Community Water System

Emergency Response Plan Template

Template and Instructions

Introduction

This template, developed by the U.S. Environmental Protection Agency (EPA), assists water utilities with developing an Emergency Response Plan (ERP) and in accordance with America's Water Infrastructure Act of 2018 (AWIA) Section 2013, which amended Section 1433 of the Safe Drinking Water Act (SDWA). The Act requires community water systems serving populations greater than 3,300 to develop or update an ERP that incorporates findings of their risk assessment.

AWIA ERP TEMPLATE

An ERP describes your utility's strategies, resources, plans, and procedures to prepare for and respond to an incident, natural or man-made, that threatens life, property, or the environment. Incidents can range from small main breaks or localized flooding to large scale hurricanes, earthquakes or system contamination, among other examples.

When an incident occurs that requires response, you will need to activate the procedures and protocols described in your ERP. This can include implementing personnel emergency roles and responsibilities, standing up your utility's Incident Command System (ICS) structure, recalling personnel on vacations, and notifying external agencies such as your local emergency management agency, police, fire department, and state regulatory agency.

As you respond to an incident, you should immediately begin documenting your decisions, actions, and expenditures. This step is important for justifying incident costs and potentially seeking reimbursement once the incident is resolved. Good incident documentation involves creating a paper trail for receipts, records, photographs, and personnel timesheets. A formal mutual aid agreement will also help in getting reimbursement for any mutual aid you receive during a declared disaster. Access both the Federal Emergency Management Agency (FEMA) Public Assistance Program and EPA's Fed FUNDS websites for guidance on documenting incident costs.

How to Use this Template

The template serves as a starting point in building an ERP that meets SDWA Section 1433 requirements. Since each water utility has unique challenges in managing an incident response, you may want to include additional sections with information tailored to your utility's needs. You may also use a completely different format, such as a state regulatory agency or water association template. Irrespective of what format you use**, you must ensure that your ERP addresses all of the ERP criteria as outlined in SDWA Section 1433:**

In addition to these instructions, you may view a recorded presentation on how to use this template at EPA's AWIA Workshop Part 3: ERP Template and Guidance YouTube site.

SDWA 1433 ERP Criteria
Strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system
Plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water
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 communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers
Strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system

Before beginning your ERP, save the ERP template to your computer, delete the EPA cover page from the template, remember to delete italicized example text in the tables, and follow the steps below to gather the key information you'll need to develop or update your ERP:

1. **Conduct an RRA:** the findings and countermeasures identified in your RRA, which is required under SDWA Section 1433 for community water systems serving greater than 3,300 persons, will enhance the effectiveness of your ERP and must be incorporated. For example, your RRA may identify hurricanes as a significant risk for your utility and outline cost-effective countermeasures to lower your risk. Your ERP, grounded in the results of the RRA, then describes the processes and procedures that can be implemented to mitigate hurricane impacts (e.g., flooding) to your utility. See EPA's online Vulnerability Self-Assessment Tool or Small System Risk and Resilience Assessment Checklist for more information on conducting an RRA.

2. **Identify state regulatory requirements**: many states have specific regulatory requirements for ERP content and provide their own ERP templates. However, your utility is responsible for checking with your state to be sure that any state-provided templates also meet SDWA Section 1433 ERP requirements, as outlined in this template.

3. **Identify and integrate local plans:** your ERP should dovetail with other emergency plans in your community as much as possible. These may include county emergency operations plans, hazardous materials (Hazmat) response plans, or local hazard mitigation plans.

4. **Coordinate with LEPCs and response partners:** The SDWA Section 1433 requires that community water systems, to the extent possible, coordinate with their existing Local Emergency Planning Committee (LEPC) when preparing or revising their ERP. EPA's Local Emergency Planning Committees website can help you identify your LEPC. Partnering with stakeholders like LEPCs allows all parties to understand response processes and procedures used during a drinking water incident.

5. **Plan for resources:** the resources (i.e., personnel, equipment, supplies, and facilities) your utility owns or has access to will influence how you develop your ERP procedures. Resource Typing, defined as categorizing by capability the resources requested, deployed, and used in incidents, is a key activity in identifying resource gaps. You will need to partner with your local emergency management agency and regional mutual aid partners to develop strategies to obtain needed equipment and resources that you do not own, or that are not readily available. See the American Water Works Association (AWWA) Water Sector Resource Typing Guidance prepared under a Memorandum of Agreement with FEMA and in collaboration with EPA.

