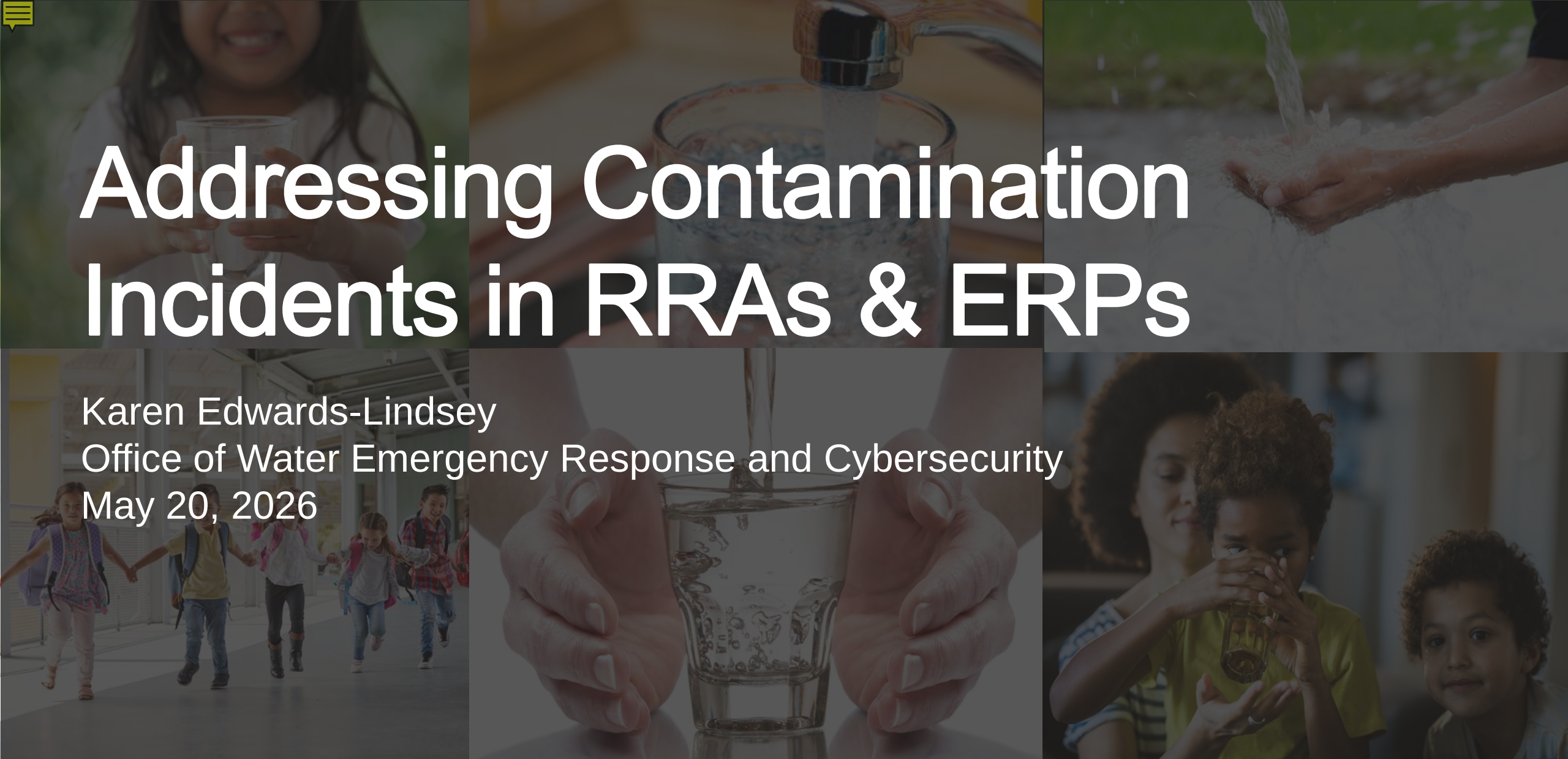




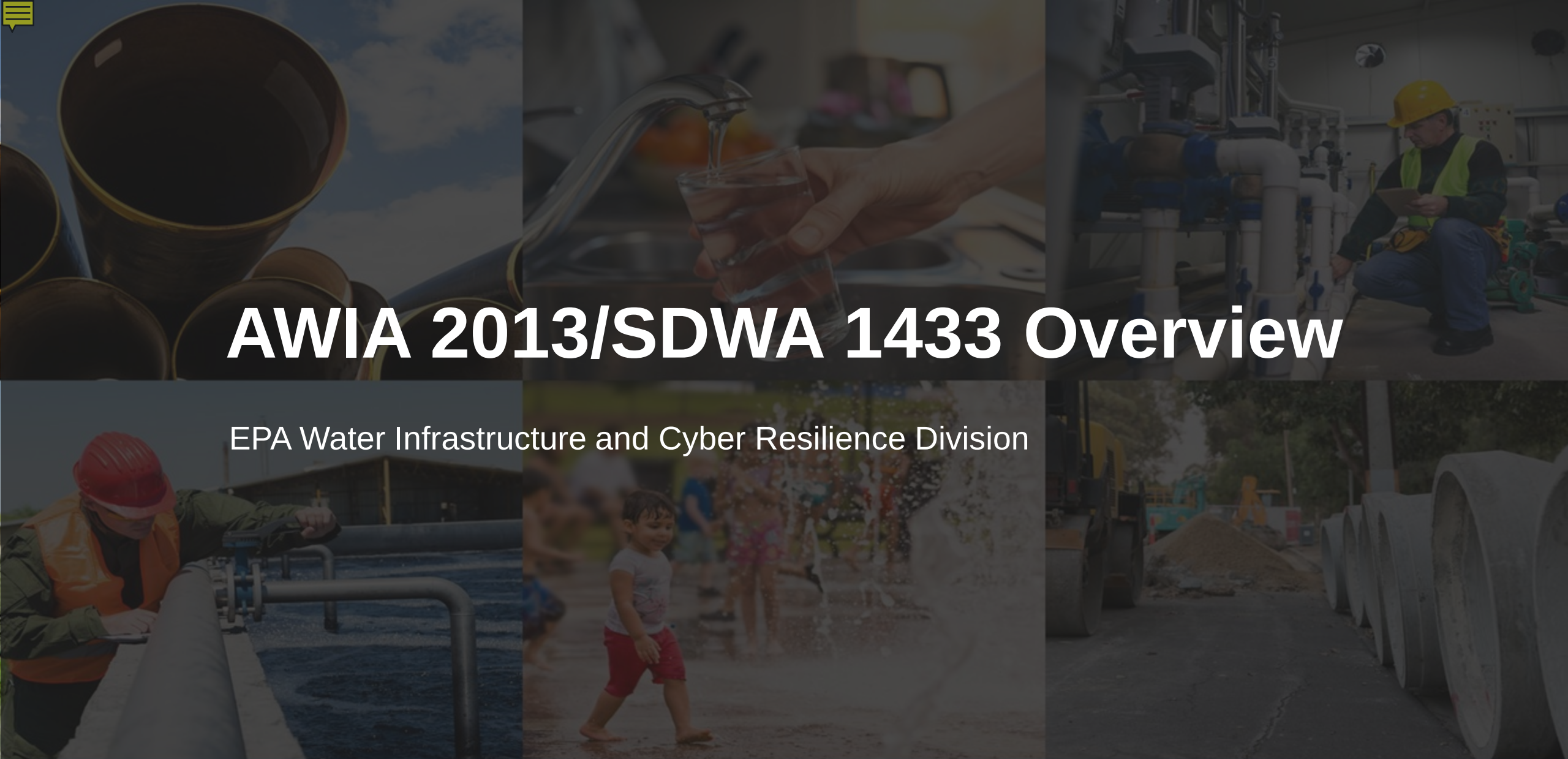
Addressing Contamination Incidents in RRA's & ERPs

Karen Edwards-Lindsey
Office of Water Emergency Response and Cybersecurity
May 20, 2026



Agenda

1. Overview of AWIA section 2013/SDWA section 1433
2. Reviewing and Revising Risk and Resilience Assessments (RRAs) and Emergency Response Plans (ERPs)
3. Contamination Incidents at Water Utilities
4. Incorporating Contamination Incidents in your RRA and ERP



AWIA 2013/SDWA 1433 Overview

EPA Water Infrastructure and Cyber Resilience Division



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. **See published here:**
<https://www.epa.gov/waterresilience/sdwa-section-1433-compliance-data>



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;

May 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

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





Reviewing and Revising your RRA and ERP





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, has resources on many threats of concern to water systems, including cyber threats, supply chain disruptions, and more





