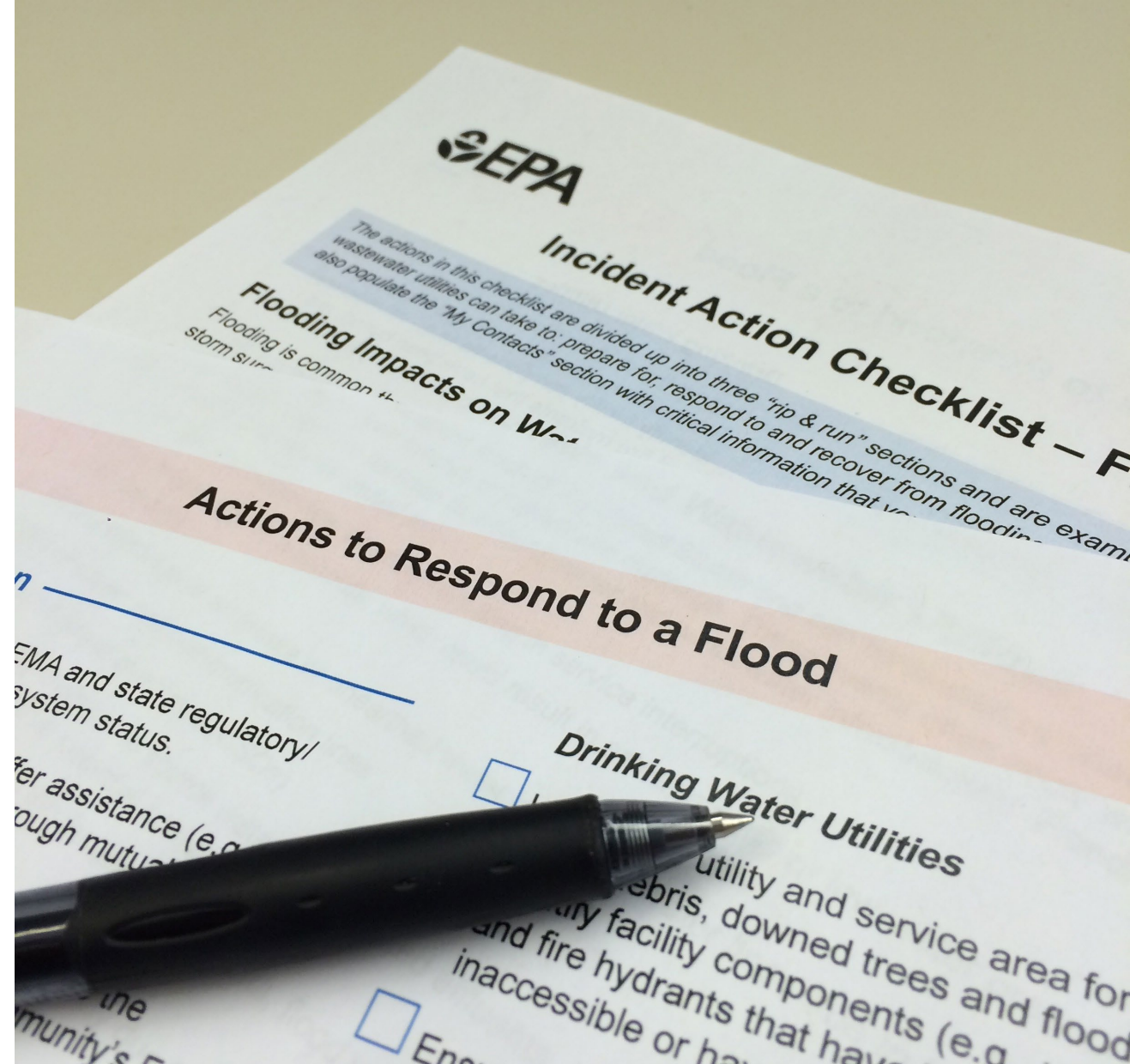
- Access
- Physical Security
- Cybersecurity
- Power Loss
- Emergency Alternate Drinking Water Supplies
- Sampling & Analysis
- Family and Utility Personnel Well Being





# Incident Specific Response Procedures (ISRPs)

- ISRPs are specialized procedures tailored to a particular type of incident.
- They provide a quick approach for responding to an incident and complement the actions already taken under your ERP.



