Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Below 3,300

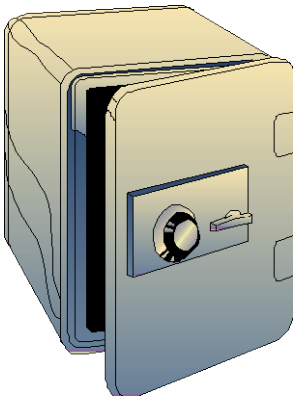
Association of State Drinking Water Administrators

National Rural Water Association

Mississippi Rural Water Association

May 30, 2002

A Note about Security for this Document



This document contains sensitive information about the security of your water system. Therefore, it should be treated as **Confidential Information** and should be stored in a secure place at your water system. A duplicate copy should also be stored in a secure off-site location.

Acknowledgments

This document is the result of collaboration among the Association of Drinking Water Administrators (ASDWA), the U.S. Environmental Protection Agency (U.S. EPA), the U.S. EPA Drinking Water Academy, and the National Rural Water Association (NRWA). We also thank NRWA for the template that was used as the foundation for this project.

Contents

SECURITY VULNERABILITY SELF-ASSESSMENT GUIDE FOR SMALL WATER SYSTEMS 3
INTRODUCTION 3
HOW TO USE THIS SELF-ASSESSMENT GUIDE 3
KEEP THIS DOCUMENT 3
SECURITY VULNERABILITY SELF-ASSESSMENT 4
RECORD OF SECURITY VULNERABILITY SELF-ASSESSMENT COMPLETION 4
INVENTORY OF SMALL WATER SYSTEM CRITICAL COMPONENTS 5
SECURITY VULNERABILITY SELF-ASSESSMENT FOR SMALL WATER SYSTEMS 6
GENERAL QUESTIONS FOR THE ENTIRE WATER SYSTEM 6
WATER SOURCES 9
TREATMENT PLANT AND SUPPLIERS 9
DISTRIBUTION 11
PERSONNEL 11
INFORMATION STORAGE/COMPUTERS/CONTROLS/MAPS 12
PUBLIC RELATIONS 13
ATTACHMENT 1. PRIORITIZATION OF NEEDED ACTIONS 15
ATTACHMENT 2. EMERGENCY CONTACT LIST 16
SECTION 1. SYSTEM IDENTIFICATION 16
SECTION 2. NOTIFICATION/CONTACT INFORMATION 17
SECTION 3. COMMUNICATION AND OUTREACH 20
ATTACHMENT 3: THREAT IDENTIFICATION CHECKLISTS 21
WATER SYSTEM TELEPHONE THREAT IDENTIFICATION CHECKLIST 21
WATER SYSTEM REPORT OF SUSPICIOUS ACTIVITY 23
CERTIFICATION OF COMPLETION 26

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: _____

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 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 backsiphonage 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 components 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 you in prioritizing actions is provided in Attachment 1.

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				
Pipe Supplier				
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				
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.

X How will you reach all customers in the first 24 hours of an emergency?

X Appoint a media spokesperson—a single person in your water system who will be authorized to make all public statements to the media.

X 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, conclusions, or opinions contained in this document.

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 pubic 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.