

# Nevada Utility Vulnerability Assessment and Emergency Response Plan Guide



Nevada Office of  
Emergency Management  
Version 3  
October 29, 2025

## **Foreword**

NRS 239C.270 as amended in the 2019 legislative session by Senate Bill 69, requires all utilities as defined by NRS 704.020, 704.021, 704.023, 704.225, 704.027 and 704.028, to conduct a vulnerability assessment (VA) and prepare and maintain an emergency response plan (ERP). NRS 239C.270 further requires the utilities to submit its VA and ERP to the Office of Emergency Management. Utilities are also required by NRS 239C.270 to each year review its plan and submit the result of its review no later than December 31 of each year. ERPs, as required by statute and explored in this document, are intended to mitigate the risks and consequences of potential manmade and natural threats and hazards, specifically as they may occur to disrupt lifeline services to the residents of Nevada. This guide is intended to provide a starting point for Utilities just beginning the planning process or thoughts for refining existing plans.

Brett Compston  
Nevada Office of Emergency  
Management

# Document Change Control

Version	Date	Summary of Changes	Name
2	July 2024	Reviewed and updated document formatting, graphics, and overall guidance.	R. Graves
3	October 2025	Reviewed and updated the document and change from the Division of Emergency Management to Office of Emergency Management	B Elliott

# Table of Contents

I.	Purpose.....	1
II.	Scope.....	1
III.	Authorities.....	4
IV.	Utility ERP Requirements under NRS 239C.270 .....	5
V.	Vulnerability Assessment.....	6
VI.	Integrated Preparedness Program Management Guidance .....	8
VII.	Planning Guidance and Best Practices.....	10
	a. The Planning Process.....	10
	b. Access and Functional Needs Planning Best Practices .....	12
	c. Community Lifelines .....	16
	d. Utility ERP Format and Contents .....	17
VIII.	Organization Guidance and Best Practices .....	20
IX.	Equipment Guidance and Best Practices .....	22
X.	Training and Exercise Guidance and Best Practices .....	23
XI.	Utility ERP NRS Review and Submission Requirements .....	25
XII.	Conclusion .....	25
XIII.	Acronyms .....	26
	ANNEX A: Utilities ERP/VA Certificate of Review .....	28
	Annex B: Vulnerability Assessment Templates .....	31
	Annex C Rapid Emergency Response Plan Template .....	57

This page is intentionally left blank.

## I. Purpose

In the 2019 Nevada legislative session, the Legislature passed Senate Bill (SB) 69, which amended numerous Nevada Revised Statutes (NRS) which pertained to required Emergency Response Plans (ERP) for political sub-division Utilities, private, charter and public schools, and utilities. SB 69 also required the Office of Emergency Management (OEM) to develop emergency response planning guides for each of the industries affected by SB69 including utilities. The purpose of this statutory requirement is to facilitate the development of comprehensive and actionable all-hazards emergency response plans in order to provide opportunities for collaboration between utilities and first responder agencies through planning, training, and exercises in order to restore lifeline utilities during an emergency or disaster. This guide is intended to provide a basis for the development or refinement of quality Utility Vulnerability Assessment (VA) and Emergency Response Plans (ERP).

Many Utilities have developed well-crafted vulnerability assessments and plans, which meet their business, security, and operational needs. This guide is not intended to be an all-encompassing template, nor is it intended to discourage innovation. Rather, this guide is intended to make plain the minimum requirements annotated in Nevada Revised Statutes (NRS) 239C.250 and to recommend VA/ERP components and preparedness activities which will mitigate the effects of an emergency or disaster and pave the way to lifeline restorations.

## II. Scope

This guide applies to Utilities as defined by Nevada Revised Statutes (NRS) 704.020 – 704.028.

NRS 704.020-NRS 704.028:

1. “Public utility” or “utility” defined:
  - a. Any person who owns, operates, manages, or controls any railroad or part of a railroad as a common carrier in this State, or cars or other equipment used thereon, or bridges, terminals, or sidetracks, or any docks or wharves or storage elevators used in connection therewith, whether or not they are owned by the railroad.
  - b. Any person, other than a provider of commercial mobile radio service, that provides a telecommunication service to the public, but only with regard to those operations which consist of providing a telecommunication service to the public.
  - c. Any provider of commercial mobile radio service, but such providers:
    1. Must be regulated in a manner consistent with federal law; and

2. Must not be regulated as telecommunication providers for the purposes of this chapter.

2. "Public utility" or "utility" also includes:

- a. Any plant or equipment, or any part of a plant or equipment, within this State for the production, delivery or furnishing for or to other persons, including private or municipal corporations, heat, gas, coal slurry, light, power in any form or by any agency, water for business, manufacturing, agricultural or household use, or sewerage service, whether or not within the limits of municipalities.
- b. Any system for the distribution of liquefied petroleum gas to 10 or more users.

↪The Commission may supervise, regulate and control all such utilities, subject to the provisions of this chapter and to the exclusion of the jurisdiction, regulation and control of such utilities by any municipality, town or village, unless otherwise provided by law.

3. The provisions of this chapter and the term "public utility" apply to all railroads, express companies, car companies and all associations of persons, whether or not incorporated, that do any business as a common carrier upon or over any line of railroad within this State.

#### NRS 704.021

1. Persons engaged in the production and sale of natural gas, other than sales to the public, or engaged in the transmission of natural gas other than as a common carrier transmission or distribution line or system.
2. Persons engaged in the business of furnishing, for compensation, water or services for the disposal of sewage, or both, to persons within this State if:
  - a. They serve 25 persons or less; and
  - b. Their gross sales for water or services for the disposal of sewage, or both, amounted to \$25,000 or less during the immediately preceding 12 months.
3. Persons not otherwise engaged in the business of furnishing, producing or selling water or services for the disposal of sewage, or both, but who sell or furnish water or services for the disposal of sewage, or both, as an accommodation in an area where water or services for the disposal of sewage, or both, are not available from a public utility, cooperative corporations and associations or political subdivisions engaged in the business of furnishing water or services for the disposal of sewage, or both, for compensation, to persons within the political subdivision.
4. Persons who are engaged in the production and sale of energy, including electricity, to public utilities, cities, counties or other entities which are reselling the energy to the public.
5. Persons who are subject to the provisions of [NRS 590.465](#) to [590.645](#), inclusive.

6. Persons who are engaged in the sale or use of special fuel as defined in [NRS 366.060](#).
7. Persons who provide water from water storage, transmission and treatment facilities if those facilities are for the storage, transmission or treatment of water from mining operations.
8. Persons who are video service providers, as defined in [NRS 711.151](#), except for those operations of the video service provider which consist of providing a telecommunication service to the public, in which case the video service provider is a public utility only with regard to those operations of the video service provider which consist of providing a telecommunication service to the public.
9. Persons who own or operate a net metering system described in paragraph (c) of subsection 1 of [NRS 704.771](#).
10. Persons who own or operate a net metering system or systems described in paragraph (a) of subsection 1 of [NRS 704.771](#) and deliver electricity to multiple persons, units or spaces on the premises if:
  - a. The electricity is delivered only to persons, units or spaces located on the premises on which the net metering system or systems are located;
  - b. The residential or commercial units or spaces do not have individual meters measuring electricity use by an individual unit or space; and
  - c. Persons occupying the individual units or spaces are not charged for electricity based upon volumetric usage at the person's individual unit or space.
11. Persons who for compensation own or operate individual systems which use renewable energy to generate electricity and sell the electricity generated from those systems to not more than one customer of the public utility per individual system if each individual system is:
  - a. Located on the premises of another person;
  - b. Used to produce not more than 150 percent of that other person's requirements for electricity on an annual basis for the premises on which the individual system is located; and
  - c. Not part of a larger system that aggregates electricity generated from renewable energy for resale or use on premises other than the premises on which the individual system is located.

↪ As used in this subsection, "renewable energy" has the meaning ascribed to it in [NRS 704.7715](#).

12. Persons who own, control, operate or manage a facility that supplies electricity only for use to charge electric vehicles.
13. Any plant or equipment that is used by a data center to produce, deliver or furnish electricity at agreed-upon prices for or to persons on the premises of the data center for the sole purpose of those persons storing, processing or distributing data, but only with



regard to those operations which consist of providing electric service. As used in this subsection, “data center” has the meaning ascribed to it in [NRS 360.754](#).

#### NRS 704.023

“Small-scale provider of last resort” means an incumbent local exchange carrier that is a provider of last resort of basic network service and business line service to customers through less than 60,000 access lines.

#### NRS 704.025

“Telecommunication” means the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information sent and received, regardless of the facilities, equipment or technology used.

#### NRS 704.027

“Telecommunication provider” or “telephone company” means any person required to obtain from the Commission a certificate of public convenience and necessity pursuant to NRS 704.330 to provide telecommunication service.

#### NRS 704.028

“Telecommunication service” or “telephone service” means the offering of telecommunication for a fee directly to the public, or such classes of users as to be effectively available directly to the public, regardless of the equipment, facilities or technology used.

### III. Authorities

- NRS 414: Emergency Management
- NRS 704.020 Utilities Defined
- NRS 239C.270 Vulnerability assessment and response plan of utility: Confidentiality; penalties.
- State Comprehensive Emergency Management Plan (SCEMP)
- Comprehensive Preparedness Guide (CPG) 101
- CPG 201 – Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide
- Homeland Security Exercise and Evaluation Program (HSEEP) January 2020

## IV. Utility ERP Requirements under NRS 239C.270

NRS 239C.270 Vulnerability assessment and response plan of utility and provider of new electric resources; confidentiality; penalties.

1. Each utility and each provider of new electric resources shall:
  - a. Conduct a vulnerability assessment in accordance with the requirements of the federal and regional agencies that regulate the utility or provider; and
  - b. Prepare and maintain an emergency response plan in accordance with the requirements of the federal and regional agencies that regulate the utility or provider.
2. Each utility shall:
  - a. As soon as practicable but not later than December 31, 2003, submit its vulnerability assessment and emergency response plan to the Office; and
  - b. At least once each year thereafter, review its vulnerability assessment and emergency response plan and, as soon as practicable after its review is completed but not later than December 31 of each year, submit the results of its review and any additions or modifications to its emergency response plan to the Office.
3. Each provider of new electric resources shall:
  - a. As soon as practicable but not later than December 31, 2019, submit its vulnerability assessment and emergency response plan to the Office; and
  - b. At least once each year thereafter, review its vulnerability assessment and emergency response plan and, as soon as practicable after its review is completed but not later than December 31 of each year, submit the results of its review and any additions or modifications to its emergency response plan to the Office.
4. On or before June 30 of each year, the Public Utilities Commission of Nevada, the Division of Environmental Protection of the State Department of Conservation and Natural Resources and the Office of Energy shall coordinate with the Office to compile a list of each utility and provider of new electric resources required to submit a vulnerability assessment and an emergency response plan pursuant to subsection 2 or 3.
5. Except as otherwise provided in [NRS 239.0115](#), each vulnerability assessment and emergency response plan of a utility or provider of new electric resources and any other information concerning a utility or provider that is necessary to carry out the provisions of this section is confidential and must be securely maintained by each person or entity that has possession, custody or control of the information.