Thoroughly addressing cybersecurity is essential in your CWS's ERP. The SDWA Section 1433 states that ERPs must "incorporate findings of the [risk and resilience] assessment' and "shall include strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system." Therefore, based on the results of your RRA, you must incorporate or reference (e.g., in other function-specific procedures such as Incident Specific Response Procedures) cybersecurity response, mitigation, and detection actions in your ERP. This can be done under Sections 2.1, 3.2, 3.3, and 4 of the accompanying ERP template.

If your utility would prefer to have assistance assessing cybersecurity in its RRA, consider participating in EPA's Water Sector Cybersecurity Evaluation Program. In this program, EPA will conduct a free cybersecurity assessment using EPA's Cybersecurity Checklist for water and wastewater systems to identify cybersecurity gaps and vulnerabilities. Utilities who participate in the program will receive an Assessment Report and a Risk Mitigation Plan in a secure file that can be added to their RRA and be used to help inform the cybersecurity measures in their ERP.

For more information and resources related to cybersecurity, please visit the EPA Cybersecurity for the Water Sector website.

To meet SDWA Section 1433 certification requirements, you must maintain a copy of your ERP for five years after the certification date. Since your ERP may contain sensitive information, it should be stored safely and securely. Consider storing one copy on site and one copy off site in case you are unable to access your offices or facilities during an incident. You may also store an electronic copy on a shared drive or other digital platform (protected by a firewall) easily accessible by your utility personnel. Similarly, up-to-date plans and schematics of your treatment and distribution systems, as well as current operations manuals, could be maintained and kept in at least two secure locations.

Your ERP should be viewed as a living and evolving document with established maintenance guidelines for routine and non-routine updates, the circumstances under which the updates will occur, and the personnel or departments responsible for the updates. *The SDWA Section 1433 requires that utilities serving a population of 3,300 persons or more review and, if necessary, update their ERP at least once every five years, within six months of the utility reviewing and, if necessary, updating its RRA*. Utilities must submit new certification statements to EPA after each required ERP update.

Lastly, once your ERP is complete, consider training your utility personnel and response partners on its contents and their individual roles and responsibilities. A multi-year training and exercise plan can help you schedule periodic trainings for both senior and new personnel to help ensure that your ERP procedures will be effectively implemented during an actual response. Tabletop exercises are also an effective means to practice and test your response procedures – access EPA's Tabletop Exercise Tool website to learn how.

How to Certify your SDWA-compliant ERP

Community water systems serving populations greater than 3,300 must certify to EPA that they have completed an ERP that incorporates findings of the RRA conducted under SDWA Section 1433 and meets the criteria outlined there. U.S. EPA strongly recommends you electronically submit your community water system's ERP certification statement by clicking here. Alternate certification statement submittal options are accessible by clicking here.

The SDWA Section 1433 requires you to submit only a certification of completion of an RRA and an ERP; therefore, do not submit the RRA and ERP documents to EPA.

TABLE OF CONTENTS

UTILITY INFORMATION

During an incident, you need to have system information about your water utility readily available for your personnel, first responders, repair contractors/vendors, the media, and other response partner agencies.

i Utility Overview

Provide basic information about your utility in the table in this section. The information required here should be readily available.

You may also choose to provide additional detailed information about your utility, such as distribution system maps, plan drawings, site plans, source water locations, and operations manuals. This information, although not required by SDWA Section 1433, may serve as orientation materials for response partners and others who may not be familiar with your utility. You can use the checklist in this portion of the ERP template to ensure that applicable and relevant documents, as appropriate, are included as a part of your ERP.

ii Personnel Information

It is important to have a personnel roster available during an incident to quickly contact your employees. Attach your staff roster or fill out the table provided in this section.

iii Primary Utility Components

In the tables provided, list as appropriate all the components necessary to maintain effective operation of your utility. This includes information on wells, intakes, treatment plants, storage/distribution systems (e.g., tanks, primary mains, pumping stations), and treatment chemical storage, as appropriate. These components were identified as you developed your RRA or, if you use an asset management system, you may simply generate a list of your primary components and insert that list into this section. See EPA's Asset Management website for more information.