# ISRP - Wildfire

## Actions to Prepare for a Wildfire

### Pre-Planning

- Identify critical infrastructure and develop contingency plans for loss of access and operations.
- Review and update your utility's emergency response plan (ERP) to include (but not limited to):
  - Updated emergency contacts.
  - Current GIS map(s) of all system components, facilities, and distribution lines, including coordinates for each facility.
  - Steps for shut down and start-up of system.
  - Steps for manual operation of all facilities.
  - Treatment adjustments to make based on raw water quality changes during and after fire, if necessary.
  - A fire-specific sampling plan that can be adjusted during the incident based on the location and extent of the fire relative to your system (includes groundwater wells as new MCL violations for nitrates and arsenic have been observed at groundwater systems following wildfires).
- Complete pre-disaster activities to help apply for disaster funding (e.g., contact state/ local officials with connections to funding, set up a system to document damage and costs, take photographs of the facility for comparison to post-damage photographs). Publicly-owned or private non-profit utilities may be eligible for federal reimbursement if a federal declaration is made.
  - Private for-profit utilities are not eligible for federal disaster funding and will need to rely on existing reserves, insurance, and loans.
- Ensure adequate personal protective equipment (PPE) is available for field employees.
- Conduct briefings, trainings and exercises to ensure utility staff is aware of all preparedness, response and recovery procedures.
- Develop emergency evacuation and shelter in place procedures as pertinent to wildfires.

### Coordination

- Coordinate with your local emergency responders and EMA to:

## Actions to Respond to a Wildfire

## Actions to Recover from a Wildfire

<https://www.epa.gov/waterutilityresponse/incident-action-checklists-water-utilities>

# Section 3: Mitigation Actions

This section of your ERP includes actions which can lessen the impact of a malevolent act or natural hazard on the public health and water services provided to your community.

- 3.1 –Alternate Source Water Options and Interconnected Utilities
- 3.2 – Cybersecurity Mitigation Actions
- 3.3 – Other Mitigation Actions



# 3.1 Alt. Source Water and Interconnected Utilities

List information on alternative source water options to mitigate impacts during incidents.

## Alternative Source Water Options

Type	Location	Comments
Well	Municipal golf course	This irrigation well can be used to supply water under emergency approval from state. Chlorination is needed and the well can produce up to 300 gpm.
Other		

List information on interconnected utilities to mitigate impacts during incidents.

## Interconnected Utilities

Utility Name	Location	Contact Information	Comments
ABC Water	Nearby Town	Jane Doe: 555-555-1234	Plans on file in engineering to construct emergency connection if needed.
Other			

# Section 4: Detection Strategies

This section of your ERP contains strategies that can aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of your utility, including;

- Unauthorized Entry into Utility Facilities
- Water Contamination
- Cyber Intrusion
- Hazardous Chemical Release
- Natural Disasters
- Power Outages

Effective response to an emergency requires timely detection, which allows your utility to implement its ERP as soon as possible.



# Contact Us

## Water Infrastructure and Cyber Resilience Division

- [WICRD-outreach@epa.gov](mailto:WICRD-outreach@epa.gov)
- [www.epa.gov/waterresilience](http://www.epa.gov/waterresilience)

## SDWA Section 1433/AWIA Section 2013

- [dwresilience@epa.gov](mailto:dwresilience@epa.gov)
- [www.epa.gov/waterresilience/awia-section-2013](http://www.epa.gov/waterresilience/awia-section-2013)