6. Except as otherwise provided in [NRS 239C.210](#), a person shall not disclose such information, except:
  - a. Upon the lawful order of a court of competent jurisdiction;
  - b. As is reasonably necessary to carry out the provisions of this section or the operations of the utility or provider of new electric resources, as determined by the Office;
  - c. As is reasonably necessary in the case of an emergency involving public health or safety, as determined by the Office; or
  - d. Pursuant to the provisions of [NRS 239.0115](#).
7. If a person knowingly and unlawfully discloses such information or assists, solicits or conspires with another person to disclose such information, the person is guilty of:
  - a. A gross misdemeanor; or
  - b. A category C felony and shall be punished as provided in [NRS 193.130](#) if the person acted with the intent to:
    1. Commit, cause, aid, further or conceal, or attempt to commit, cause, aid, further or conceal, any unlawful act involving terrorism or sabotage; or
    2. Assist, solicit or conspire with another person to commit, cause, aid, further or conceal any unlawful act involving terrorism or sabotage.
8. As used in this section, “provider of new electric resources” has the meaning ascribed to it in [NRS 704B.130](#).

## V. Vulnerability Assessment

A Vulnerability Assessment (VA) is required for a complete ERP submission under NRS 239C.270(1)(a) and NRS 239C.270 (2)(a).

A Vulnerability Assessment for a utility is an assessment of any natural and technological hazards that could interrupt lifeline services to customers. The VA assesses the threat or hazard based on likelihood and the impact on the utilities’ ability to provide its mission essential services. The VA also establishes a list of mitigation measures a utility might be able perform to lessen the impact of the threat and hazards. Annex A shows two types of VAs a utility might wish to use. Some utilities are required to utilize a specific VA, please refer to your utility’s federal requirements.

## Vulnerability Assessment Instructions

### Step 1

#### Identify Potential Threats and Hazards

What threat and hazards could interrupt Mission Essential Function (MEF) performance (e.g. earthquake, flood, wildfire, haz-mat, civil disturbance, severe storm, terrorist attack, cyber, etc.)

### Step 2

#### Identify Potential Threats and Hazards Characteristics

What are the characteristics of the potential threats and hazards?

### Step 3

#### Estimate the Likelihood of the Threat or Hazard

Based on a numerical scale of 1 to 10, what is the likelihood each threat or hazard could occur and affect MEF (Mission Essential Function) performance?

### Step 4

#### Evaluate the MEF Vulnerability to Each Threat or Hazard

Based on a numerical scale of 1 to 10, how susceptible is the MEF to failure due to each threat or hazard.

### Step 5

#### Estimate Overall Impact if MEF Failure Occurs

Based on a numerical scale of 1 to 10, how significant is the impact if the MEF cannot be performed?

### Step 6

#### Determine Risk Value for Each Threat or Hazard

Based on the likelihood, vulnerability, and impact of the threat or hazard, what is the risk value for the MEF?

**Develop Mitigation Strategies**

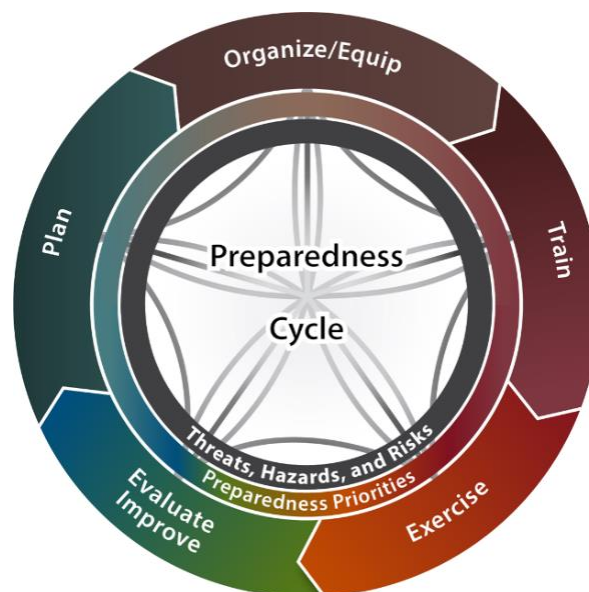
Determine what equipment or procedures may be implemented which will mitigate the effects of the threat or hazard and develop a prioritization action list.

## VI. Integrated Preparedness Program Management Guidance

It is recommended by OEM, but **not** required by NRS 239C.270, that each Utility implement an Integrated Preparedness Cycle of planning, organizing/equipping, training, exercising, and evaluating/improving (POETE) as a continuous process that ensures the regular examination of ever-changing threats, hazards, and risks.

POETE Areas	
<b>P</b> lanning	Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
<b>O</b> rganization	Individual teams, an overall organizational structure, and leadership at each level in the structure
<b>E</b> quipment	Equipment, supplies, and systems that comply with relevant standards
<b>T</b> raining	Content and methods of delivery that comply with relevant training standards
<b>E</b> xercises	Exercises and actual incidents that provide an opportunity to demonstrate, evaluate, and improve the ability of core capabilities to perform assigned missions and tasks to standards

The Cycle involves the assessment of threats, hazards, and risks; new and updated plans; and improvements implemented from previously identified shortfalls or gaps. The preparedness priorities are developed to ensure that the needed preparedness elements are incorporated. This cycle provides a continual and reliable approach to support decision making, resource allocation, and measure progress toward building, sustaining, and delivering capabilities based on the Utility's threats, hazards, and risks.

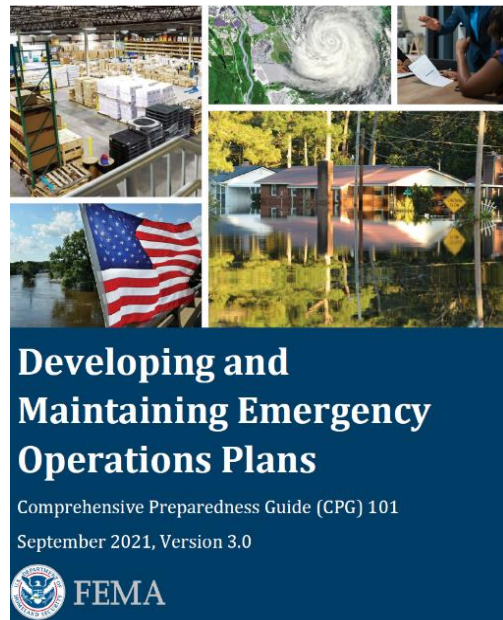


This integrated planning approach begins when property leaders, working with whole community stakeholders, identify and develop a set of multi-year preparedness priorities based on relevant threats, hazards, and risks to the Utility company with consideration for the life safety of its people and the continuity of its business. It is recommended by OEM but **not** required by NRS 239C.270, that each Utility utilize the Homeland Security Exercise and Evaluation Program (HSEEP) Program Management Templates available at <https://preptoolkit.fema.gov/web/hseep-resources/program-management> to facilitate Integrated Preparedness Cycle activities.

It is recommended by OEM but **not** required by NRS 239C.270, that the Utility utilize Federal Emergency Management Agency's (FEMA's) *Comprehensive Preparedness Guide 102 Threat and Hazard Identification and Risk Assessment (THIRA)* and *Stakeholder Preparedness Review (SPR) Guide* as guidance for conducting a threat, hazard, and risk assessment; however, the Utility may use any threat and hazards risk assessment processes or tools on the market based on its particular needs. Regardless of the threats, hazards, and risks assessment process and tools selected by the organization, it is recommended that the threat, hazard, and risk assessment serve as a foundation for identification of POETE Capability Gaps (see **Annex B: Example POETE Capability Gap Identification**). The organization can use the information from the threat and risk assessment and POETE Capability Gap analysis to establish preparedness activity priorities to develop an Integrated Preparedness Plan (IPP) and Multi-Year Preparedness Activity Schedule.

## VII. Planning Guidance and Best Practices

FEMA's CPG 101 *Developing and Maintaining Emergency Operations Plans* provides guidance for developing emergency operations plans. It promotes a common understanding of the fundamentals of risk-informed planning and decision making to help planners examine a hazard or threat and produce integrated, coordinated, and synchronized plans. CPG 101 assists in making the planning process routine across all phases of emergency management and for all homeland security mission areas. It helps planners at all levels in their efforts to develop and maintain viable all-hazards, all-threats Emergency Operations Plans (EOPs). Accomplished properly, planning provides a methodical way to engage the whole community in thinking through the life cycle of a potential crisis, determining required capabilities, and establishing a framework for roles and responsibilities. It shapes how a community envisions and shares a desired outcome, selects effective ways to achieve it, and communicates expected results. Each plan must reflect what that community will do to address its specific risks with the unique resources it has or can obtain.



CPG 101 can be found at:

[https://www.fema.gov/sites/default/files/documents/fema\\_cpg-101-v3-developing-maintaining-eops-checklist.pdf](https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops-checklist.pdf)

### a. The Planning Process

There are many ways to develop an ERP. The planning process that follows is flexible and allows Utilities to adapt it to varying characteristics and situations. The following diagram depicts steps in the planning process, and at each step in the planning process, Utilities should consider the impact of the decisions made on training, exercises, equipment, and other preparedness requirements.





#### **Step 1: Form a Collaborative Planning Team Designated by Organization Leadership**

- The overarching corporation should exercise authority and ownership of the planning process and designate a multi-disciplined planning team for the development of the ERP.
- The process of ERP development should be collaborative and involve entities that may be called on to support the Utility in an emergency. These may include local police, fire department, mass transportation, and cooperating properties in an evacuation.

#### **Step 2: Understand the Situation**

- Go through the process of performing a threats and hazards vulnerability assessment to determine which natural and manmade emergencies the property is vulnerable to, and develop a gap analysis to understand what the property needs to prepare and plan for.
- Annex A has an example of the instructions and an example worksheet to perform a threats and hazards vulnerability assessment. There are many threat and risk assessment tools in the marketplace which may be used to assist in the development of an ERP. The property management should determine which tool is best suited for its particular needs.

#### **Step 3: Determine Goals and Objectives**

- The development of goals and objectives assists planners in the identification of tasks, tactics, and resources necessary to achieve the goal.

#### **Step 4: Plan Development**

- Generate, compare, and select possible solutions for achieving the goals and objectives identified in *Step 3*. Planners consider the requirements, goals, and objectives to develop several response alternatives.
- For each operational task identified, some basic information is needed. Developing this information helps planners incorporate the task into the plan when they are writing it.



- Planners correctly identify an operational task when they can answer the following questions about it:
  - What is the action?
  - Who is responsible for the action?
  - When should the action take place?
  - How long should the action take and how much time is actually available?
  - What has to happen before?
  - What happens after?
  - What resources does the person/entity need to perform the action?

#### **Step 5: Plan Preparation, Review and Approval**

- The planning team writes the plan.
- The plan is then distributed to all the stakeholders and departments that have to implement aspects of the plan for review, comments, and revision.
- And finally, the plan is submitted to Utility leadership for review, approval, and promulgation.