iv Industry Chemical Handling and Storage Facilities

Industry surrounding your utility can also be impacted by incidents such as accidental releases, hurricanes or earthquakes. It is important that you understand what chemicals may be released in your area during an incident and how they may impact your utility operations. You may have already identified these as threats in your RRA, or potentially in other documents such as a source water protection plan. Additionally, AWIA Section 2018 amended the Emergency Planning and Community Right to Know Act (EPCRA) to require state agencies to notify affected community water systems of spills that may impact utility source water intakes, and to allow community water system access to EPCRA Tier II chemical storage information; see EPA's AWIA Section 2018 website for more information.

As you complete the tables in this section, you should consult your LEPC, which will know the locations of Tier II chemical handling and storage facilities in your area. You may also refer to your source water protection plan and online planning tools, such as EPA's Drinking Water Mapping Application to Protect Source Waters (DWMAPS) website, to help you locate potential sources of contamination upstream from your facility.

v Safety

Having easy access to safety materials and important safety information and procedures will help protect utility personnel during an incident. You can use the tables in this section of the ERP template to record that information, or, if your utility has a Health and Safety Plan, you can simply reference that in this section.

vi Response Resources

Having an accurate inventory of available resources (e.g., equipment, supplies) either maintained onsite or readily available offsite (e.g., neighboring water system) allows utility responders to know what resources are immediately available during an incident. Some resources may have already been identified as existing countermeasures in your RRA. For example, you may have identified generators that can help mitigate the impacts of a power outage.

Resource typing defines and categorizes resources by capability and classifies resources by "kind" and "type". For instance, a generator is a "kind" of resource, and a 50Kw generator is a "type" of generator. Resource typing is performed to ensure that a uniform system exists when requesting or providing resources. Resources that you can inventory and type include both personnel (e.g., special skills, licenses) and equipment. You can learn more about resource typing by accessing FEMA's NIMS Components - Guidance and Tools website or the AWWA Water Sector Resource Typing Guidance and the Implementation Toolkit for Water Sector Resource Typing.

Insert an existing inventory sheet or fill out the table provided in this section. Insert copies of any equipment manuals or instruction sheets, as applicable, at the back of your ERP.

vii Key Local Services

In the table provided note the closest locations of key logistical and medical services that you or mutual aid and assistance providers may need during an incident. These include hospitals, gas stations, and other facilities like drugstores or ATM machines. Include a map or maps if available.

1 RESILIENCE STRATEGIES

This section of your ERP should contain strategies and resources to improve the resilience of your system, including the physical security and cybersecurity of your system. Resilience strategies incorporate how you will assign roles and responsibilities, how you will work with response partners, and how you intend to communicate during an incident. Further information regarding both physical security and cybersecurity can be found in Section 2.1 below.

1.1 Emergency Response Roles and Responsibilities

An effective ERP involves active participation of a variety of both utility and external response partner agency personnel, each having well-defined roles and responsibilities. Your ERP should identify the roles and responsibilities in a manner that works well for your utility and your response partner agencies. The roles and responsibilities outlined in your ERP should cover your utility response actions as well as what response actions are expected from local, state and federal supporting agencies during an incident.

It is important to first establish an Emergency Response Lead (ER Lead) and Alternate ER Lead at your utility. The ER Lead should be the main point of contact during an incident and may also have a role in developing and updating the ERP, as well as forming partnerships with external stakeholders. Both the ER Lead and the alternate may need to be accessible 24 hours a day, seven days a week.

Your utility should also consider forming an ER team that uses a well-defined command structure. Within the ER team, identify personnel who will notify others (e.g., regulatory agency, fire department, downstream water users), who will speak to the public on topics such as water use advisories and who will answer the phones during incidents. Some of these tasks may be performed by the ER Lead or alternate, but during a large-scale incident with high public interest, even simple tasks like answering the phones can become overwhelming. Coordinate with your response partners for additional assistance if you feel your utility does not have the resources to effectively manage a large-scale incident.

In this section, use the table to describe the roles and responsibilities for key utility and external response partner agency personnel (e.g., law enforcement, public health).

