State of Nevada

Nevada Utility

Vulnerability Assessment and

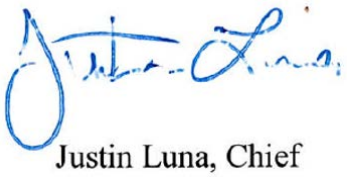
Emergency Response Plan Guide

January 2020

This page is intentionally left blank.

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 Division 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.



Justin Luna, Chief
Nevada Department of Public Safety
Division of Emergency Management

DOCUMENT CHANGE CONTROL

Version	Date	Summary of Changes	Name

Table of Contents

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 Division of Emergency Management (DEM) 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, if implemented properly, 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.

NRS 704.020 "Public utility" or "utility" defined.

1. "Public utility" or "utility" includes:

(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.

Ê 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.

[Part 7:109:1919; A 1925, 243; 1928, 58; NCL § 6106] — (NRS A 1963, 10, 811, 1115; 1967, 1230; 1969, 1155; 1971, 724; 1977, 630; 1981, 154; 1983, 154; 1985, 1016, 2049; 1987, 1541; 1997, 1904; 2003, 3036; 2007, 693, 1771)

NRS 704.021 "Public utility" or "utility" further defined. "Public utility" or "utility" does not include:

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 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.

Ê As used in this subsection, "renewable energy" has the meaning ascribed to it in NRS 704.7715.

11. Persons who own, control, operate or manage a facility that supplies electricity only for use to charge electric vehicles.

12. 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.

[Part 7:109:1919; A 1925, 243; 1928, 58; NCL § 6106] — (NRS A 1963, 403, 816; 1969, 1001; 1971, 725, 1208; 1979, 1717; 1981, 661; 1983, 234, 1227; 1985, 1017, 2298; 1987, 477,

1388, 1542; 1997, 1905; 2001, 346; 2007, 489, 1351; 2009, 1201, 1392; 2011, 1940; 2017, 1269; 2019, 12, 3513)

NRS 704.023 "Small-scale provider of last resort" defined. "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.

(Added to NRS by 2007, 686)

NRS 704.025 "Telecommunication" defined. "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.

(Added to NRS by 2007, 686)

NRS 704.027 "Telecommunication provider" or "telephone company" defined. "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.

(Added to NRS by 2007, 686)

NRS 704.028 "Telecommunication service" or "telephone service" defined. "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.

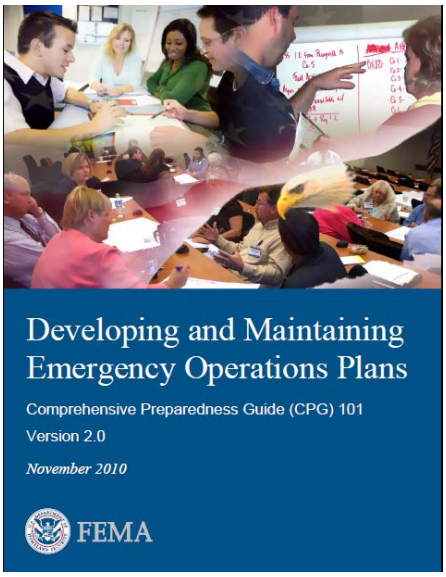
(Added to NRS by 2007, 686)

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

IV. CPG101

The Federal Emergency Management Agency's Comprehensive Preparedness Guide (CPG) 101 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 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.



A copy of CPG 101 can be found at https://www.fema.gov/media-library/assets/documents/25975.

V. 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 Division; 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 Division.

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 Division; 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 Division.

4. 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.

5. 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 Division;

(c) As is reasonably necessary in the case of an emergency involving public health or safety, as determined by the Division; or

(d) Pursuant to the provisions of NRS 239.0115.

6. 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.