#### **b. Access and Functional Needs Planning Best Practices**

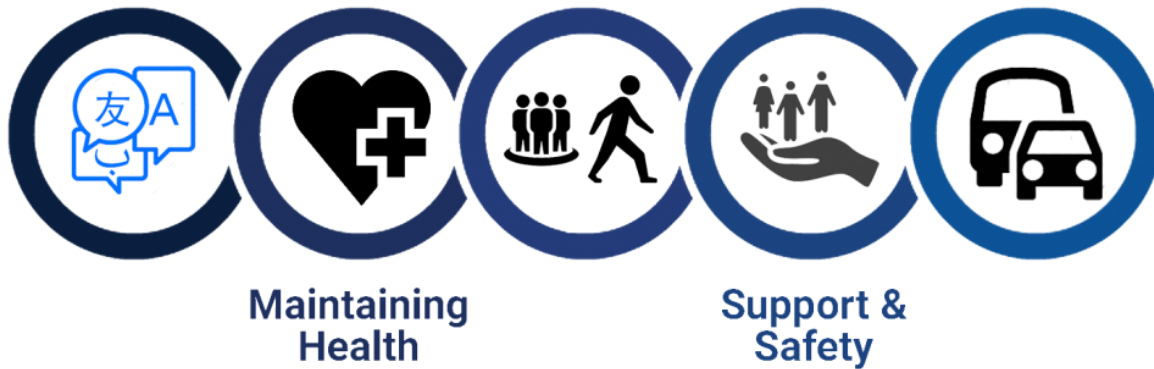
Incorporating the needs of people with access and functional needs into all phases of prevention, mitigation, protection, response, and recovery programs is a best practice based on FEMA's strategic goals of whole community inclusion. Individuals with access and functional needs can be aided to preserve their health, safety, and independence before, during, and after an incident by identifying their needs using the "C-MIST" framework. The C-MIST abbreviation stands for Communication, Maintaining Health, Independence, Safety, Support Services, Self-Determination, and Transportation.

In emergency or crisis situations, individuals are able to preserve their health, safety, and independence when physical and programmatic access, auxiliary aids and services, integration, and efficient communications are provided. Individuals with access and functional needs may have extra needs in one or more of the following functional categories to participate in and benefit from emergency preparedness programs and services.

## Communication

## Independence

## Transportation



### **C = Communication**

Individuals with communication requirements may communicate using American Sign Language (ASL), Limited English Proficiency (LEP), braille print, or other auxiliary aids and technology to communicate or navigate their surroundings. These persons may be unable to hear announcements, see signs, comprehend communications, or articulate their problems.

A disaster or public health emergency may necessitate specific medications, supplies, services, Durable Medical Equipment (DME), electricity for life-sustaining equipment, breastfeeding and infant/childcare, or nutrition to mitigate the negative health effects.

### **M = Maintaining Health**

A disaster or public health emergency may necessitate specific medications, supplies, services, DME, electricity for life-sustaining equipment, breastfeeding and infant/childcare, or nutrition to mitigate the negative health effects. Those at risk who are identified and screened early, and whose functional independence needs are met within the first 48 hours, can avoid costly health deterioration and hospitalization. Maintaining functional independence may necessitate replacement of essential blood pressure medications, seizures, diabetes, psychiatric disorders, lost or damaged teeth, mobility equipment, other assistive devices (wheelchairs, walkers, scooters, and canes), and necessary consumables. It may include individuals who are unable to provide for themselves or who lack adequate resources.

### **I = Independence**

When relocating adults with disabilities to shelters, and medical care settings and when discharging them home or into the community, it is essential to ensure continuity of access to necessary mobility devices or assistive technology, vision and communication aids, and service animals that help the individual maintain independence. Maintaining independence requires that persons are not separated from their mobility devices, assistive technology, service animals, or primary support person.

**S = Support**

Early detection and planning for Access and Functional Needs (AFNs) can lessen the negative effects of a public health emergency on the autonomy and well-being of individuals. Some individuals may have lost caregiver assistance during a hospital stay and require additional support following discharge; others may find it difficult to adapt to a new or unfamiliar environment or have trouble understanding or remembering; and still others may have suffered trauma or be victims of abuse.

**T = Transport**

Individuals may lack access to personal transportation or be unable to operate a motor vehicle due to decreased or impaired mobility caused by age and/or disability, temporary conditions, injury, or legal constraint. In some places, disasters and public health situations can dramatically decrease transportation alternatives, making it difficult to obtain services and remain connected. Coordination with mass transit and accessible transportation service providers is required for disaster preparation.

<b>C-MIST ATTACHMENT TABLE</b>
<b>COMMUNICATIONS:</b>
<i>ACTIONS ITEMS:</i>
SOCIAL MEDIA (Website, Twitter, Facebook, Really Simple Syndication (RSS), etc.)
OTHER MEDIA (T.V., Radio, Flyers, Newspapers, Loudspeakers)
SIGNS (Language other than English, Cartoon, Brail, Low eye site,)
ALERTS (Voice message, Alerts for hearing impaired, Alerts for visually impaired, Alerts for cognitively impaired, foreign language)
DIRECTIONS (Where to go, Where not to go, Traffic, Weather, Screening forms (all forms at POD in language other than English available))
<b>MAINTAINING HEALTH:</b>
<i>ACTION ITEMS:</i>
ITEMS PEOPLE MAY ALREADY HAVE (Syringes, Prescription medications, Glasses, Batteries, OTC medications, Gauze and band aids, BP machine, disposable medical equipment, Caregiver support)
ITEMS PEOPLE MAY NEED (Syringes, Prescription medications, Over the Counter (OTC) medications, Emergency equipment, Saline bags, disposable medical equipment, Caregiver support)
MISCELLANEOUS (Access to medical professionals, Access to medications, Access to sanitation, Access to medical records and information, Gurneys, Surgical suite, Defibrillator, Vital sign equipment)
<b>INDEPENDENCE:</b>
<i>ACTION ITEMS:</i>
ITEMS PEOPLE MAY ALREADY HAVE (Wheelchairs, Walkers, Motorized wheelchairs, Transportation, Internet and computer access, Catheters and other disposable medical equipment, Caregivers)
ITEMS PEOPLE MAY NEED (Wheelchairs, Walkers, Transportation, Catheters, and other disposable medical equipment)
MISCELLANEOUS (Access to facilities that are Americans with Disabilities Act (ADA) compliant, Access to medical professionals, Access to medications, Access to medical information)
<b>SAFETY AND SELF DETERMINATION</b>
<i>ACTION ITEMS:</i>
Family reunification
Access to caregivers
Access to psychiatric services
Access to legal-council and documents
Access to monetary assistance plans
Security and other law enforcement
Access to counseling
<b>TRANSPORTATION</b>
<i>ACTION ITEMS:</i>

Cars
Vans
Busses
Ride sharing services
Light rail
Taxi
Bike
Emergency transportation (ambulance, police cars, fire trucks)
Helicopter
Airplanes
Transportation costs

### c. Community Lifelines

Community Lifelines are the fundamental services that enable the continuous operation of critical government and business functions. They are essential to human health, safety, and economic security. During initial response, a priority needs to be placed on assessing the status of community lifelines for stabilization. An ERP needs to identify community lifelines and specify how they will be restored when a disaster strikes.

The Community Lifelines are as follows:

- **Safety and Security:** Includes law enforcement, fire service, search and rescue, government, and community safety services.
- **Food, Water, and Shelter:** Includes services responsible for providing food, hydration, shelter, and maintaining agriculture during a disaster.
- **Health and Medical:** Includes medical care, public health, patient movement, medical supply chain management, and fatality management services.
- **Energy:** Includes power grid and fuel services.
- **Communications:** Includes infrastructure, responder communications, finance, 911 and dispatch, alerts, warnings, and messages.
- **Transportation:** Includes highway/roadway/motor vehicle, mass transit, railway, aviation, and maritime services.
- **Hazardous Materials:** Includes facilities, hazardous material (HAZMAT) services, and pollutant management and contaminant services.
- **Water Systems:** Includes potable water infrastructure and wastewater management.



#### **d. Utility ERP Format and Contents**

Utility ERPs should be risk-based, flexible, implementable from the bottom up, and understandable from the lowest level. The best plans are action oriented, concise, and emphasize actions to protect visitors and employees.

What follows are two examples of formats that Utilities may consider in developing their ERPs. These examples are intended to give Utilities suggested options for the development of ERPs and are not intended to limit innovation. They are also intended to provide scalable options for Utilities to consider based on their needs.

<b>Rapid Emergency Response Plan</b>
Utility Name Date Approved Date Updated Senior Official Reviewing the Plan Business Address Telephone Fax Email
<ol style="list-style-type: none"><li>1. Loss of Service Procedure</li><li>2. Identified Threat/Hazard Specific (Wind, Cyber, Earthquake, or Other Identified in the vulnerability assessment) Procedure.</li><li>3. Identified Threat/Hazard Specific (Wind, Cyber, Earthquake, or Other Identified in the vulnerability assessment) Procedure.</li><li>4. Identified Threat/Hazard Specific (Wind, Cyber, Earthquake, or Other Identified in the vulnerability assessment) Procedure.</li><li>5. Public Notification Procedure</li><li>6. Points of Contact</li></ol>

<b>Rural Water Format</b>
Cover Page Promulgation Statement Approvals Record of Change Table of Contents
<b>Section 1: System Information</b> A. System Name and Address

- B. Basic Description of the System
- C. Location/Town
- D. Name and Contact Information of the People Responsible for the Plan

## **Section 2: Chain of Command/Lines of Authority**

- A. Name and Title
- B. Responsibilities in an Emergency
- C. Contact Numbers

## **Section 3: Events that Cause Emergencies (Taken from Vulnerability Assessment)**

- A. Types of Events
- B. Probability
- C. Comments

## **Section 4: Notification**

- A. Emergency Notification List
- B. Priority Customers
- C. State, Federal, or Tribal Notifications
- D. Service/Repair Notification
- E. Media Notification
- F. Notification Procedures and Who is Responsible
- G. Contact Service Contractors
- H. Contact Neighboring Systems
- I. Procedure for Issuing Health Advisory
- J. Other Procedures

## **Section 5: Effective Communications**

- A. Public Information Officer Designation
- B. Prepared Messages

## **Section 6: Response Actions for Specific Events**

In any event, there is a series of general steps to take:

- Analyze the type and severity of the emergency
- Take immediate action to save lives
- Take action to reduce injuries and system damage
- Make repairs based on priority demand
- Return the system to normal operation

## **Section 7: Alternative Lifelines Service Source**

## **Section 8: Returning to Normal Operations**

## **Section 9: Plan Approval**

Regardless of the format used, it is recommended that all ERPs include the following:

- A cover page with the date and name of the organization or names of the jurisdiction(s) covered by the plan.
- A letter of promulgation signed by the executive head making the document official.
- Purpose, scope and/or goals and objectives
- Authority
- Table of contents
- Situation and assumptions
- Functional roles and responsibilities
- Logistics support and resource requirements necessary to implement the plan
- Concept of operations
- Plan maintenance
- A drawing or map of the layout and boundaries of the utility
- A drawing or description of any approved routes for evacuation
- The location and inventory of the utility's emergency response equipment and resources
- The location of any unusually hazardous substances within the utility
- Plans for the continuity of the operations and services of the utility
- Any other information that the utility may determine to be relevant

Utility ERPs in Nevada shall also identify and assign specific areas of responsibility for performing essential functions in response to an emergency or disaster. Areas of responsibility to be addressed include:

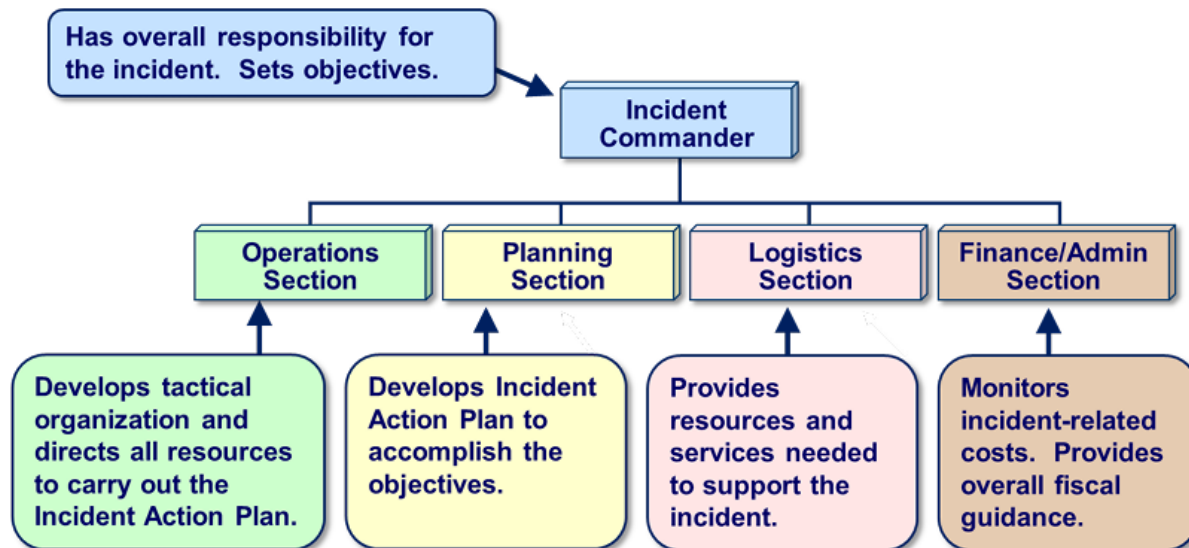
- Direction/control and coordination
- Information and planning
- Detection and monitoring
- Alert and notification
- Warning
- Communications
- Emergency public information
- Resource management
- Evacuation



- Needs and damage assessment
- Hazardous materials
- Priority populations
- Fatality and mortuary services

## VIII. Organization Guidance and Best Practices

It is recommended by OEM, but **not** required by NRS 239C.270, that the Utility adopts the National Incident Management System (NIMS) to organize an Incident Management Team (IMT) which is a rostered group of personnel trained in the Incident Command System (ICS) in which the organization of the IMT consists of an Incident Commander, Command and General Staff, and personnel assigned to ICS leadership positions. The IMT provides on-scene incident management and integrates a combination of facilities, equipment, personnel, procedures, and communications of different business units within the organization under one common organizational structure.



Adoption of the NIMS and the ICS would enhance the Utility's capability to collaborate and coordinate during response operations with all levels of government, nongovernmental organizations, and other private sector partners through use of shared vocabulary, systems, and processes. Simply stated, the NIMS defines the vocabulary, systems, and processes that guide all whole community stakeholders through working together during incidents.

The benefits to adopting NIMS include:

- A standardized approach that is scalable and flexible.
- Enhanced cooperation and interoperability among responders from different agencies, organizations, and jurisdictions.
- Comprehensive all-hazards preparedness.

- Efficient resource coordination among different agencies, organizations, and jurisdictions.
- Integration of best practices and lessons learned for continuous improvement across different agencies, organizations, and jurisdictions.

Furthermore, the OEM recommends, though it is **not** required by NRS 239C.270, that Utilities establish and staff an Emergency Operations Center (EOC). An EOC is not an on-scene incident command post (ICP) - where the IMT convenes to focus on tactics to deal with the immediate situation. An EOC is used to support on-scene tactics through the prioritization of activities and the allocation of available resources. A major function within the EOC is communications between the IMT, business continuity team, crisis communications team and company management.

An EOC differs from on-scene incident management by performing the following functions:

- **Situation Analysis** – Gathering information to determine what is happening and to identify potential impacts to the business.
- **Incident Briefing** – Efficiently share information among IMT, business continuity team, crisis communications team, and company management.
- **Incident Strategic Planning** – Provide a single point for executive-level decision-making to decide on a course of action for the current situation.
- **Resource Management** – Provide a single point of contact to identify, procure and allocate resources to sustain business continuity, facilitate crisis communications, and support on-scene incident management.
- **Support Incident Management** – Monitor team actions, capture event data and discuss adjustment of strategies at the executive-level as needed.

Ready.gov provides additional guidance and tools for private sector NIMS and ICS adoption, and EOC staff activities which can be found at <https://www.ready.gov/incident-management>.

Additionally, the *National Incident Management System Emergency Operations Center How-To Quick Reference Guide August 2021* provides organizational considerations for private-sector EOCs and the guide can be accessed at

[https://www.fema.gov/sites/default/files/documents/fema\\_eoc-quick-reference\\_guide.pdf](https://www.fema.gov/sites/default/files/documents/fema_eoc-quick-reference_guide.pdf).

## IX. Equipment Guidance and Best Practices

It is recommended by OEM, however not required by NRS 239C.270, that Utilities have equipment and supplies available to handle the needs of emergency response operations. It is recommended that IMT and EOC staff members build an individual “go kit” which includes an ICS/EOC position job aid, initial response guidebook, planning forms and worksheets, ICS/EOC position vest/badge, writing utensils and paper, communications device (e.g., radio, phone, laptop, etc.), and other supplies and equipment that would make the IMT/EOC member successful in carrying out their ICS/EOC role. A conference room or other large space can be designated as an EOC that should be equipped with the following equipment and supplies:

- Communications equipment including sufficient telephones (cell and landline with at least one speakerphone) to handle incoming and outgoing calls; incoming and outgoing fax machines; and access to any radio systems used by the business.
- Computers and printers with access to network resources (including electronic copies of emergency response, business continuity and crisis communications plans that can be printed on demand), electronic mail and the internet.
- Information gathering and display tools including access to broadcast radio and television (preferably with recording capability) or internet news sources; white boards, TV monitors, projection units or flipcharts with easel and markers to compile and display information.
- Hard copies of emergency response, business continuity and crisis communications plans, contact/telephone lists, resource inventory and diagrams of facilities and systems.
- Stationery, business and incident management forms, pens, pencils, markers, and supplies.
- Food, water, and dining supplies for EOC staff.

A “grab and go package” is a best practice used by many Utilities in Nevada. This package contains specific information for police, fire, and other first responders about the property which will give the first responder information and tools unique to the property to expedite response. The property should determine how many “Grab and Go Packages” it needs for an adequate first responder response and store them in strategic locations. The use of the “Grab and Go Package” is a recommendation by OEM for Utilities to use, however its use is **not** mandated by NRS 239C.270.

### Recommended “Grab and Go” Kit Contents

First Aid Kit including: <ul style="list-style-type: none"> <li>• Tourniquets</li> <li>• Compression bandages</li> <li>• Rolled Gauze</li> <li>• Assorted dressings</li> <li>• Gloves</li> <li>• Chest Seals</li> <li>• Trauma Tape</li> <li>• Trauma shears</li> </ul>	Doorstops	Glow sticks	Location of access and functional needs rooms
	Evacuation plans with maps of egress and muster stations	Laminated property maps with all exits clearly marked, and a dry erase marker	Radio with property frequencies attached and extra batteries
	Exclusion tape	Location and keys to elevators	Roster of key utility staff and contact numbers
	Flashlight with extra batteries	Location of fire suppression system controls, fire hydrants, and HVAC systems	Set of master keys

## X. Training and Exercise Guidance and Best Practices

Achieving preparedness at its core is implementing an emergency response plan, training to the plan, and then exercising the plan to reinforce best practices and identify areas to improve upon the plan. Organizations cannot claim to have an emergency preparedness capability until the plan is trained and tested by a realistic series of exercises. The OEM highly recommends, though it is not required by NRS 239C.270, that all Utility staff members undergo annual training on their role within the Utility ERP. Ensuring that training is offered to all Utility staff members on a regular and consistent basis will enhance everyone’s capability to recognize what to do when there is an emergency, crisis, or disruption to the business.

Recommendation for who needs training	Recommendation for what training should be provided
All employees	<ul style="list-style-type: none"> <li>Protective actions for life safety (evacuation, shelter, shelter-in-place, lockdown)</li> <li>Safety, security, and loss prevention programs</li> </ul>
Incident Management Team (emergency response, evacuation, shelter, shelter-in-place)	<ul style="list-style-type: none"> <li>Roles and responsibilities as defined in the plan</li> <li>Training as required to comply with regulations or maintain certifications (if employees administer first aid, CPR or AED or use fire extinguishers or clean up spills of hazardous chemicals)</li> <li>Additional training for leaders including incident management</li> </ul>
Business Continuity Team	<ul style="list-style-type: none"> <li>Roles and responsibilities as defined in the plan</li> <li>Additional training for leaders including incident management</li> </ul>
Crisis Communications Team	<ul style="list-style-type: none"> <li>Roles and responsibilities as defined in the plan</li> <li>Additional training for leaders including incident management</li> <li>Training for spokespersons</li> </ul>

It is recommended by OEM but **not** required by NRS 239C.270, that Utilities utilize the HSEEP methodology to develop increasingly complex realistic exercises. It is recommended that Utilities perform an internal exercise each year. It is also recommended that Utilities participate in full scale exercises offered by the emergency management organization in the city/county the Utility is located in.



For each exercise, it is recommended by OEM but **not** required by NRS 239C.270, the Utility should develop an After-Action Report (AAR) and Improvement Plan (IP) to detail lessons learned from the exercise. The AAR/IP should include recommendations from lessons learned to revise the ERP, develop training programs, order equipment, or develop agreements outside the Utility.

FEMA has dedicated an entire preparedness toolkit (PrepToolkit) to HSEEP. The HSEEP PrepToolkit includes policy and program management guidance, documentation templates, and starter kits which can be adopted and adapted

by any organization to accomplish the Exercise POETE area of the Integrated Preparedness Cycle. The HSEEP PrepToolkit can be found at <https://preptoolkit.fema.gov/web/hseep-resources/about>.

## XI. Utility ERP NRS Review and Submission Requirements

### NRS 239C.270

2. Each utility shall:
  - a. As soon as practicable but not later than December 31, 2003, submit its vulnerability assessment and emergency response plan to the Office of Emergency Management of the Department of Public Safety; and
  - b. At least once each year thereafter, review its vulnerability assessment and emergency response plan and, as soon as practicable after its review is completed but not later than December 31 of each year, submit the results of its review and any additions or modifications to its emergency response plan to the Office.

### Submission Requirements:

In accordance with NRS 239C.270 as amended by SB69, each utility must review its response plan at least once per year and no later than December 31 of each year submit its newly revised plan to the Office of Emergency Management. Should the ERP and VA not require any update, each utility can submit a ERP/VA Certificate of Review instead of the full plan. **This Certificate of Review can be found in Annex A.** Otherwise, a plan can be submitted in the following ways:

**Mail to:** Office of Emergency Management  
2478 Fairview Drive  
Carson City, NV 89701

**Or submit via the OEM's online plan portal. For access, please email the following:**  
[OEMplanning@dem.nv.gov](mailto:OEMplanning@dem.nv.gov), [sgrennan@dem.nv.gov](mailto:sgrennan@dem.nv.gov), [rgraves@dem.nv.gov](mailto:rgraves@dem.nv.gov)

**As of 2024, the OEM plan portal will require a passcode before a plan submission can be made. Once you email the above-listed addresses, the access code will be sent to you.**

## XII. Conclusion

Having a well-conceived ERP, which is trained upon and rigorously tested, can save lives, and protect property. These plans are currently required by law and are explored within this document. Once developed, they should also serve to facilitate opportunities for collaboration and coordination between private entities and public safety organizations.