At the local level, the use of memoranda of understanding, mutual aid and assistance agreements, and other agreements can be invaluable for water utilities in time of need. These documents contain legal language that is mutually agreed upon by the parties to the agreements and generally define worker's compensation, indemnification, and other response related considerations. For mutual aid and assistance, utilities can participate in Water and Wastewater Agency Response Networks (WARNs), or other local water utility response networks. A WARN is a group of "utilities helping utilities" within a state to respond to and recover from emergencies by sharing resources with one another. Learn more by accessing EPA's WARN website or AWWA's WARN website.

1.2 Incident Command System (ICS) Roles

Your utility should consider integrating a standardized incident management structure, such as the Incident Command System, into your response procedures. ICS is used to organize both near-term and long-term field-level operations for a broad spectrum of emergencies from small to complex incidents, both natural and manmade. ICS is used by all levels of government - federal, state, local, and tribal - as well as by many private-sector and nongovernmental organizations. ICS is also applicable across disciplines (e.g., fire, police, public works), allowing your local, state and federal response partners to more easily integrate into your utility response structure, or vice versa.

You can learn more about ICS at the FEMA ICS Resource Center website, which provides ready-to-use forms such as the ICS Form 207, Incident Organization Chart. This chart can be completed for your utility and inserted into your ERP.

1.3 Communication

Communication during an incident is critical to relay information to employees, government agencies, the public, the media, and others about potential risks to health, infrastructure, and the environment. This information should be presented in a timely and accurate manner to enhance understanding of an incident, build trust and credibility, encourage constructive dialogue, and provide guidance on appropriate protective actions following the incident. Good communication procedures outlined in your ERP will guide your utility personnel on when and how to communicate (e.g., who is responsible for notifying the utility emergency response team and outside agencies, and what information should be relayed), how to work with response partners and the media, how to compose messages, and how to deliver messages (e.g., website, television, social media). You should also consider contingency measures for loss of communications (e.g., a switch to 2-way radios, meet at a certain location). More information on these measures can be found at EPA's Water Sector Guide to Telecommunications During Power Outages website.

Internal Communication

Internal communications should address what, when, and how a message will be provided to utility personnel who are directly and indirectly involved in an incident. Internal communications and notification lists should outline the personnel responsible for activating communications, the order in which notification occurs, and the members of the emergency response team (as defined in the ICS structure). In addition, your strategy should provide information on the specific communication method(s) that could be used (e.g., telephone, radio, e-mail, face-to-face). Use the table in this section to list all utility emergency response team members, their response role, title, and contact information.

External Response Partner Communication

Your external response partner notification list should ensure that all appropriate partners are notified. Procedures should also be established as to who should be notified, when they should be notified, and who is responsible for making the notifications from your utility. It is recommended that local response partners be engaged first, followed by county, state, and federal agencies as appropriate. Also, keep in mind any specific state regulatory notification requirements. In some

instances, these agencies may require that they be notified within a specified time from when your utility first experiences or notices an incident that may significantly impact operations. Sending a utility representative to your local emergency operations center (EOC) helps with external partner communication during a longer duration incident. At your local EOC, you can have face-to-face conversations with representatives from multiple response partner agencies. The table in this section of the ERP template can be used to list all your utility's response partners as well as contact information.

After initially notifying your partners of an incident, the next step is regular sharing of incident information as it becomes available. Many localities use web-based information management systems (e.g., WebEOC) that provide a single access point for the collection and dissemination of emergency or incident-related information. Group e-mails could also be used, or you could leverage an agency such as your local Emergency Management Agency (EMA) to help keep your partners informed.

Communication with Critical Customers

A list of critical customers should be maintained as a part of your ERP. Some of these customers may be given priority notification due to their reliance on the water supply either for medical reasons (e.g., hospitals, dialysis clinics), based on usage (e.g., fire department, industry, manufacturing), public health mission, or because they may serve customers considered to be sensitive sub-populations (e.g., those who may be more sensitive than the general population to the harmful effects of contaminants in drinking water). Certain critical customer types, such as large water users, may have already been identified in your RRA when you discussed your customers. The table in this section of the ERP template can be used to list all your critical customers and their contact information.