Lessons Learned

- Pass along RRA and ERP files to other utility staff if someone leaves the water system
- Check state vs. federal requirements for RRAs and/or ERPs
- Make sure all required elements of RRAs and ERPs are included
- Best practice: include malevolent acts or natural hazards that have happened at the CWS





Contamination Incidents at Water Utilities

Contamination Incidents

- Can occur from natural, accidental, and intentional causes
- Can result from other emergencies or specific contamination scenarios
- Begins with some type of indicator
 - Monitoring signal
 - Customer complaints
- Requires a measured, yet appropriate response



Responding to Contamination

Investigation

- Check other indicators
- Assess other data sources
- Site characterization and sampling
- Field and laboratory analysis



Operational Responses and Notifications

- Isolation
- Flushing / disinfection
- Risk communication
- Use restrictions



Remediation and Recovery

- System / contaminant characterization
- Remediation planning
- Decontamination
- Clearance



Benefits of Preparing for Contamination

- Understand capabilities and limitations
- Identify the correct personnel and response partners
- Establish processes and procedures
- Respond effectively with appropriate resources



Learn more: <https://www.epa.gov/waterresilience/contamination-preparedness-and-response>



Addressing Contamination in Your RRA and ERP



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** 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** systems (serving over 50,000 people)



RRA and Contamination

Malevolent Acts

Intentional acts carried out against the utility. Perpetrators may be an individual, group, or state, and attacks may be motivated by theft, terrorism, vandalism, or other objectives. A utility should consider potential impacts of the following types of malevolent acts on their critical operations in each asset category:

- Assault on Utility – Physical
- Intentional Contamination of Finished Water
- Intentional Contamination of Source Water
- Theft or Diversion – Physical
- Cyberattack
- Directed/Sabotage – Physical

Natural Hazards

Climatic, geologic, or other natural phenomena. E.g., earthquake, flood, hurricane, ice storm, tornado, wildfire

Other Hazards

VSAT and the Small System RRA Checklist allow users to input custom hazards of concern to their utility, beyond EPA's preset examples.

☐ Other(s), enter below:

Small System RRA Checklist: Contamination

Table 2a: Source Water (Malevolent Acts)
Table 3a: Pipes and Constructed Conveyances, Water Collection, and Intake (Malevolent Acts)
Table 4a: Pretreatment and Treatment (Malevolent Acts)
Table 5a: Storage and Distribution Facilities (Malevolent Acts)
Table 7a: Monitoring Practices (Malevolent Acts) ²⁵
Table 9a: The Use, Storage, or Handling of Chemicals (Malevolent Acts)
Table 10a: The Operation and Maintenance of the System (Malevolent Acts)

Asset Category: <i>The Operation and Maintenance of the System</i> Examples of Assets in this Category: 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).	
Malevolent Acts²⁵ Select the malevolent acts in this column that pose a <u>significant risk</u> to this asset category at the CWS.	Brief Description of Impacts If you select a malevolent act 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 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.

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

Asset Category: <i>Storage and Distribution Facilities</i> 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.	
Malevolent Acts¹⁹ Select the malevolent acts in this column that pose a <u>significant risk</u> to this asset category at the CWS.	Brief Description of Impacts 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.
☐ Intentional Contamination of Finished Water	potential exposure for customers, increased operational and sampling costs, regional economic consequences, loss of confidence
☐ Intentional Contamination of Source Water	

Access RRA Checklist here: www.epa.gov/waterresilience/small-system-risk-and-resilience-assessment-checklist



Small System RRA Checklist: Countermeasures

- Countermeasures: mitigation steps to reduce risk and increase resilience
- Examples:
 - Employee screening program
 - Backup power generation on-site
 - Guard(s)
 - Perimeter fencing
 - Hardened doors
 - Continuous process monitoring
 - Redundant water source(s)
 - Distribution of alternative drinking water
 - Site lighting
 - Emergency operating procedural plan
 - Intrusion sensors
 - Security cameras
 - Backflow prevention devices
 - Water/Wastewater Agency Response Network (WARN)
 - Hardened ladder access
 - Toxicity monitoring
 - Note: VSAT and the RRA Checklist allow custom countermeasures

Table 12: Countermeasures (Optional)³⁹

Countermeasures (optional)		Brief Description of Risk Reduction or Increased Resilience
List countermeasures in the left column the CWS could potentially implement to reduce risk from the malevolent acts and natural hazards that were selected.		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.	Contamination Response Procedure	Decrease the response time and improve decision-making for contamination incidents to return the system to normal operations faster.