We encourage you to work with your local law enforcement, fire/emergency medical services, emergency manager, and public health preparedness agencies to increase resilience. These groups commonly meet in a local emergency planning committee (LEPC) which encourages business participation.

### **XIII. Acronyms**

<b>AFN</b>	Access and Functional Need
<b>AAR/IP</b>	After Action Report/Improvement Plan
<b>ASL</b>	American Sign Language
<b>ADA</b>	Americans with Disabilities Act
<b>C-MIST</b>	Communication, Maintaining Health, Independence, Safety, Support Services, Self-Determination, and Transportation
<b>CPG</b>	Comprehensive Planning Guide
<b>OEM</b>	Office of Emergency Management
<b>DME</b>	Durable Medical Equipment
<b>EOC</b>	Emergency Operations Center
<b>EOP</b>	Emergency Operations Plan
<b>ERP</b>	Emergency Response Plan
<b>FEMA</b>	Federal Emergency Management Agency
<b>FEMA</b>	Federal Emergency Management Agency
<b>HSEEP</b>	Homeland Security Exercise and Evaluation Program
<b>ICP</b>	Incident Command Post
<b>ICS</b>	Incident Command System
<b>IMT</b>	Incident Management Team

<b>IPP</b>	Integrated Preparedness Plan
<b>LEP</b>	Limited English Proficiency
<b>LEPC</b>	Local Emergency Planning Committee
<b>MEF</b>	Mission Essential Functions
<b>NIMS</b>	National Incident Management System
<b>NRS</b>	Nevada Revised Statutes
<b>OTC</b>	Over the Counter
<b>POETE</b>	Planning, Organization, Equipment, Training, and Exercises
<b>RSS</b>	Really Simple Syndication
<b>SPR</b>	Stakeholder Preparedness Review
<b>SEMP</b>	State Comprehensive Emergency Management Plan
<b>THIRA</b>	Threat and Hazard Identification and Risk Assessment



## **ANNEX A: Utilities ERP/VA Certificate of Review**



**NRS 239C.270 Utilities**  
**Emergency Plan Response Plan (ERP) /**  
**Vulnerability Assessment (VA)**  
**Certificate of Review**

Nevada Office of Emergency Management / Homeland Security  
 2478 Fairview Drive  
 Carson City, Nevada 89701  
 775.687.0300

**Select Utility Type:** Water System/GID ☐      Clean Water Only ☐      Wastewater/Sewer Only ☐  
 Natural Gas ☐      Electric ☐

Utility/Entity Name:			
Preparer's Name			
Business Address:			
City, State, Zip:			
Phone Number:		Email:	

Year of Emergency Response Plan (ERP): \_\_\_\_\_

Date ERP was reviewed: \_\_\_\_\_

Expected Year for ERP Revision (if available): \_\_\_\_\_

Year of most recent Vulnerability Assessment (VA): \_\_\_\_\_

Date VA was reviewed: \_\_\_\_\_

*By signing this certificate of review, the preparer acknowledges according to NRS 239C.270 § 2(b) that an annual review of the utility's emergency response plan and vulnerability assessment have been conducted and no additions or modifications to the emergency response plan are necessary.*

\_\_\_\_\_  
 Signature of Preparer

\_\_\_\_\_  
 Date

This page is intentionally blank.

## Annex B: Vulnerability Assessment Templates

### Vulnerability Assessment Template #1

Utility Name:				Date Performed:		
<b>Business Impact Analysis Worksheet: Threat and Hazard Analysis</b>						
Entry Number	Threat/Hazard	Threat/Hazard Characteristics	Threat/Hazard Likelihood (0-10)	MEF Vulnerability (0-10)	MEF Failure Impact (0-10)	MEF Risk Value (0-30)
1	Earthquake					
2	Flood					
3	Wildfire					
4	Severe Winter Storm					
5	Active Assailant					
06	Cyber Attack					

## **Mitigation Plan**

- 1. Hazard 1:**
- 2. Hazard 2:**
- 3. Hazard 3**

This page is intentionally blank.

# Security Vulnerability Self-Assessment Guide for Small Water Systems

### ***Introduction***

Water systems are critical to every community. Protection of public drinking water systems must be a high priority for local officials and water system owners and operators to ensure an uninterrupted water supply, which is essential for the protection of public health (safe drinking water and sanitation) and safety (fire fighting).

Adequate security measures will help prevent loss of service through terrorist acts, vandalism, or pranks. If your system is prepared, such actions may even be prevented. The appropriate level of security is best determined by the water system at the local level.

This Security Vulnerability Self-Assessment Guide is designed to help small water systems determine possible vulnerable components and identify security measures that should be considered. A “vulnerability assessment” is the identification of weaknesses in water system security, focusing on defined threats that could compromise its ability to provide adequate potable water, and/or water for firefighting. This document is designed particularly for systems that serve populations of 3,300 or less. This document is meant to encourage smaller systems to review their system vulnerabilities, but it may not take the place of a comprehensive review by security experts.

The Self-Assessment Guide has a simple design. Answers to assessment questions are “yes” or “no,” and there is space to identify needed actions and actions you have taken to improve security. For any “no” answer, refer to the “comment” column and/or contact your state drinking water primacy agency.

### ***How to Use this Self-Assessment Guide***

This document is designed for use by water system personnel. Physical facilities pose a high degree of exposure to any security threat. This self-assessment should be conducted on all components of your system (wellhead or surface water intake, treatment plant, storage tank(s), pumps, distribution system, and other important components of your system).

The Assessment includes an emergency contact list for your use. This list will help you identify who you need to contact in the event of an emergency or threat and will help you develop communication and outreach procedures. Filling out the Emergency Contact List is an important step toward developing an Emergency Response Plan, which provides detailed procedures on how to respond to an emergency.

You may be able to obtain sample Emergency Response Plans from your state

drinking water primacy agency.

Security is everyone's responsibility. We hope this document helps you to increase the awareness of all your employees, governing officials, and customers about security issues.

Once you have completed this document, review the actions you need to take to improve your system's security. Make sure to prioritize your actions based on the most likely threats. Please complete the Certificate of Completion on page 27 and return only the certificate to your state drinking water primacy agency. Do not include a full copy of your self-assessment.

### ***Keep this Document***

This is a working document. Its purpose is to start your process of security vulnerability assessment and security enhancements. Security is not an end point, but a goal that can be achieved only through continued efforts to assess and upgrade your system.

Don't forget that this is a sensitive document. It should be stored separately in a secure place at your water system. A duplicate copy should also be retained at a secure off-site location.

Access to this document should be limited to key water system personnel and local officials as well as the state drinking water primacy agency and others on a need-to-know basis.



# Security Vulnerability Self-Assessment

## *Record of Security Vulnerability Self-Assessment Completion*

*The following information should be completed by the individual conducting the self-assessment and/or any additional revisions.*

**Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Area of Responsibility:** \_\_\_\_\_

**Water System**

**Name:** \_\_\_\_\_

**Water System**

**PWSID:** \_\_\_\_\_

**Address:** \_\_\_\_\_

**City:** \_\_\_\_\_

**County:** \_\_\_\_\_

**State:** \_\_\_\_\_

**Zip Code:** \_\_\_\_\_

**Telephone:** \_\_\_\_\_

**Fax:** \_\_\_\_\_

**E-mail:** \_\_\_\_\_

**Date Completed:** \_\_\_\_\_

**Date Revised:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Date Revised:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

### ***Inventory of Small Water System Critical Components***

Component	Number & Location (if applicable)	Description
<b>Source Water Type</b>		
Ground Water		
Surface Water		
Purchased		
<b>Treatment Plant</b>		
Buildings		
Pumps		
Treatment Equipment (e.g., basin, clearwell, filter)		
Process Controls		
Treatment Chemicals and Storage		
Laboratory Chemicals and Storage		
<b>Storage</b>		
Storage Tanks		
Pressure Tanks		
<b>Power</b>		
Primary Power		
Auxiliary Power		
<b>Distribution System</b>		
Pumps		
Pipes		
Valves		
Appurtenances (e.g., flush hydrants, backflow preventers, meters)		
Other Vulnerable Points		
<b>Offices</b>		
Buildings		
Computers		
Files		
Transportation/ Work Vehicles		
<b>Communications</b>		
Telephone		
Cell Phone		
Radio		
Computer Control Systems (SCADA)		













# Security Vulnerability Self-Assessment for Small Water Systems

## **General Questions for the Entire Water System**

*The first 13 questions in this vulnerability self-assessment are general questions designed to apply to all components of your system (wellhead or surface water intake, treatment plant, storage tank(s), pumps, distribution system, and offices). These are followed by more specific questions that look at individual system components in greater detail.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
1. Do you have a written emergency response plan (ERP)?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>It is essential that you have an ERP. If you do not have an ERP, you can obtain a sample from your state drinking water primacy agency. As a first step in developing your ERP, you should develop your Emergency Contact List (see Attachment 2).</p> <p>A plan is vital in case there is an incident that requires immediate response. Your plan should be reviewed at least annually (or more frequently if necessary) to ensure it is up-to-date and addresses security emergencies.</p> <p>You should designate someone to be contacted in case of emergency regardless of the day of the week or time of day. This contact information should be kept up-to-date and made available to all water system personnel and local officials (if applicable).</p> <p>Share this ERP with police, emergency personnel, and your state primacy agency. Posting contact information is a good idea only if authorized personnel are the only ones seeing the information. These signs could pose a security risk if posted for public viewing since it gives people information that could be used against the system.</p>	
2. Is access to the critical components of the water system (i.e., a part of the physical infrastructure of the system that is essential for water flow and/or water quality) restricted to authorized personnel only?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>You should restrict or limit access to the critical components of your water system to authorized personnel only. This is the first step in security enhancement for your water system. Consider the following:</p> <ul style="list-style-type: none"> <li>◆ Issue water system photo identification cards for employees, and require them to be displayed within the restricted area at all times.</li> <li>◆ Post signs restricting entry to authorized personnel and ensure that assigned staff escort people without proper ID.</li> </ul>	

3. Are facilities fenced, including wellhouses and pump pits, and are gates locked where appropriate?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Ideally, all facilities should have a security fence around the perimeter.</p> <p>The fence perimeter should be walked periodically to check for breaches and maintenance needs. All gates should be locked with chains and a tamper- proof padlock that at a minimum protects the shank. Other barriers such as concrete "jersey" barriers should be considered to guard certain critical components from accidental or intentional vehicle intrusion.</p>	
4. Are your doors, windows, and other points of entry such as tank and roof hatches and vents kept closed and locked?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Lock all building doors and windows, hatches and vents, gates, and other points of entry to prevent access by unauthorized personnel. Check locks regularly. Dead bolt locks and lock guards provide a high level of security for the cost.</p> <p>A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place.</p> <p>Doors and hinges to critical facilities should be constructed of heavy- duty reinforced material. Hinges on all outside doors should be located on the inside.</p> <p>To limit access to water systems, all windows should be locked and reinforced with wire mesh or iron bars, and bolted on the inside. Systems should ensure that this type of security meets with the requirements of any fire codes. Alarms can also be installed on windows, doors, and other points of entry.</p>	
5. Is there external lighting around the critical components of your water system?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Adequate lighting of the exterior of water systems' critical components is a good deterrent to unauthorized access and may result in the detection or deterrence of trespassers. Motion detectors that activate switches that turn lights on or trigger alarms also enhance security.	
6. Are warning signs (tampering, unauthorized access, etc.) posted on all critical components of your water system? (For example, well houses and storage tanks.)	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Warning signs are an effective means to deter unauthorized access.</p> <p>"Warning - Tampering with this facility is a federal offense" should be posted on all water facilities. These are available from your state rural water association.</p> <p>"Authorized Personnel Only," "Unauthorized Access Prohibited," and "Employees Only" are examples of other signs that may be useful.</p>	
7. Do you patrol and inspect your source intake, buildings, storage tanks, equipment, and other critical components?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Frequent and random patrolling of the water system by utility staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol.</p> <p>Consider asking your local law enforcement agencies to conduct patrols of your water system. Advise them of your critical components and explain why they are important.</p>	