Communication Equipment Inventory

You should inventory and track all your utility's communication equipment to help ensure maintenance is scheduled as appropriate and that equipment replacement can be planned. Service plans and contracts should also be tracked to make sure they are current. Your utility's communication equipment, and any service plans or contracts that support it, may have been identified as existing countermeasures in your RRA. Use the table to inventory your communications equipment (e.g., mobile phones, two-way radios).

1.4 Media Outreach and Risk Communication

List contact information in the table provided for all media outlets that your utility may coordinate with during notification efforts. This may include newspapers, social media sites, television, and radio stations, etc.

Risk communication is a tool that helps water utilities deal with public messaging during emergencies to enhance knowledge and understanding of an incident, build trust and credibility, encourage constructive dialogue, and provide guidance on appropriate protective actions. EPA provides guidance on its website for Risk Communication Plans that may be incorporated into your ERP to guide utility personnel on when and how to communicate, how to compose messages, how to work with response partners and the media, and how to develop a delivery system for messages.

1.5 Public Notification Templates

Insert your templates for public notifications in this portion of the ERP template, or reference where they may be found. Be sure that your templates are consistent with the regulatory requirements for public notification contained in the Public Notification Rule (see 40 CFR 141, Subpart Q) and all relevant state regulations. Refer to EPA's Public Notification Rule Compliance Help for Water System Owners and Operators website for regulatory guidelines, additional information, and public notification templates. Check with your regulatory agency for any state-specific requirements.

2 EMERGENCY PLANS AND PROCEDURES

This section of your ERP should contain plans, procedures, and equipment that can be used in the event of a malevolent act or natural hazard that threatens your utility's ability to deliver safe drinking water. Two types of emergency response plans and procedures should be considered as part of your ERP: Core and Incident-specific. Both types are listed in this section.

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.

Access

A significant challenge your utility may face after a major incident is gaining access to critical facilities and other locations to assess damage and implement repairs. Access to sites may be hampered by debris, road and bridge damage, downed power lines, snow and ice, and roadblocks established by law enforcement agencies for public protection. Use the table is this section to identify access related challenges in your area and identify ways to mitigate those challenges.

DHS's Crisis Event Response and Recovery Access (CERRA) Framework website informs local officials and emergency planners of key components and best practices to consider when planning for access and re-entry operations. The CERRA Framework specifically identifies water utility personnel as first responders that require access to water utility assets during and after disasters. Your utility should inquire with its jurisdiction to determine if they are applying the principles and concepts of this framework.

Physical Security

Protecting utility facilities, equipment, and vital records is essential to restoring operations once an incident has occurred. Your ERP should identify measures aimed at securing and protecting your utility. Use the table in this section to describe physical security measures for your utility assets. You can learn more about physical security measures under the Detection Strategies section of the template.

Cybersecurity

Cyber-attacks on electronic information technology (IT) and operation technology (OT) are increasingly common. These attacks can result in the loss of critical communications with employees, customers, and process controls; the destruction of records and networks; and the theft of valuable utility and customer data. Impacts from cyber-attacks can have a severe adverse impact on water utility operations and entail high costs for response and recovery. The SDWA Section 1433 states that ERPs must "incorporate findings of the [risk and resilience] assessment' and "shall include strategies and resources to improve the resilience of the system, including…cybersecurity." Therefore, your utility's ERP must address the overall cybersecurity resilience of the water system and findings of the cybersecurity portion of the RRA. To address cybersecurity concerns in your ERP, you can use the resources at EPA's Cybersecurity Planning website, such as the Cybersecurity Incident Action Checklist or use the provided table to describe the processes and procedures your utility will use during a cyber incident. In addition, AWWA's Water Sector Cybersecurity Risk Management Guidance and Assessment Tool provide a means for utilities to assess vulnerabilities, track implementation status, and develop mitigation options.

Power Loss

Your utility should consider preparing for a loss of power and know what to do to respond and recover from such an incident. An extended power loss can have devastating impacts on your utility and the community you serve. Inoperable

pumps at a drinking water utility can make firefighting difficult and cause local health care facilities and restaurants to close. Use the table in this section to describe your utility's resources and procedures for the loss of grid power. EPA's Build Power Resilience at Your Water Utility website can help you to better prepare and respond to an unexpected power loss.

Emergency Alternate Drinking Water Supplies

Your ERP should consider clearly defining how your utility, along with other external response partners such as emergency management, would supply alternate drinking water to your community during both short-term (hours to days) and long-term (weeks to months) outages. Alternate drinking water sources may include interconnections with neighboring water utilities, bulk water haulers, bottled water supplied locally or regionally (a common federal response), or locally produced water via packaged pre-treated water or mobile treatment units. List your emergency alternate drinking water supplies in the table provided. You can learn more about emergency alternate drinking water by accessing EPA's Planning for Emergency Drinking Water Supplies guidance website.

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.

Family and Utility Personnel Well Being

Your personnel are more likely to report for duty or stay on the job during an incident if they know that their families are safe and cared for. Use the table provided to identify actions that could be taken before, during, and after an incident that are unique to each hazard (e.g., hurricanes, floods, earthquakes). Actions may include alternate work locations, on-site emergency supplies such as cots, and ensuring that staff have developed family disaster plans. The ready.gov website can assist with preparing individual family disaster plans. Local emergency management agencies can also help identify the hazards in your area and outline the local plans and recommendations for each hazard.

Your utility should also consider how it wants to support personnel who may be working extended shifts during an incident. The All-Hazard Consequence Management Planning for the Water Sector document provides a list of actions you could take to support personnel.

2.2 Incident-Specific Response Procedures

Incident-Specific Response Procedures (ISRPs) are specialized procedures tailored to a particular type of incident. These procedures will typically align with the specific threats (e.g., flooding, earthquake, cyber) identified in your RRA. So, if tornadoes were identified as a threat to your utility you should ensure that your ERP has a procedure for responding to tornadoes.

ISRPs provide a quick approach for responding to a specific incident and complement actions already initiated under your ERP. You may only need one or two pages to cover specific response information since you have already addressed basic emergency response steps under your core response procedures. An ISRP should be an accessible (i.e., "rip and run") document that can be detached and taken to the field.

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

You can insert your utility's existing ISRPs into this section of ERP template. EPA also provides a number of incident action checklists (IACs) that you can use to help develop your own ISRPs. Or, you can use EPA's IACs as your utility's ISRPs by checking the appropriate activities. These customized IACs can then be inserted into your ERP. EPA also published the Prepared for Contamination in your Distribution System? guidance that can help you develop a distribution system contamination ISRP.

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. These mitigation actions, procedures, and equipment help your utility to better withstand and rapidly recover from incidents (e.g., cyber-attack, flooding, earthquake), thereby increasing overall resilience. It is more cost-effective to mitigate the risks from natural disasters than it is to repair damage after the disaster. Examples of mitigation projects include:
- Elevation of electrical panels at a lift station to prevent flooding damage
- Replacement of piping with flexible joints to prevent earthquake damage
- Reinforcement of water towers to prevent tornado damage

Mitigation measures require financial investment by your utility; however, mitigation could prevent more costly future damage and improve the reliability of service during a disaster. Learn more about hazard mitigation, including coordinating with your community's local mitigation planners, identifying potential disaster-specific mitigation projects, and funding proposed mitigation projects by accessing the Hazard Mitigation Guide for Natural Disasters: A Starter Guide for Water and Wastewater Utilities on EPA's website.

3.1 Alternative Source Water Options and Interconnected Utilities

Information on alternative source water options and interconnected utilities helps you to maintain awareness of how these sources and utilities may mitigate impacts during incidents. For example, drilling a backup well to supplement or replace your primary well during an incident is a mitigation action to increase resilience to the loss of your primary well. Interconnections allow two (or more) utilities to each have a backup source of drinking water by relying on each other. You can list these kinds of mitigating actions in the table provided here.

3.2 Cybersecurity Mitigation Actions

One of the best ways to avoid cyber-attack impacts at your utility is to take every measure you can to prevent them. To help you implement cybersecurity mitigation actions, EPA developed the Checklist of Priority Cybersecurity Practices for Water Systems which is included in the ERP template (Section 3.2). This checklist will guide you through eight priority topics based on CISA's Cross-Sector Cybersecurity Performance Goals with a series of questions regarding your current cybersecurity practices. The checklist also contains recommendations for mitigating actions you can take if you answer

"no" to a question. Just note that you may have already used this checklist if you conducted your RRA using the following EPA guidance: Small System RRA Checklist; Vulnerability Self-Assessment Tool (VSAT); Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems; Water Cybersecurity Assessment Tool and Risk Mitigation Template.