VSAT and Contamination: Qualitative

Qualitative Risk Assessment

Compliance with SDWA Section 1433(a) Risk and Resilience Assessments

To use this qualitative risk assessment to comply with the requirements for Risk and Resilience Assessments in SDWA Section 1433(a), you must do the following:

- (1) For each asset category in the list below, determine whether the utility has one or more critical assets within the category that are necessary to achieve water quality, treatment, or distribution objectives.
- (2) Determine whether any critical asset in an asset category is at risk from a malevolent threat, natural hazard, or both. Move the slider buttons accordingly.
- (3) For critical assets that are at risk from a malevolent act or natural hazard, use the text box for the asset category to describe:
 - (a) the specific asset(s),
 - (b) the malevolent act(s) and/or natural hazard(s) that present a risk to the asset, and
 - (c) the potential consequences to the utility and the region served by the utility if the malevolent act(s) and/or natural hazard(s) impact(s) the asset.
- (4) For each asset category where neither malevolent act nor natural hazard are selected, describe why there are no critical assets in this category at risk.

For additional information about malevolent acts, see [Baseline Information on Malevolent Acts for Community Water Systems](#).



VSAT and Contamination: Asset Categories

Asset Category

Category Names	Malevolent Act? ?	Natural Hazards? ?	Describe Potential Impact, or Reason for No Selection ?
Physical Barriers i	☐	☐	This was not selected as a high risk asset because the utility recently underwent a thorough
Source Water i	☐	☐	Not a high risk asset - Utility will describe potential impacts including assets, threats, and
Pipes and Constructed Conveyances, Water Collection, and Intake i	☐	☐	Not a high risk asset - Utility will describe potential impacts including assets, threats, and
Pretreatment and Treatment i	☐	☐	Not a high risk asset - Utility will describe potential impacts including assets, threats, and
Storage and Distribution Facilities i	☒	☐	potential exposure for customers, increased operational and sampling





VSAT and Contamination: Quantitative

Quantitative Risk Assessment

The dashboard keeps track of the utility's baseline risk assessments, which are conducted for the high-risk asset categories selected in the Qualitative Risk Assessment. **EPA recommends that the quantitative risk assessment be limited to a small number of the assets and threats that present the highest risk.**

Baseline risk assessments can be completed in four steps:

1. For each asset category, define a utility asset that is at risk. This could be the asset category itself (e.g., physical barriers), a piece of equipment or a facility (e.g., a storage tank) or an entire system (e.g., a treatment train). You can also define multiple assets for each asset category.
2. Next, you should select at least one specific threat, which may be a malevolent act, natural hazard, or dependency/proximity threat, for each asset you define.
3. By assigning a specific threat to an asset, you create an asset/threat (A/T) pair. For each A/T pair, you can assess risk. VSAT provides information and tools to help you assess risk.
4. Once a baseline risk assessment for one A/T pair is complete, you may conduct baseline risk assessments for other A/T pairs. EPA recommends that you complete at least one baseline risk assessment for one A/T pair in each high-risk asset category.



VSAT and Contamination: Asset/Threat Pairs

Category Name

^

Storage and Distribution Facilities

+ Add Asset

^

✓

Storage Tank

+ Add Threat

✓

Intentional Contamination of Finished Water

Chemical dumped into storage tank



VSAT and WARN: Countermeasures

Assets

Asset Name

Storage Tank

Intentional Contamination of Finished Water

Chemical dumped into storage tank

 [Edit Countermeasures](#)

Select all potential countermeasures that apply

Countermeasure Names

☐	Employee screening program
☐	Backup power generation on-site
☐	Guard(s)
☐	Perimeter fencing
☐	Hardened doors
☐	Continuous process monitoring
☐	Redundant water source(s)
☐	Distribution of alternative drinking water
☐	Site lighting
☒	Emergency operating procedural plan



United States
Environmental Protection
Agency

Office of Water

Learn More about VSAT and other EPA RRA and ERP tools

Want to learn more about VSAT?

Visit www.epa.gov/waterresilience/awia-section-2013sdwa-section-1433-workshops for video recordings of past workshops on how to use all of EPA's SDWA 1433 RRA and ERP resources, including VSAT.