7. As used in this section, "provider of new electric resources" has the meaning ascribed to it in NRS 704B.130.

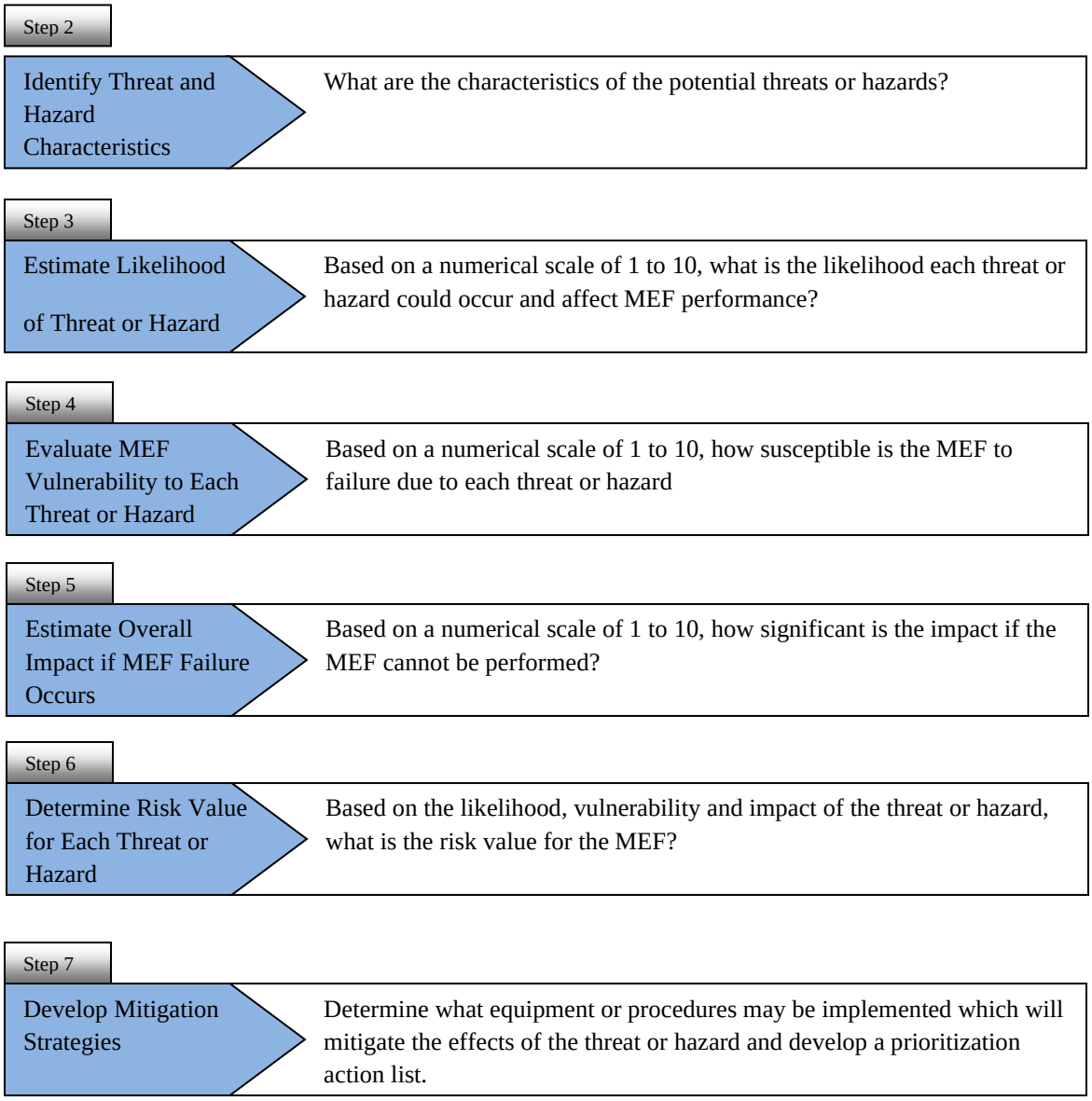
(Added to NRS by 2003, 2460; A 2005, 1536; 2007, 2065; 2011, 2884; 2019, 3530)

VI. Vulnerability Assessment

A Vulnerability Assessment (VA) for a utility is an assessment of what kind of natural and technological hazards 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.