To learn more about cybersecurity mitigation actions, see the EPA Cybersecurity for the Water Sector web page and EPA's Cybersecurity IAC "Actions to Prepare for a Cyber Incident" section.

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 here. To learn more about specific mitigation options for water utilities, see the following online resources from EPA and others:

Build Pandemic Resilience at Your Water or Wastewater Utility - Provides good practices, real-world examples, and key resources for responding to pandemic emergencies and building long-term resilience.

Cyber Hygiene Scanning and Testing Services - Helps utilities reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

Drought Response and Recovery Guide for Water Utilities - Provides worksheets, best practices, videos and key resources for responding to drought emergencies and building long-term resilience. The guide relays lessons learned from seven small- to medium-sized utilities nationwide that have responded to extreme drought conditions.

Earthquake Resilience Guide for Water and Wastewater Utilities - Helps water and wastewater utilities to be more resilient to earthquakes. It contains best practices from utilities that have used mitigation measures to address the earthquake threat.

Flood Resilience Guide - Helps water utilities know the local flooding threat and identifies practical mitigation options to protect critical assets.

Power Resilience Guide for Water and Wastewater Utilities - Helps utilities identify how to increase their resilience to power outages.

Resilient Strategies Guide for Water Utilities - Helps water utilities understand how extreme weather events can impact utility operations and missions and provides examples of different actions utilities can take to prepare for potential impacts.

Supply Chain Resilience Guide for Water and Wastewater Utilities - Provides actions to prepare for, or respond to, both equipment and water treatment chemical supply chain challenges. Through best practices, utility case studies, and EPA resources, the Guide provides information that utilities can use to mitigate the impacts of a future supply chain disruption.

4 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. These detection strategies can be almost no-cost (e.g., instituting a "See Something, Say Something" campaign at your utility) or require more resources (e.g., installing motion sensors and video cameras to monitor for facility break-ins or tampering) to implement. Effective response to an emergency requires timely detection, which allows your utility to implement its ERP as soon as possible.

The most appropriate method of detecting a possible incident depends on the type of threat. Where possible, multiple detection methods should be used. This increases your utility's ability to receive timely warning of an imminent threat or incident. Examples of effective strategies for detecting common threats are listed below, and you can list your utility's strategies in the table provided in this section.

4.1 Unauthorized Entry into Utility Facilities

Properly installed and maintained intrusion detection systems provide almost instantaneous notification of break-ins and other unauthorized access into your utility facilities, but notifications from local law enforcement officers and community watch groups are also effective.

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. Therefore, it is important to build working relationships with these entities and exchange emergency contact information.

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. These are all components of an integrated Water Quality Surveillance and Response System as described on EPA's Water Quality Surveillance and Response website.

4.3 Cyber Intrusion

Cyber-attacks against public water systems occur, and implementing basic cyber hygiene practices can help your utility to prevent and detect cyber incidents. Signing up for both EPA water sector and DHS Cybersecurity and Infrastructure Security Agency (CISA) cyber alerts provides timely information about current security issues, vulnerabilities, and exploits. Utilities that rapidly adopt security patches and implement corrections to system vulnerabilities can significantly reduce the risk of a cyber-attack. Learn more about detecting a cyber intrusion in the joint CISA, Federal Bureau of Investigation (FBI) and EPA Incident Response Guide: Water and Wastewater Sector document.

4.4 Hazardous Chemical Release

Routine inspection of your hazardous chemical storage facilities will aid in detecting problems that could lead to an unexpected chemical release. Identified problems can be fixed to help prevent emergencies. Air monitors, such as for chlorine gas, can alert you to any leaks in a timely fashion.

4.5 Natural Hazards

Natural hazards such as extreme weather can cause severe damage to your utility. Real-time tools such as EPA's online Water Utility Response On-The-Go Mobile Application can help you track severe weather and access other information and forms (e.g., damage assessment) for an efficient response.

4.6 Power Outages

Your utility can detect impending power outages more effectively by signing up to receive notifications from your power provider for any planned maintenance activities or brown outs.

APPENDIX: PRACTICAL MITIGATION OPTIONS FOR UTILITIES

After assessing risks from various threats (e.g., natural disasters, malevolent acts) and developing an emergency response plan as required by SDWA Section 1433, utilities should pursue countermeasures or mitigation actions to reduce risk. Mitigation actions such as flood barriers, seismic pipe, and intrusion detection, reduce risk by reducing adverse impacts from the threat and enabling your utility to restore services more rapidly. As a supplement to the Emergency Response Planning Instructions and Template, this appendix identifies some practical mitigation options for various threats. To help you find ways to fund these mitigation options, see EPA's Federal Funding for Utilities – Water/Wastewater– in National Disasters (Fed FUNDs).

All-Threats
- Join a mutual aid network (Water/Wastewater Agency Response Network)
- Coordinate with key partners and critical customers (e.g., hospitals)
- Train and exercise your emergency response plan
- Plan for supply chain disruptions before they occur, see EPA's Supply Chain Resilience Guide for Water and Wastewater Utilities web page.

Power Outage
- Contact your power utility and local emergency management agency to prioritize restoration of key facilities
- Define power needs for key assets (lift station) to ensure proper backup
- Install connections to rapidly hook up generators to your key systems
- Purchase, rent or borrow a backup power generator (e.g., mutual aid)
- Secure generators against wind, flooding (i.e., elevate) and seismic activity
- Maintain fuel on-site and/or have multiple ways to obtain fuel (vendors)
- For additional mitigation options, see EPA's Build Power Resilience at Your Water Utility web page

Flooding
- Implement a program to keep all drains and culverts clear of debris
- Use sandbags to make a quick and low-cost barrier to minor flooding
- Install flap valves on low-lying overflow pipes to protect finished water
- Secure or elevate chemical/air tanks to prevent floating and content release
- Elevate, relocate or floodproof instrumentation, electrical controls, pumps,
- Install gates and backflow valves to prevent flooding of lift station and keep list of pump vendors
- Move assets (e.g., vehicles) to higher ground and develop alternative ways to access your facilities
- For additional mitigation options by asset, see EPA's Flood Resilience Guide

Earthquake
- Retrofit occupied utility buildings to prevent collapse
- Seismically retrofit water towers to protect public from catastrophic failure
- Reinforce "backbone" by retrofitting pipelines to critical facilities (hospitals)
- Replace inflexible joints with flexible or ball joints on storage tanks and pumps
- Install buttress walls on water basins and automatic shutoff valves on tanks
- Design upper casing on wells to resist loads or locate outside of seismic zone
- For more mitigation options by asset, see EPA's Earthquake Resilience Guide

Drought
- Implement a leak detection and repair program to reduce lost water
- Consider interconnections with other water systems and water reuse
- Consider adding raw water storage and aquifer recharge
- Develop conservation program with public outreach and join WaterSense
- Coordinate water usage with neighboring irrigation districts and communities
- For more mitigation options, see EPA's Drought Response and Recovery Guide

Pandemic
- Develop a pod system to minimize contact among groups of employees
- Establish a corporate account with e-commerce websites or other health and safety supply vendors to purchase medical and safety supplies available to frontline workers
- Assess your system's Information Technology (IT) capability to ensure it can accommodate remote work arrangements without compromising security.
- For more mitigation options, see EPA's Build Pandemic Resilience at Your Water or Wastewater Utility web page

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

Tornado
- Reinforce water tower legs and welds
- Remove sources of potential flying debris and bolt down chemical tanks
- Design new facilities, control rooms and offices to withstand high winds
- Secure and anchor any trailers or temporary structures and designate them as non-habitable during severe weather
- For more mitigation options, see EPA's Incident Action Checklist for Tornadoes

Future Extreme Weather Events and Climate Change Impacts
- For adaptation strategies for future extreme weather (e.g., intense rain events) and ecological changes, see EPA's Resilient Strategies Guide
- View case studies for adaptation and climate change mitigation

Cyber-attack
- Reduce exposure to the public-facing Internet
- Conduct regular cybersecurity assessments
- Change default passwords immediately
- Conduct inventory of operational technology (OT) and information technology (IT) assets
- Develop and exercise cybersecurity incident response and recovery plans
- Backup OT and IT systems
- Reduce exposure to vulnerabilities
- Conduct cybersecurity awareness training
- For more mitigation options, see EPA's Cybersecurity for the Water Sector web page

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