The video player thumbnail features the EPA logo in the top left corner. The title is "Creating or Revising an RRA Using EPA's VSAT" with a subtitle "Hypothetical Threat: Flooding". A "Copy link" button is in the top right. The main content area lists four bullet points: "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 water quality monitoring equipment (elevated) could be damaged", and "This could disable continuous monitoring of the finished water leaving the treatment plant". A red YouTube play button is centered over the text. On the right, a video frame shows a flooded street with a "SPEED LIMIT 20" sign partially submerged. The bottom of the player has a "Watch on YouTube" button and the "Office of Water" text on the right.

- 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 water quality monitoring equipment (elevated) could be damaged
- This could disable continuous monitoring of the finished water leaving the treatment plant

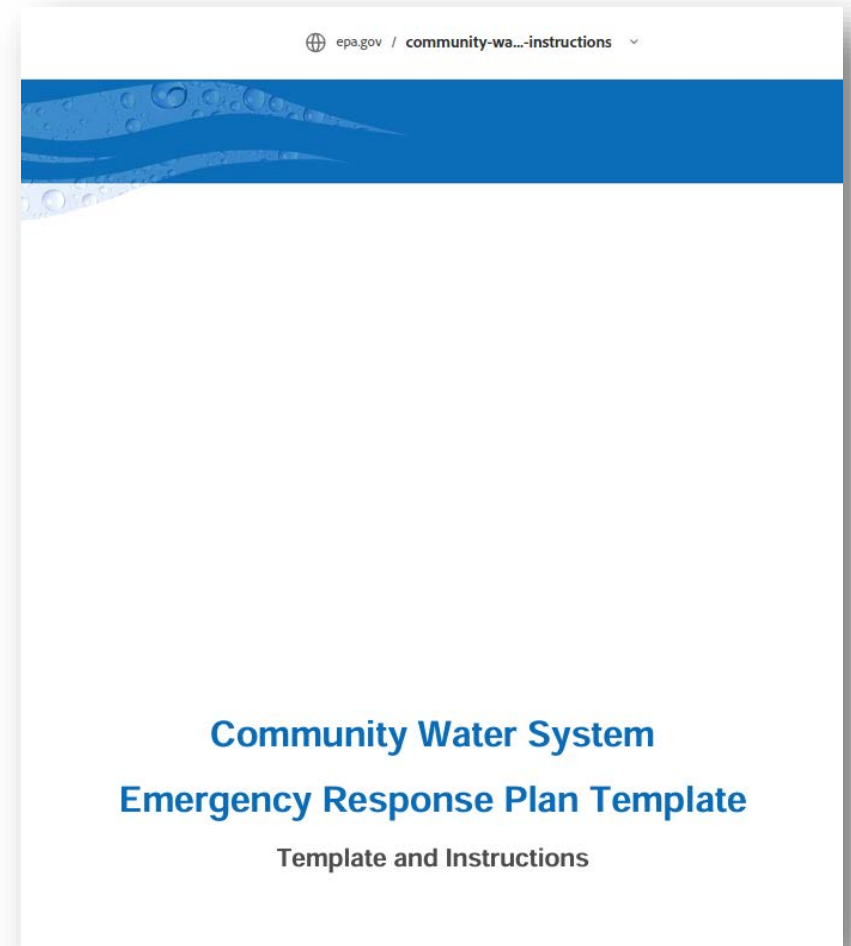
Watch on YouTube

Office of Water



Emergency Response Plan (ERP)

- Access ERP here:
www.epa.gov/waterutilityresponse/develop-or-update-emergency-response-plan
- The ERP Template and Instructions PDF document features an embedded blank ERP template in Word format that can be easily accessed and modified by utility personnel to meet their own water system needs
- The Word ERP template is also available to download directly for ease