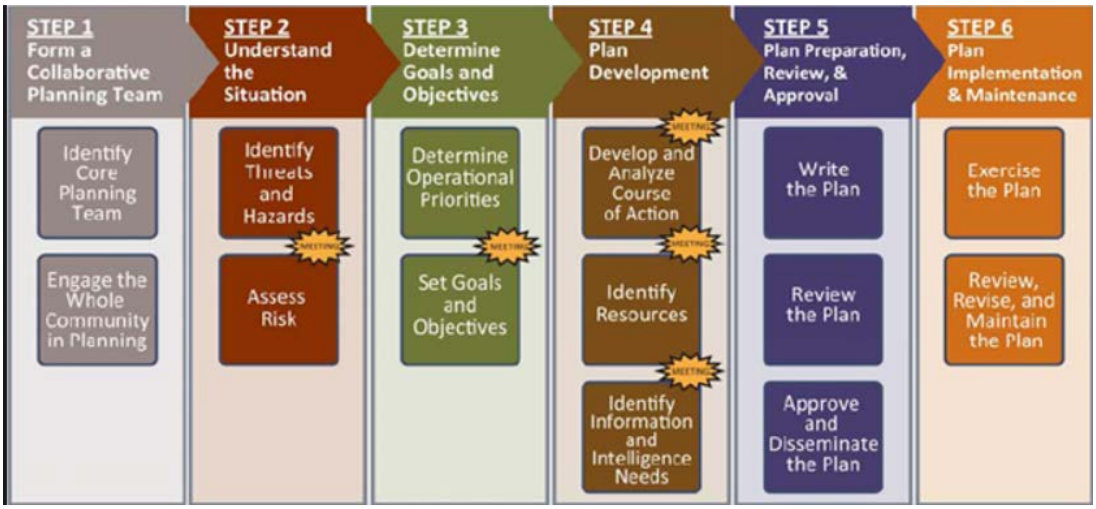
Vulnerability Assessment Instructions

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.)



VII. Planning Development

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 below 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 has to write 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.

VIII. Plan Format and Content

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 reestablish lifeline services.

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.

Example Formats

Rapid Emergency Response Plan (Annex B)
Utility Name Date Approved Date Updated Senior Official Reviewing the Plan Business Address Telephone Fax E-Mail
1. Loss of Service Procedure 2. Identified Threat/Hazard Specific (Wind, Cyber, Earthquake or Other Identified in VA) Procedure

3. Identified Threat/Hazard Specific (Wind, Cyber, Earthquake or Other Identified in VA) Procedure
4. Identified Threat/Hazard Specific (Wind, Cyber, Earthquake or Other Identified in VA) Procedure
5. Public Notification Procedure
6. Points of Contact

Rural Water Format (Annex C)

Cover Page
Promulgation Statement
Approvals
Record of Change
Table of Contents

Section 1. System Information

a. System Name and Address
b. Basic Description of the System
c. Location/Town
d. Name and Contact Information of 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 VA)

a. Types of Events
b. Probability
c. Comments

Section 4. Notification

a. Emergency Notification List
b. Priority Customers
c. State, Federal or Tribal Notification
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 are a series of general steps to take:

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

Section 7. Alternative Lifeline Service Source
Section 8. Returning to Normal Operations
Section 9. Plan Approval

a.

IX. 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 Division 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 Division.

Submission Requirements:

In accordance with NRS 239C.270 as amended by SB69, each resort hotel 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 Division of Emergency Management at the following Address:

Mail to: Division of Emergency Management
2478 Fairview Drive
Carson City, NV 89701
Or E-Mail: NDEMplanning@dps.state.nv.us

X. Emergency Response Plan Training

Emergency Response plans are useless unless all personnel are aware of the contents of the ERP and his/her roles within the plan.

It is recommended that each Utility implement a training program as part of the new hire and continuing training curriculum, which details the ERP contents, concept of operations, and roles and responsibilities of individuals and teams. Quick Reference Tools should also be developed so staff can quickly refer to specific emergency response procedures.

It is recommended that the staff is trained initially upon hire and provided with refresher training every three years.

XI. Emergency Response Plan Exercise

Organizations cannot claim to have an emergency response capability until the plan is tested by a realistic series of exercises. It is recommended by DEM but **not** required by NRS 239C.270, that Utilities utilize the Homeland Security Exercise and Evaluation Program (HSEEP) 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 DEM 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.

XII. Conclusion

Having a well-conceived Emergency Response Plan, 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.

XIII. Acronyms

Acronyms

AAR/IP	After Action Report/Improvement Plan
CPG101	Comprehensive Planning Guide
DEM	Division of Emergency Management
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
ERP	Emergency Response Plan
FEMA	Federal Emergency Management Agency
HSEEP	Homeland Security Exercise and Evaluation Program
IC	Incident Command
MEF	Mission Essential Functions
NRS	Nevada Revised Statutes

This page is intentionally blank.