8. Is the area around the critical components of your water system free of objects that may be used for breaking and entering?	Yes  No 	When assessing the area around your water system's critical components, look for objects that could be used to gain entry (e.g., large rocks, cement blocks, pieces of wood, ladders, valve keys, and other tools).	
9. Are the entry points to your water system easily seen?	Yes  No 	<p>You should clear fence lines of all vegetation. Overhanging or nearby trees may also provide easy access. Avoid landscaping that will permit trespassers to hide or conduct unnoticed suspicious activities.</p> <p>Trim trees and shrubs to enhance the visibility of your water system's critical components.</p> <p>If possible, park vehicles and equipment in places where they do not block the view of your water system's critical components.</p>	
10. Do you have an alarm system that will detect unauthorized entry or attempted entry at critical components?	Yes  No 	<p>Consider installing an alarm system that notifies the proper authorities or your water system's designated contact for emergencies when there has been a breach of security. Inexpensive systems are available. An alarm system should be considered whenever possible for tanks, pump houses, and treatment facilities.</p> <p>You should also have an audible alarm at the site as a deterrent and to notify neighbors of a potential threat.</p>	
11. Do you have a key control and accountability policy?	Yes  No 	<p>Keep a record of locks and associated keys, and to whom the keys have been assigned. This record will facilitate lock replacement and key management (e.g., after employee turnover or loss of keys).</p> <p>Vehicle and building keys should be kept in a lockbox when not in use.</p> <p>You should have all keys stamped (engraved) "DO NOT DUPLICATE."</p>	
12. Are entry codes and keys limited to water system personnel only?	Yes  No 	Suppliers and personnel from co-located organizations (e.g., organizations using your facility for telecommunications) should be denied access to codes and/or keys. Codes should be changed frequently if possible. Entry into any building should always be under the direct control of water system personnel.	
13. Do you have a neighborhood watch program for your water system?	Yes  No 	Watchful neighbors can be very helpful to a security program. Make sure they know whom to call in the event of an emergency or suspicious activity.	

### *Water Sources*









*In addition to the above general checklist for your entire water system (questions 1-13), you should give special attention to the following issues, presented in separate tables, related to various water system components. Your water sources (surface water intakes or wells) should be secured. Surface water supplies present the greatest challenge. Typically they encompass large land areas. Where areas cannot be secured, steps should be taken to initiate or increase law enforcement patrols. Pay particular attention to surface water intakes. Ask the public to be vigilant and report suspicious activity.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
14. Are your wellheads sealed properly?	Yes <input type="checkbox"/> No <input type="checkbox"/>	A properly sealed wellhead decreases the opportunity for the introduction of contaminants. If you are not sure whether your wellhead is properly sealed, contact your well drilling/maintenance company, your state drinking water primacy agency, your state rural water association, or other technical assistance providers.	
15. Are well vents and caps screened and securely attached?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Properly installed vents and caps can help prevent the introduction of a contaminant into the water supply.  Ensure that vents and caps serve their purpose, and cannot be easily breached or removed.	
16. Are observation/test and abandoned wells properly secured to prevent tampering?	Yes <input type="checkbox"/> No <input type="checkbox"/>	All observation/test and abandoned wells should be properly capped or secured to prevent the introduction of contaminants into the aquifer or water supply. Abandoned wells should be either removed or filled with concrete.	
17. Is your surface water source secured with fences or gates? Do water system personnel visit the source?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Surface water supplies present the greatest challenge to secure. Often, they encompass large land areas. Where areas cannot be secured, steps should be taken to initiate or increase patrols by water utility personnel and law enforcement agents.	

### *Treatment Plant and Suppliers*

*Some small systems provide easy access to their water system for suppliers of equipment, chemicals, and other materials for the convenience of both parties. This practice should be discontinued.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
18. Are deliveries of chemicals and other supplies made in the presence of water system personnel?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Establish a policy that an authorized person, designated by the water system, must accompany all deliveries. Verify the credentials of all drivers. This prevents unauthorized personnel from having access to the water system.	

19. Have you discussed with your supplier(s) procedures to ensure the security of their products?	Yes  No 	<p>Verify that your suppliers take precautions to ensure that their products are not contaminated. Chain of custody procedures for delivery of chemicals should be reviewed. You should inspect chemicals and other supplies at the time of delivery to verify they are sealed and in unopened containers. Match all delivered goods with purchase orders to ensure that they were, in fact, ordered by your water system.</p> <p>You should keep a log or journal of deliveries. It should include the driver's name (taken from the driver's photo I.D.), date, time, material delivered, and the supplier's name.</p>	
20. Are chemicals, particularly those that are potentially hazardous or flammable, properly stored in a secure area?	Yes  No 	<p>All chemicals should be stored in an area designated for their storage only, and the area should be secure and access to the area restricted. Access to chemical storage should be available only to authorized employees. You should have tools and equipment on site (such as a fire extinguisher, drysweep, etc.) to take immediate actions when responding to an emergency.</p>	
21. Do you monitor raw and treated water so that you can detect changes in water quality?	Yes  No 	<p>Monitoring of raw and treated water can establish a baseline that may allow you to know if there has been a contamination incident.</p> <p>Some parameters for raw water include pH, turbidity, total and fecal coliform, total organic carbon, specific conductivity, ultraviolet adsorption, color, and odor.</p> <p>Routine parameters for finished water and distribution systems include free and total chlorine residual, heterotrophic plate count (HPC), total and fecal coliform, pH, specific conductivity, color, taste, odor, and system pressure.</p> <p>Chlorine demand patterns can help you identify potential problems with your water. A sudden change in demand may be a good indicator of contamination in your system.</p> <p>For those systems that use chlorine, absence of a chlorine residual may indicate possible contamination. Chlorine residuals provide protection against bacterial and viral contamination that may enter the water supply.</p>	
22. Are tank ladders, access hatches, and entry points secured?	Yes  No 	<p>The use of tamper-proof padlocks at entry points (hatches, vents, and ladder enclosures) will reduce the potential for unauthorized entry.</p> <p>If you have towers, consider putting physical barriers on the legs to prevent unauthorized climbing.</p>	

23. Are vents and overflow pipes properly protected with screens and/or grates?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Air vents and overflow pipes are direct conduits to the finished water in storage facilities. Secure all vents and overflow pipes with heavy-duty screens and/or grates.	
24. Can you isolate the storage tank from the rest of the system?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>A water system should be able to take its storage tank(s) out of operation or drain its storage tank(s) if there is a contamination problem or structural damage.</p> <p>Install shut-off or bypass valves to allow you to isolate the storage tank in the case of a contamination problem or structural damage.</p> <p>Consider installing a sampling tap on the storage tank outlet to test water in the tank for possible contamination.</p>	

### *Distribution*

*Hydrants are highly visible and convenient entry points into the distribution system. Maintaining and monitoring positive pressure in your system is important to provide fire protection and prevent introduction of contaminants.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
25. Do you control the use of hydrants and valves?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Your water system should have a policy that regulates the authorized use of hydrants for purposes other than fire protection. Require authorization and backflow devices if a hydrant is used for any purpose other than fire fighting.</p> <p>Consider designating specific hydrants for use as filling station(s) with proper backflow prevention (e.g., to meet the needs of construction firms). Then, notify local law enforcement officials and the public that these are the only sites designated for this use.</p> <p>Flush hydrants should be kept locked to prevent contaminants from being introduced into the distribution system, and to prevent improper use.</p>	
26. Does your system monitor for, and maintain, positive pressure?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Positive pressure is essential for fire fighting and for preventing back siphonage that may contaminate finished water in the distribution system. Refer to your state primacy agency for minimum drinking water pressure requirements.	
27. Has your system implemented a backflow prevention program?	Yes <input type="checkbox"/> No <input type="checkbox"/>	In addition to maintaining positive pressure, backflow prevention programs provide an added margin of safety by helping to prevent the intentional introduction of contaminants. If you need information on backflow prevention programs, contact your state drinking water primacy agency.	



## Personnel

*You should add security procedures to your personnel policies.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
28. When hiring personnel, do you request that local police perform a criminal background check, and do you verify employment eligibility (as required by the Immigration and Naturalization Service, Form I-9)?	Yes <input type="checkbox"/> No <input type="checkbox"/>	It is good practice to have all job candidates fill out an employment application. You should verify professional references. Background checks conducted during the hiring process may prevent potential employee-related security issues.  If you use contract personnel, check on the personnel practices of all providers to ensure that their hiring practices are consistent with good security practices.	
29. Are your personnel issued photo-identification cards?	Yes <input type="checkbox"/> No <input type="checkbox"/>	For positive identification, all personnel should be issued water system photo-identification cards and be required to display them at all times. Photo identification will also facilitate identification of authorized water system personnel in the event of an emergency.	
30. When terminating employment, do you require employees to turn in photo IDs, keys, access codes, and other security-related items?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Former or disgruntled employees have knowledge about the operation of your water system and could have both the intent and physical capability to harm your system. Requiring employees who will no longer be working at your water system to turn in their IDs, keys, and access codes helps limit these types of security breaches.	
31. Do you use uniforms and vehicles with your water system name prominently displayed?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Requiring personnel to wear uniforms and requiring that all vehicles prominently display the water system name, helps inform the public when water system staff is working on the system. Any observed activity by personnel without uniforms should be regarded as suspicious. The public should be encouraged to report suspicious activity to law enforcement authorities.	
32. Have water system personnel been advised to report security vulnerability concerns and to report suspicious activity?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Your personnel should be trained and knowledgeable about security issues at your facility, what to look for, and how to report any suspicious events or activity.  Periodic meetings of authorized personnel should be held to discuss security issues.	
33. Do your personnel have a checklist to use for threats or suspicious calls or to report suspicious activity?	Yes <input type="checkbox"/> No <input type="checkbox"/>	To properly document suspicious or threatening phone calls or reports of suspicious activity, a simple checklist can be used to record and report all pertinent information. Calls should be reported immediately to appropriate law enforcement officials. Checklists should be available at every telephone. Sample checklists are included in Attachment 3.  Also consider installing caller ID on your telephone system to keep a record of incoming calls.	

### *Information storage/computers/controls/maps*

*Security of the system, including computerized controls like a Supervisory Control and Data Acquisition (SCADA) system, goes beyond the physical aspects of operation. It also includes records and critical information that could be used by someone planning to disrupt or contaminate your water system.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
34. Is computer access “password protected?” Is virus protection installed and software upgraded regularly and are your virus definitions updated at least daily? Do you have Internet firewall software installed on your computer? Do you have a plan to back up your computers?	Yes <input type="checkbox"/> No <input type="checkbox"/>	All computer access should be password protected. Passwords should be changed every 90 days and (as needed) following employee turnover. When possible, each individual should have a unique password that they do not share with others. If you have Internet access, a firewall protection program should be installed on your computer. Also consider contacting a virus protection company and subscribing to a virus update program to protect your records. Backing up computers regularly will help prevent the loss of data in the event that your computer is damaged or breaks. Backup copies of computer data should be made routinely and stored at a secure off-site location.	
35. Is there information on the Web that can be used to disrupt your system or contaminate your water?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Posting detailed information about your water system on a Web site may make the system more vulnerable to attack. Web sites should be examined to determine whether they contain critical information that should be removed.  You should do a Web search (using a search engine such as Google, Yahoo!, or Lycos) using key words related to your water supply to find any published data on the Web that is easily accessible by someone who may want to damage your water supply.	
36. Are maps, records, and other information stored in a secure location?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only.  You should make back-up copies of all data and sensitive documents. These should be stored in a secure off-site location on a regular basis.	
37. Are copies of records, maps, and other sensitive information labeled confidential, and are all copies controlled and returned to the water system?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Sensitive documents (e.g., schematics, maps, and plans and specifications) distributed for construction projects or other uses should be recorded and recovered after use. You should discuss measures to safeguard your documents with bidders for new projects.	
38. Are vehicles locked and secured at all times?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Vehicles are essential to any water system. They typically contain maps and other information about the operation of the water system. Water system personnel should exercise caution to ensure that this information is secure. Water system vehicles should be locked when they are not in use or left unattended. Remove any critical information about the system before parking vehicles for the night. Vehicles also usually contain tools (e.g., valve wrenches) that could be used to access critical components of your water system. These tools should be secured and accounted for daily.	

## Attachment 1. Prioritization of Needed Actions

Once you have completed the “Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems,” review the actions you need to take to improve your system’s security. Note the questions to which you answered “no” on this worksheet. You can use it to summarize the areas where your system has vulnerability concerns. It can also help you prioritize the actions you should take to protect your system from vulnerabilities. Make sure to prioritize your actions based on the most likely threats to your water system.

Question Number	Needed Action	Scheduled Completion

## Attachment 2. Emergency Contact List

We urge all public water systems to adopt an emergency response plan (ERP). Emergency plans are action steps to follow if a primary source of drinking water becomes contaminated or if the flow of water is disrupted. You can obtain sample ERPs from your state drinking water administrator, or from your state primacy agency.

This sample document is an “Emergency Contact List.” It is an essential part of your ERP. It contains the names and telephone numbers of people you might need to call in the event of an emergency. This is a critical document to have at your disposal at all times. It gives you a quick reference to all names and telephone numbers that you need for support in the case of an emergency.

Filling out this Emergency Contact List reminds you to think about all of the people you might need to contact in an emergency. It also may encourage you to talk with these people about what you and they would do if an emergency were to occur.

### ***Section 1. System Identification***

Public Water System (PWS) ID Number		
System Name		
Town/City		
Telephone Numbers	System Telephone	Evening/Weekend Telephone
Other Contact Information	System Fax	Email
Population Served and Number of Service Connections	People Served	Connections
System Owner (The owner must be listed as a person's name)		
Name, title, and telephone number of person responsible for maintaining this emergency contact list	Name and title	Telephone

## ***Section 2. Notification/Contact Information***

### **Local Notification List**

<b>ORGANIZATION</b>	<b>CONTACT NAME/TITLE</b>	<b>TELEPHONE (DAY)</b>	<b>TELEPHONE (NIGHT)</b>	<b>EMAIL</b>
Fire Department				
Police Department				
FBI Field Office				
Health Department				
Primacy Agency District Office				
Local Hospital				
Local Emergency Planning Committee				
EMS				
Local Pharmacy				
Local Nursing Homes				
Local Schools				
Local Prisons				
Local Government Official				
Local Hazmat Team				
Water System Operator				
Neighboring Water System				
Neighboring Water System				
Other				

## Service/Repair Notification List

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Electrician				
Electric Utility Company				
Gas Utility Company				
Sewer Utility Company				
Telephone Utility Company				
Plumber				
Pump Specialist				
"Dig Safe" or local equivalent				
Soil Excavator/Backhoe Operator				
Equipment Rental (Power Generators)				
Equipment Rental (Chlorinators)				
Equipment Rental (Portable Fencing)				
Equipment Repairman				
Radio/Telemetry Repair Service				
Bottled Water Source				
Bulk Water Hauler				
Pump Supplier				
Well Drillers				
Chemical Supplier				
Local/Regional Analytical Laboratory				

### State Notification List

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Drinking Water Primacy Agency				
Department of Environmental Protection (or state equivalent)				
Department of Health				
Emergency Management Agency				
Hazmat Hotline				

### Media Notification List

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Designated Water System Spokesperson				
Newspaper - Local				
Newspaper – Regional/State				
Radio				
Radio				
Radio				
Television				
Television				

## ***Section 3. Communication and Outreach***

### ***Communication***

Communications during an emergency poses some special problems. A standard response might be to call “911” for local fire and police departments. But what if your emergency had disrupted telephone lines and over-loaded cell phone lines? Talk with your state drinking water primacy agency about local emergency preparedness and solutions to these problems. Increasingly, state emergency agencies are establishing secure lines of communication with limited access. Learn how you can access those lines of communication if all others fail.

### ***Outreach***

If there is an incident of contamination in your water supply, you will need to notify the public and make public health recommendations (e.g., boil water, or use bottled water). To do this, you need a plan.

- C How will you reach all customers in the first 24 hours of an emergency?
- C Appoint a media spokesperson—a single person in your water system who will be authorized to make all public statements to the media.
- C Make arrangements for contacting institutions with large numbers of people, some of whom may be immuno-compromised:
  - Nursing homes
  - Hospitals
  - Schools
  - Prisons



### Attachment 3: Threat Identification Checklists

#### Water System Telephone Threat Identification Checklist

In the event your water system receives a threatening phone call, remain calm and try to keep the caller on the line. Use the following checklist to collect as much detail as possible about the nature of the threat and the description of the caller.

<b>1. Types of Tampering/Threat:</b> <input type="checkbox"/> Contamination <input type="checkbox"/> Threat to tamper <input type="checkbox"/> Biological <input type="checkbox"/> Bombs, explosives, etc. <input type="checkbox"/> Chemical <input type="checkbox"/> Other (explain)					
<b>2. Water System Identification:</b>  Name: Address:  Telephone:  PWS Owner or Manager's Name:					
<b>3. Alternate Water Source Available: Yes/No</b>			<b>If yes, give name and location:</b>		
<b>4. Location of Tampering:</b> <input type="checkbox"/> Distribution Line <input type="checkbox"/> Water Storage Facilities <input type="checkbox"/> Treatment Plant <input type="checkbox"/> Raw Water Source <input type="checkbox"/> Treatment Chemicals <input type="checkbox"/> Other (explain):					
<b>5. Contaminant Source and Quantity:</b>					
<b>7. Date and Time of Tampering/Threat:</b>					
<b>8. Caller's Name/Alias, Address, and Telephone Number:</b>					
<b>9. Is the Caller (check all that apply):</b> <input type="checkbox"/> Male <input type="checkbox"/> Female <input type="checkbox"/> Foul <input type="checkbox"/> Illiterate <input type="checkbox"/> Well Spoken <input type="checkbox"/> Irrational <input type="checkbox"/> Incoherent					

<b>10. Is the Caller's Voice (check all that apply):</b>	
<input type="checkbox"/> Soft	<input type="checkbox"/> Calm
<input type="checkbox"/> Slurred	<input type="checkbox"/> Loud
<input type="checkbox"/> Deep	<input type="checkbox"/> Nasal
<input type="checkbox"/> Old	<input type="checkbox"/> High
<input type="checkbox"/> Angry	<input type="checkbox"/> Slow
<input type="checkbox"/> Laughing	<input type="checkbox"/> Crying
<input type="checkbox"/> Clear	<input type="checkbox"/> Lispering
<input type="checkbox"/> Cracking	<input type="checkbox"/> Excited
<input type="checkbox"/> Rapid	
<input type="checkbox"/> Normal	
<input type="checkbox"/> Stuttering	
<input type="checkbox"/> Young	
? Familiar (who did it sound like?)	
? Accented (which nationality or region?)	
<b>11. Is the Connection Clear? (Could it have been a wireless or cell phone?)</b>	
<b>12. Are There Background Noises?</b>	
<input type="checkbox"/> Street noises (what kind?)	
<input type="checkbox"/> Machinery (what type?)	
<input type="checkbox"/> Voices (describe)	
<input type="checkbox"/> Children (describe)	
<input type="checkbox"/> Animals (what kind?)	
<input type="checkbox"/> Computer Keyboard, Office	
<input type="checkbox"/> Motors (describe)	
<input type="checkbox"/> Music (what kind?)	
<input type="checkbox"/> Other	
<b>13. Call Received By (Name, Address, and Telephone Number):</b>	
<b>Date Call Received:</b>	
<b>Time of Call:</b>	
<b>14. Call Reported to:</b>	<b>Date/Time</b>
<b>15. Action(s) Taken Following Receipt of Call:</b>	

## Water System Report of Suspicious Activity

In the event personnel from your water system (or neighbors of your water system) observe suspicious activity, use the following checklist to collect as much detail about the nature of the activity.

<b>1. Types of Suspicious Activity:</b>				
<input type="checkbox"/> Breach of security systems (e.g., lock cut, door forced open)  <input type="checkbox"/> Unauthorized personnel on water system property.  <input type="checkbox"/> Presence of personnel at the water system at unusual hours	<input type="checkbox"/> Changes in water quality noticed by customers (e.g., change in color, odor, taste) that were not planned or announced by the water system  <input type="checkbox"/> Other (explain)			
<b>2. Water System Identification:</b>  Name: Address:  Telephone:  PWS Owner or Manager's Name:				
<b>3. Alternate Water Source Available: Yes/No</b> <span style="float: right;"><b>If yes, give name and location:</b></span>				
<b>4. Location of Suspicious Activity:</b>  <div style="display: flex; justify-content: space-between;"> <span><input type="checkbox"/> Distribution Line</span> <span><input type="checkbox"/> Water Storage Facilities</span> <span><input type="checkbox"/> Treatment Plant</span> <span><input type="checkbox"/> Raw Water Source</span> <span><input type="checkbox"/> Treatment Chemicals</span> </div> <input type="checkbox"/> Other (explain):				
<b>5. If Breach of Security, What was the Nature of the Breach?</b>  <input type="checkbox"/> Lock was cut or broken, permitting unauthorized entry. Specify location  <input type="checkbox"/> Lock was tampered with, but not sufficiently to allow unauthorized entry. Specify location  <input type="checkbox"/> Door, gate, window, or any other point of entry (vent, hatch, etc.) was open and unsecured Specify location  <input type="checkbox"/> Other				

Specify nature and location

**6. Unauthorized personnel on site?**

Where were these people?

Specify location

What made them suspicious?

☐ Not wearing water system uniforms

☐ Something else? (Specify) What were they doing?

**7. Please describe these personnel (height, weight, hair color, clothes, facial hair, any distinguishing marks):**

**8. Call Received By (Name, Address, and Telephone Number):**

**Date Call Received:**

**Time of Call:**

**9. Call Reported to: Date/Time:**

**9. Action(s) Taken Following Receipt of Call**

## Certification of Completion

A final step in completing the “Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems” is to notify the state drinking water primacy agency that the assessment has been conducted. Please fill in the following information and send this page only to the appropriate state drinking water primacy agency contact so that this certification can be included in the records that the state maintains on your water system.

Public Water System (PWS) ID:

---

System Name:

---

Address:

---

Phone:

---

Email:

---

Person Name:

---

Title:

---

Address:

---

Phone:

---

Email:

---

I certify that the information in this vulnerability assessment has been completed to the best of my knowledge and that the appropriate parties have been notified of the assessment and recommended steps to be taken to enhance the security of the water system. Furthermore, a copy of the completed assessment will be retained at the public water system, in a secure location, for state review as requested.

Signed:

---

Date:

---

Please send this page only to the attention of the State Drinking Water Primacy Agency.

# Annex C Rapid Emergency Response Plan Template

<b>UTILITY OPERATIONS</b>
<b>RAPID EMERGENCY RESPONSE PLAN</b>

Utility Name:	<input type="text"/>				
Date Approved:	<input type="text"/>	Date Updated:	<input type="text"/>		
Name of Senior Official reviewing this plan:	<input type="text"/>				
Business Address:	<input type="text"/>				
Telephone:	<input type="text"/>	Fax:	<input type="text"/>	E-Mail:	<input type="text"/>

## Loss of Service Emergency Procedures

- 1.
- 2.
- 3.
- 4.
- 5.

## Identified Threat/Hazard Specific Threat(Earthquake or other) Procedure

- 1.
- 2.
- 3.
- 4.
- 5.

## Identified Threat/Hazard Specific Procedures (Fire or other) Procedure

- 1.
- 2.
- 3.
- 4.
- 5.

## **Public Notification Procedures**

- 1.
- 2.
- 3.
- 4.
- 5.

**Utility point of contacts: Identify by priority the top 3 people who are to be the points of contact for your Utility responsible for restoring critical services.**

**PLEASE DO NOT USE THE SAME TELEPHONE NUMBERS IN MULTIPLE BOXES**

	Time Contacted	Job Title	First Name	Last Name	Work #
	Date	E-Mail Address	Cell#	Home#	
	Time Contacted	Job Title	First Name	Last Name	Work #
	Date	E-Mail Address	Cell#	Home#	
	Time Contacted	Job Title	First Name	Last Name	Work #
	Date	E-Mail Address	Cell#	Home#	
	Time Contacted	Job Title	First Name	Last Name	Work #
	Date	E-Mail Address	Cell#	Home#	
	Time Contacted	Job Title	First Name	Last Name	Work #
	Date	E-Mail Address	Cell#	Home#	

# Table of Contents

<b>Planning Template</b>	<b>Pg. #</b>
Introduction	Pg. #
How to Use the Template	Pg. #
Section 1: System Information	Pg. #
Section 2: Chain of Command – Lines of Authority	Pg. #
Section 3: Events that Cause Emergencies	Pg. #
Section 4: Emergency Notification	Pg. #
Section 5: Effective Communication	Pg. #
Section 6: Response Actions for Specific Events	Pg. #
Section 7: Alternative Water Sources	Pg. #
Section 8: Returning to Normal Operation	Pg. #
Section 9: Plan Approval	Pg. #



# Planning Template



## Introduction

Preparing an emergency response plan is an essential part of managing a drinking water system. Rural Community Assistance Partnership, Inc has developed this template for public water systems serving 3,300 population or fewer to help them develop such plans.



## How to Use the Template

Developing an emergency response plan can take a lot of time and effort. The purpose of this document is to make the job easier and help create a plan that works for your water system. The document is intended for use by any water system and may be modified to fit the specific needs of each system. This document can be used as a starting point based on what is relevant for the type, size, and complexity of the system.

The template is just a guide; you may modify it in any way that works for your system – add sections, take them out, or rearrange them if you wish. You may also use a completely different format for your plan if you find one that works better for your system.

Since this document may contain sensitive information, make sure to keep it stored in a safe and secure location. It is recommended you have one copy stored on-site and one off-site to ensure the document is available in the event you are unable to access your offices or facilities. The document is available electronically on the web at: <http://www.rcap.org>

You should also keep up-to-date plans and schematics of your treatment facility and distribution system (storage tanks, pump stations, etc), as well as up-to-date operations manuals. These should be kept in at least two secure locations, one being with the final version of this emergency response plan



## Section 1. System Information

Keep this basic information easily accessible to authorized staff for emergency responders, repair people, and the news media.

### System information

System Identification Number		
System Name and Address		
Directions to the System		
Basic Description and Location of System Facilities		
Location/Town		
Population Served and Service Connections from Division of Drinking Water Records	_____ people	_____ connections
System Owner		
Name, Title, and Phone Number of Person Responsible for Maintaining and Implementing the Emergency Plan		_____ Phone _____ Cell _____ Pager
Location of treatment and distribution schematics and operations manuals		



## Section 2: Chain of Command – Lines of Authority

The **first response step** in any emergency is to inform the person at the top of this list, who is responsible for managing the emergency and making key decisions.

### Chain of command – lines of authority

Name and Title	Responsibilities During an Emergency	Contact Numbers



## Section 3: Events that Cause Emergencies

The events listed below may cause water system emergencies. They are arranged from highest to lowest probable risk.

### Events that cause emergencies

Type of Event	Probability or Risk (High-Med-Low)	Comments



## Section 4: Emergency Notification

**Notification call-up lists** - Use these lists to notify first responders of an emergency.

<b>Emergency Notification List</b>				
<b>Organization or Department</b>	<b>Name &amp; Position</b>	<b>Telephone</b>	<b>Night or Cell Phone</b>	<b>Email</b>
<b>Local Law Enforcement</b>				
<b>Fire Department</b>				
<b>Emergency Medical Services</b>				
<b>Water Operator (if contractor)</b>				
<b>EPA Contact</b>				
<b>Hazmat Hotline</b>				
<b>Interconnected Water System</b>				
<b>Neighboring Water System (not connected)</b>				
<b>RCAP Contact</b>				
<b>Rural Water Contact</b>				

<b>Priority Customers</b>				
<b>Organization or Department</b>	<b>Name &amp; Position</b>	<b>Telephone</b>	<b>Night or Cell Phone</b>	<b>Email</b>
<b>Hospitals or Clinic(s)</b>				
<b>Public or Private Schools</b>				
<b>Wastewater Treatment Plant</b>				
<b>Adult Care Facility</b>				

State, Federal or Tribal NotificationList				
Organization or Department	Name & Position	Telephone	Night or Cell Phone	Email
State or Tribal Police				
Regulatory Agency State/Federal/Tribal				
Authorized Testing Laboratory				

Service / Repair Notifications				
Organization or Department	Name & Position	Telephone	Night or Cell Phone	Email
Electric Utility Co.				
Electrician				
Gas/Propane Supplier				
Water Testing Lab.				
Sewer Utility Co.				
Telephone Co.				
Plumber				
Pump Supplier				
"Call Before You Dig"				
Rental Equipment Supplier				
Chlorine Supplier				
Other Chemical Supplier				
Well Drilling Co.				
Pipe Supplier				

Media Notification List				
Organization or Department	Name & Position	Telephone	Night or Cell Phone	Email
Newspaper - Local				
Newspaper – Regional/State/Tribal				
Radio				
Radio				
TV Station				

### Notification procedures

Notify water system customers of potential water shortage.

Who is Responsible:	
Procedures:	

Alert local law enforcement, state, federal, or tribal drinking water officials, and local health agencies.

Who is Responsible:	
Procedures:	

**Contact service and repair contractors.**

<b>Procedures:</b>	
<b>Who is Responsible:</b>	

**Contact neighboring water systems, if necessary.**

<b>Who is Responsible:</b>	
<b>Procedures:</b>	

**Procedures for issuing a health advisory.**

<b>Who is Responsible:</b>	
<b>Procedures:</b>	

**Other procedures as necessary**

<b>Who is Responsible:</b>	
----------------------------	--

---





## Section 5: Effective Communication

Communication with customers, the news media, and the general public is a critical part of emergency response.

### Designated public spokesperson

Designate a spokesperson (and alternate) and contact your local primacy agency for delivering messages to the news media and the public.

### Designate a spokesperson and alternates

Spokesperson	Alternate

### Health advisories

During events when water quality and human health are in question, it may be necessary to issue a health advisory that gives advice or recommendations to water system customers on how to protect their health when drinking water is considered unsafe. These advisories are issued when the health risks to the consumers are sufficient, in the estimation of the water system, state or tribal, or local health officials, to warrant such advice.

Health advisories usually take the form of a drinking water warning or boil water advisory. Communication during these times is critical. Health advisories should always be well thought out and provide very clear messages.

The U.S. Environmental Protection Agency has put together a number of tools, including fact sheets, brochures, forms, and templates to help prepare for a health advisory. These are on the web at: <https://www.epa.gov/ground-water-and-drinking-water>.



## Section 6: Response Actions for Specific Events

In any event, there are a series of general steps to take:

1. Analyze the type and severity of the emergency
2. Take immediate actions to save lives
3. Take action to reduce injuries and system damage
4. Make repairs based on priority demand
5. Return the system to normal operation

The following tables identify the assessment, set forth immediate response actions, define what notifications need to be made, and describe important follow-up actions.

### A. Power outage

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

### B. Distribution line break

Assessment	
Immediate Actions	
Notifications	

### C. Chlorine treatment equipment failure

<b>Assessment</b>	
<b>Immediate Actions</b>	
<b>Notifications</b>	
<b>Follow-up Actions</b>	

### D. Treatment equipment

<b>Assessment</b>	
<b>Immediate Actions</b>	
<b>Notifications</b>	
<b>Follow-up Actions</b>	

### E. Source pump failure

<b>Assessment</b>	
<b>Immediate Actions</b>	
<b>Notifications</b>	
<b>Follow-up Actions</b>	

**F. Microbial (coliform, *E. coli*) contamination**

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

**G. Chemical contamination**

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

**H. Vandalism or terrorist attack**

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

## I. Reduction or loss of water in the well

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

## J. Drought

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

## K. Flood

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

## **L. Earthquake**

<b>Assessment</b>	
<b>Immediate Actions</b>	
<b>Notifications</b>	
<b>Follow-up Actions</b>	

## **M. Hazardous materials spill in vicinity of sources or system lines**

<b>Assessment</b>	
<b>Immediate Actions</b>	
<b>Notifications</b>	
<b>Follow-up Actions</b>	

## **N. Electronic equipment failure**

<b>Assessment</b>	
<b>Immediate Actions</b>	
<b>Notifications</b>	
<b>Follow-up Actions</b>	

## O. Cyber attack

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

## P. Other

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	



## Section 7.: Alternative Water Sources

**Intertie to adjacent water supply system**

Water Systems Within One-Quarter Mile of our System	Feasibility of Connecting

**Alternate source(s) of water**

Alternative Sources	Names	Phone	Availability	Is the Water Safe for Drinking?
Bottled water Suppliers for potable water use				
Tanker trucks in the area available to deliver bulk water for non-potable use				





# Section 8: Returning to Normal Operation

## Returning to normal operations

Action	Description and Actions

# Section 9. Plan Approval

## Plan approval

This plan is officially in effect when reviewed, approved, and signed by the following people:

Name/Title	Signature	Date