ERP Template Table of Contents

TABLE OF CONTENTS

UTILITY INFORMATION

i

Utility Overview

1

ii

Personnel Information

1

iii

Primary Utility Components

1

iv

Industry Chemical Handling and Storage Facilities

1

v

Safety

1

vi

Response Resources

2

vii

Key Local Services

2

1

RESILIENCE STRATEGIES

2

1.1

Emergency Response Roles and Responsibilities

2

1.2

Incident Command System (ICS) Roles

3

1.3

Communication

3

1.4

Media Outreach and Risk Communication

4

1.5

Public Notification Templates

4

2

EMERGENCY PLANS AND PROCEDURES

5

2.1

Core Response Procedures

5

2.2

Incident-Specific Response Procedures

6

3

MITIGATION ACTIONS

7

3.1

Alternative Source Water Options and Interconnected Utilities

7

3.2

Cybersecurity Mitigation Actions

7

3.3

Other Mitigation Actions

8

4

DETECTION STRATEGIES

9

4.1

Unauthorized Entry into Utility Facilities

9

4.2

Water Contamination

9

4.3

Cyber Intrusion

9

4.5

Natural Hazards

9

4.6

Power Outages

10





2.1 Core Response Procedures

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

Sampling and Analysis: Water contamination emergencies could result in a surge of water sampling and analysis that can quickly overwhelm resources or require laboratory expertise unavailable to most utilities. To prepare internally for incidents, your utility can complete the tables in this section and include pre-identified sampling sites, procedures for sample collection of both known and unknown contaminants, chain of custody, sample preservation, sample transport, as well as a list and locations of contract analytical laboratories. Also consider consulting with your state drinking water regulatory agency on the issue of water sampling and analysis. You can learn more about resources to help develop sampling procedures and coordinate laboratory support, such as the Water Laboratory Alliance (WLA), by accessing EPA’s [Water Quality Surveillance and Response System](#) website. Joining your state WARN may also help with accessing laboratory resources.



2.2 Incident-Specific Response Procedures (ISRP)

- ISRPs are specialized procedures tailored to a particular type of incident.
- Incidents include but are not limited to the following:

- Drought
- Earthquake
- Extreme Cold and Winter Storms
- Extreme Heat
- Flooding
- Harmful Algal Bloom
- Hurricane



- Pandemic
- Tornado
- Tsunami
- Volcanic Activity
- Wildfire
- Source Water Contamination
- Distribution System Contamination





3 Mitigation Actions

This section of your ERP should include actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to your community and individuals, including cybersecurity measures, the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers.

3.3 Other Mitigation Actions

Mitigation actions should be based on the countermeasures identified from your utility's RRA and implemented before an incident occurs. For example, system facilities or controls can be raised, and berms constructed ahead of time to protect against flood damage. You can also refer to the appendix for more mitigation options. List your utility's other mitigation actions in the table provided.



3.3 Other Mitigation Actions: Examples

Contamination

- Train operators and maintenance/repair staff to prevent contamination
- Install backflow prevention and on-line water quality monitoring devices
- Develop a source water monitoring program
- For more mitigation options, see EPA's Malevolent Acts for Community Water Systems

Wildfire

- Remove debris, dead trees, and other fire-hazard materials
- Institute high fire danger procedures such as smoking bans and fire bans
- Install fire-resilient building materials
- Modify treatment process for sediment in water
- Install backflow valves on service connections, fireproof concrete meter boxes, and use brass meters to prevent contamination of distribution pipes from volatile organic compounds
- For more mitigation options, see EPA's Incident Action Checklist for Wildfires



4.0 Detection Strategies

This section of your ERP should contain strategies that can aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of your utility.

4.2 Water Contamination

Notification of source water contamination may come from many different agencies and organizations including your primacy agency, 911, LEPC, the National Response Center, a source water protection collaborative, or local watershed groups.

Potential contamination in your finished water or distribution system can be detected through systematic tracking of customer complaints, public health surveillance, physical security monitoring at access points to finished water, grab sample analysis, online water quality monitoring, and advanced metering infrastructure that can alert your utility of potential backflow events or meter tampering.

4.0 Detection Strategies: SRS

A Water Quality Surveillance and Response System (SRS) is a framework designed to enhance a drinking water utility's capability to quickly detect and respond to water quality issues

- Online Water Quality Monitoring
- Physical Security Monitoring
- Customer Complaint Surveillance
- Public Health Surveillance
- Advanced Metering Infrastructure



Learn more here:

<https://www.epa.gov/waterresilience/water-quality-surveillance-and-response-0>

Questions?