Vulnerability Assessment Template #1
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 Threat and Hazard Characteristics	What are the characteristics of the potential threats or hazards?
Step 3	Estimate Likelihood of 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 performance?
Step 4	Evaluate 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?
Step 7	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.

Utility Name:			Date Performed:			
Business Impact Analysis Worksheet: Threat and Hazard Analysis						
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.

Vulnerability Assessment Template #2

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:**_____

Date Revised:_____ **Signature:**_____

Date Revised:_____ **Signature:**_____

Inventory of Small Water System Critical Components

Component	Number & Location (if applicable)	Description
Source Water Type		
Ground Water		
Surface Water		
Purchased		
Treatment Plant		
Buildings		
Pumps		
Treatment Equipment (e.g., basin, clearwell, filter)		
Process Controls		
Treatment Chemicals and Storage		
Laboratory Chemicals and Storage		
Storage		
Storage Tanks		
Pressure Tanks		
Power		
Primary Power		
Auxiliary Power		
Distribution System		
Pumps		
Pipes		
Valves		
Appurtenances (e.g., flush hydrants, backflow preventers, meters)		
Other Vulnerable Points		
Offices		
Buildings		
Computers		
Files		
Transportation/ Work Vehicles		
Communications		
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 ☐ No ☐	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). 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. 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). 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.	
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 ☐ No ☐	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: ♦ Issue water system photo identification cards for employees, and require them to be displayed within the restricted area at all times. ♦ Post signs restricting entry to authorized personnel and ensure that assigned staff escort people without proper ID.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
3. Are facilities fenced, including wellhouses and pump pits, and are gates locked where appropriate?	Yes ☐ No ☐	Ideally, all facilities should have a security fence around the perimeter. 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.	
4. Are your doors, windows, and other points of entry such as tank and roof hatches and vents kept closed and locked?	Yes ☐ No ☐	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. A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place. 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. 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.	
5. Is there external lighting around the critical components of your water system?	Yes ☐ No ☐	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 ☐ No ☐	Warning signs are an effective means to deter unauthorized access. "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. "Authorized Personnel Only," "Unauthorized Access Prohibited," and "Employees Only" are examples of other signs that may be useful.	
7. Do you patrol and inspect your source intake, buildings, storage tanks, equipment, and other critical components?	Yes ☐ No ☐	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. 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.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
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 ☐	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. Trim trees and shrubs to enhance the visibility of your water system's critical components. If possible, park vehicles and equipment in places where they do not block the view of your water system's critical components.	
10. Do you have an alarm system that will detect unauthorized entry or attempted entry at critical components?	Yes ☐ No ☐	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. You should also have an audible alarm at the site as a deterrent and to notify neighbors of a potential threat.	
11. Do you have a key control and accountability policy?	Yes ☐ No ☐	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). Vehicle and building keys should be kept in a lockbox when not in use. You should have all keys stamped (engraved) "DO NOT DUPLICATE."	
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 ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 ☐	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. 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.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
20. Are chemicals, particularly those that are potentially hazardous or flammable, properly stored in a secure area?	Yes ☐ No ☐	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.	
21. Do you monitor raw and treated water so that you can detect changes in water quality?	Yes ☐ No ☐	Monitoring of raw and treated water can establish a baseline that may allow you to know if there has been a contamination incident. Some parameters for raw water include pH, turbidity, total and fecal coliform, total organic carbon, specific conductivity, ultraviolet adsorption, color, and odor. 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. 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. 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.	
22. Are tank ladders, access hatches, and entry points secured?	Yes ☐ No ☐	The use of tamper-proof padlocks at entry points (hatches, vents, and ladder enclosures) will reduce the potential for of unauthorized entry. If you have towers, consider putting physical barriers on the legs to prevent unauthorized climbing.	
23. Are vents and overflow pipes properly protected with screens and/or grates?	Yes ☐ No ☐	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 ☐ No ☐	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. Install shut-off or bypass valves to allow you to isolate the storage tank in the case of a contamination problem or structural damage. Consider installing a sampling tap on the storage tank outlet to test water in the tank for possible contamination.	

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 ☐ No ☐	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. 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. Flush hydrants should be kept locked to prevent contaminants from being introduced into the distribution system, and to prevent improper use.	
26. Does your system monitor for, and maintain, positive pressure?	Yes ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
29. Are your personnel issued photo-identification cards?	Yes ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
35. Is there information on the Web that can be used to disrupt your system or contaminate your water?	Yes ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 ☐ No ☐	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 com ponents of your water system. These tools should be secured and accounted for daily.	

Public Relations

You should educate your customers about your system. You should encourage them to be alert and to report any suspicious activity to law enforcement authorities.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
39. Do you have a program to educate and encourage the public to be vigilant and report suspicious activity to assist in the security protection of your water system?	Yes ☐ No ☐	Advise your customers and the public that your system has increased preventive security measures to protect the water supply from vandalism. Ask for their help. Provide customers with your telephone number and the telephone number of the local law enforcement authority so that they can report suspicious activities. The telephone number can be made available through direct mail, billing inserts, notices on community bulletin boards, flyers, and consumer confidence reports.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
40. Does your water system have a procedure to deal with public information requests, and to restrict distribution of sensitive information?	Yes ☐ No ☐	You should have a procedure for personnel to follow when you receive an inquiry about the water system or its operation from the press, customers, or the general public. Your personnel should be advised not to speak to the media on behalf of the water system. Only one person should be designated as the spokesperson for the water system. Only that person should respond to media inquiries. You should establish a process for responding to inquiries from your customers and the general public.	
41. Do you have a procedure in place to receive notification of a suspected outbreak of a disease immediately after discovery by local health agencies?	Yes ☐ No ☐	It is critical to be able to receive information about suspected problems with the water at any time and respond to them quickly. Procedures should be developed in advance with your state drinking water primacy agency, local health agencies, and your local emergency planning committee.	
42. Do you have a procedure in place to advise the community of contamination immediately after discovery?	Yes ☐ No ☐	As soon as possible after a disease outbreak, you should notify testing personnel and your laboratory of the incident. In outbreaks caused by microbial contaminants, it is critical to discover the type of contaminant and its method of transport (water, food, etc.). Active testing of your water supply will enable your laboratory, working in conjunction with public health officials, to determine if there are any unique (and possibly lethal) disease organisms in your water supply. It is critical to be able to get the word out to your customers as soon as possible after discovering a health hazard in your water supply. In addition to your responsibility to protect public health, you must also comply with the requirements of the Public Notification Rule. Some simple methods include announcements via radio or television, door-to-door notification, a phone tree, and posting notices in public places. The announcement should include accepted uses for the water and advice on where to obtain safe drinking water. Call large facilities that have large populations of people who might be particularly threatened by the outbreak: hospitals, nursing homes, the school district, jails, large public buildings, and large companies. Enlist the support of local emergency response personnel to assist in the effort.	
43. Do you have a procedure in place to respond immediately to a customer complaint about a new taste, odor, color, or other physical change (oily, filmy, burns on contact with skin)?	Yes ☐ No ☐	It is critical to be able to respond to and quickly identify potential water quality problems reported by customers. Procedures should be developed in advance to investigate and identify the cause of the problem, as well as to alert local health agencies, your state drinking water primacy agency, and your local emergency planning committee if you discover a problem.	

Now that you have completed the "Security Vulnerability Self-Assessment Guide for Small Water Systems," review your needed actions and then prioritize them based on the most likely threats. A Table to assist

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

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
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.

1. Types of Tampering/Threat:

⎦ Contamination ⎨ Threat to tamper

⎦ Biological ⎨ Bombs, explosives, etc.

⎦ Chemical ⎨ Other (explain)

2. Water System Identification:

Name:
Address:

Telephone:

PWS Owner or Manager's Name:

3. Alternate Water Source Available: Yes/No **If yes, give name and location:**

4. Location of Tampering:

⎦ Distribution Line ⎨ Water Storage Facilities ⎨Treatment Plant ⎨ Raw Water Source ⎨ Treatment Chemicals

⎦ Other (explain):

5. Contaminant Source and Quantity:

7. Date and Time of Tampering/Threat:

8. Caller's Name/Alias, Address, and Telephone Number:

9. Is the Caller (check all that apply):

⎦ Male ⎨ Female ⎨ Foul ⎨ Illiterate ⎨ Well Spoken ⎨ Irrational ⎨ Incoherent

10. Is the Caller's Voice (check all that apply):

⎦ Soft	⎦ Calm	⎦ Angry	⎦ Slow	⎦ Rapid
⎦ Slurred	⎦ Loud	⎦ Laughing	⎦ Crying	⎦ Normal
⎦ Deep	⎦ Nasal	⎦ Clear	⎦ Lisping	⎦ Stuttering
⎦ Old	⎦ High	⎦ Cracking	⎦ Excited	⎦ Young

? Familiar (who did it sound like?)

? Accented (which nationality or region?)

11. Is the Connection Clear? (Could it have been a wireless or cell phone?)

12. Are There Background Noises?

⎦ Street noises (what kind?)	
⎦ Machinery (what type?)	
⎦ Voices (describe)	
⎦ Children (describe)	
⎦ Animals (what kind?)	
⎦ Computer Keyboard, Office	
⎦ Motors (describe)	
⎦ Music (what kind?)	
⎦ Other	

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

Date Call Received:

Time of Call:

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

15. Action(s) Taken Following Receipt of Call:

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.

1. Types of Suspicious Activity:

- ⎦ Breach of security systems (e.g., lock cut, door forced open)
- ⎦ Unauthorized personnel on water system property.
- ⎦ Presence of personnel at the water system at unusual hours
- ⎦ Changes in water quality noticed by customers (e.g., change in color, odor, taste) that were not planned or announced by the water system
- ⎦ Other (explain)

2. Water System Identification:

Name:
Address:

Telephone:

PWS Owner or Manager's Name:

3. Alternate Water Source Available: Yes/No **If yes, give name and location:**

4. Location of Suspicious Activity:

⎦ Distribution Line ⎦ Water Storage Facilities ⎦ Treatment Plant ⎦ Raw Water Source ⎦ Treatment Chemicals

⎦ Other (explain):

5. If Breach of Security, What was the Nature of the Breach?

⎦ Lock was cut or broken, permitting unauthorized entry.

Specify location

⎦ Lock was tampered with, but not sufficiently to allow unauthorized entry.

Specify location

⎦ Door, gate, window, or any other point of entry (vent, hatch, etc.) was open and unsecured

Specify location

⎦ 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:**

10. Action(s) Taken Following Receipt of Call:

Disclaimer

This document contains information on how to plan for protection of the assets of your water system. The work necessarily addresses problems in a general nature. You should review local, state, and federal laws and regulations to see how they apply to your specific situation.

Knowledgeable professionals prepared this document using current information. The authors make no representation, expressed or implied, that this information is suitable for any specific situation. The authors have no obligation to update this work or to make notification of any changes in statutes, regulations, information, or programs described in this document. Publication of this document does not replace the duty of water systems to warn and properly train their employees and others concerning health and safety risks and necessary precautions at their water systems.

Neither the Association of State Drinking Water Administrators, the National Rural Water Association, the U. S. Environmental Protection Agency, or the Drinking Water Academy, nor its contractor, The Cadmus Group, Inc., assume any liability resulting from the use or reliance upon any information, guidance, suggestions,

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: _____

Town/City: _____ State: _____

ZIP Code: _____

Phone: _____ Fax: _____

Email: _____

Person Name: _____

Title: _____

Address: _____

Town/City: _____ State: _____

ZIP Code: _____

Phone: _____ Fax: _____

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 B Rapid Emergency Response Plan Template

UTILITY OPERATIONS

RAPID EMERGENCY RESPONSE PLAN

Utility Name:

Date Approved: Date Updated:

Name of Senior Official reviewing this plan:

Business Address:

Telephone: Fax: E-Mail:

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#	

Contents

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.

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

Priority Customers				
Organization or Department	**Name & Position**	**Telephone**	**Night or Cell Phone**	**Email**
Hospitals or Clinic(s)				
Public or Private Schools				
Wastewater Treatment Plant				
Adult Care Facility				

State, Federal or Tribal Notification List				
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

Procedures:	
Who is Responsible:	

Contact neighboring water systems, if necessary

Who is Responsible:	
Procedures:	

Procedures for issuing a health advisory

Who is Responsible:	
Procedures:	

Other procedures as necessary

Who is Responsible:	

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, and
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

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

D. Treatment equipment

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

E. Source pump failure

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

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

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

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

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

N. Electronic equipment failure

Assessment	
Immediate Actions	
Notifications	
Follow-up Actions	

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