Action Items

- Consider addressing contamination incidents as you review and revise your RRA and ERP
- Connect with EPA's Office of Water Emergency Response and Cybersecurity by scanning this barcode to our [Water Resilience Website](#)

Scan Me





Contact Us

**Office of Water Emergency Response and
Cybersecurity**

dwresilience@epa.gov

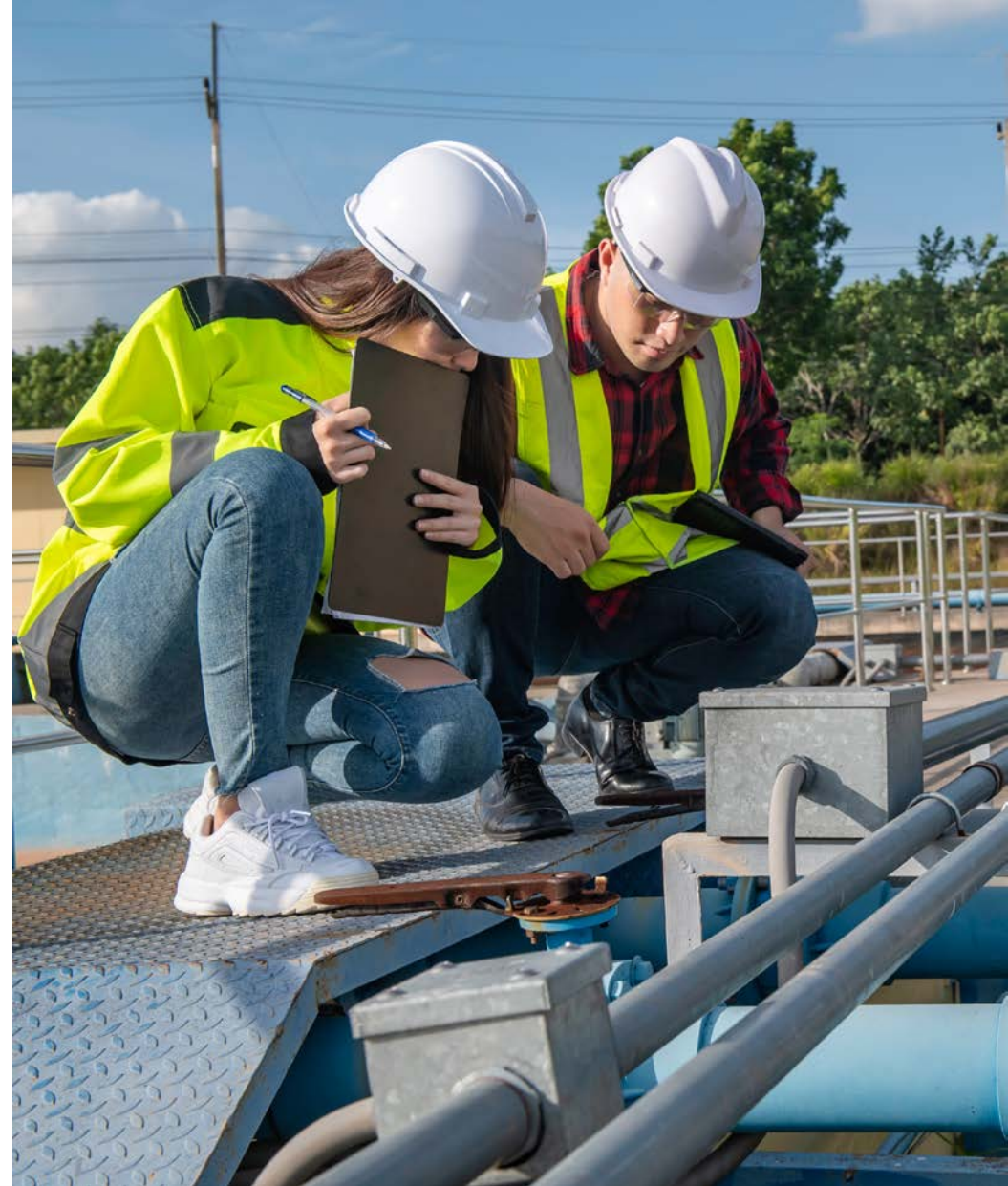
www.epa.gov/waterresilience

SDWA Section 1433/AWIA Section 2013

www.epa.gov/waterresilience/awia-section-2013

Contamination Preparedness and Response

[www.epa.gov/waterresilience/contamination-
preparedness-and-response](http://www.epa.gov/waterresilience/contamination-preparedness-and-response)





Contact Us

EPA's Office of Water Emergency Response and Cybersecurity (OWERC)

Visit our website: www.epa.gov/waterresilience

Email us: OWERC-Outreach@epa.gov

Scan the QR code to join OWERC's email list:

