

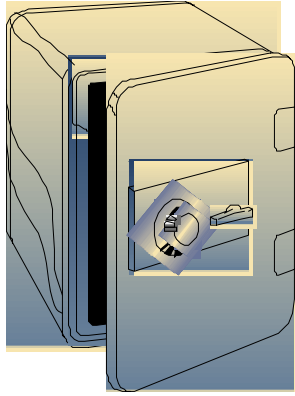


# **Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000**

**Association of State Drinking Water  
Administrators**

**National Rural Water Association**

November 13, 2002



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).

# Contents

SECURITY VULNERABILITY SELF-ASSESSMENT GUIDE FOR SMALL WATER SYSTEMS .....	4
Introduction .....	4
How to Use this Self-Assessment Guide .....	4
Before Starting this Assessment.....	5
Keep this Document.....	5
SECURITY VULNERABILITY SELF-ASSESSMENT .....	6
Record of Security Vulnerability Self-Assessment Completion .....	6
Inventory of Small Water System Critical Components .....	7
SECURITY VULNERABILITY SELF-ASSESSMENT FOR SMALL WATER SYSTEMS.....	8
General Questions for the Entire Water System.....	8
Water Sources .....	11
Treatment Plant and Suppliers .....	11
Distribution .....	13
Personnel .....	14
Information/Storage/Computers/Controls/Maps.....	15
Public Relations .....	16
ATTACHEMENT 1. PRIORITIZATION OF NEEDED ACTIONS .....	18
ATTACHEMENT 2. EMERGENCY CONTACT LIST.....	19
Section 1 System Identification .....	19
Section 2 Notification/Contact Information.....	20
Section 3 Communication and Outreach .....	24
ATTACHMENT 3. THREAT IDENTIFICATION CHECKLISTS.....	25
Water System Telephone Threat Identification Checklist .....	25
Water System Report of Suspicious Activity.....	27
CERTIFICATION OF COMPLETION.....	29

# **Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000**

## **Introduction**

Water systems are critical to every community. Protection of public drinking water systems should 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 in order to protect the system and the customers it serves. A “vulnerability assessment” (VA) is the identification of weaknesses in water system security, focusing on defined threats that could compromise its ability to meet its various service missions - such as providing adequate drinking water, water for firefighting, and/or water for various commercial and industrial purposes. This document is designed particularly for systems that serve populations of 3,300 up to 10,000. 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. Completion of this document will meet the requirement for conducting a Vulnerability Assessment as directed under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. Community Water Systems (CWSs) serving more than 3,300 and fewer than 50,000 people must submit their completed vulnerability assessment to the U.S. EPA no later than June 30, 2004 in order to meet the provisions of the Act. **See page 29 for mailing and delivery instructions. You must follow these instructions to protect your information.**

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. According to the Bioterrorism Law, vulnerability assessments should include, but not be limited to, a review of pipes and constructed conveyances, physical barriers, water collection, pretreatment, treatment, storage and distribution facilities, electronic, computer or other automated systems which are utilized by the public water system, the use, storage, or handling of various chemicals, and the operation and maintenance of such system. 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 a basic emergency contact list for your use; however, under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, all systems serving a population greater than 3,300 must complete or revise an emergency response plan based on their vulnerability assessment. Systems must certify to the U.S. EPA Administrator that incorporates the results of the VA that have been completed or revised within six months of submitting their vulnerability assessment to U.S.

EPA. The list included as Attachment 2 will not meet the requirements of the Bioterrorism Act, but it 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. You may be able to obtain sample Emergency Response Plans from your state drinking water primacy agency. Development of the emergency response plan should be coordinated with the Local Emergency Planning Committee (LEPC).

Security is everyone's responsibility. This document should help you to increase the awareness of all your employees, governing officials, and customers about security issues. Once you have completed the questions, review the actions you need to take to improve your system's security. The goal of the vulnerability assessment is to develop a system-specific list of priorities intended to reduce risks to threats of attack. Make sure to prioritize your actions based on the most likely threats to your system. Once you have developed your list of priority actions, you have completed your vulnerability assessment. Please complete the Certificate of Completion on page 29 and return only the certificate to your state drinking water primacy agency. Unless your state has its own requirement that the vulnerability assessments be submitted to the state for review (e.g. New York) do not include a full copy of your self-assessment with the certification submitted to the state primacy agency. Please check with your state drinking water primacy agency to find out what is required for your state. In addition, under the Bioterrorism Act all systems serving a population greater than 3,300 and less than 50,000 must submit their completed vulnerability assessment and a Certificate of Completion to the U.S. EPA by June 30, 2004. (See page 29 for instructions on how to do this.)

## **Before Starting this Assessment**

Systems should make an effort to identify critical services and customers, such as hospitals or power facilities, as well as critical areas of their drinking water system that if attacked could result in a significant disruption of vital community services, result in a threat to public health, or a complete shut down of the system (e.g. inability to provide an adequate supply of water for fire prevention, inability to provide safe potable water, or release of hazardous chemicals that could cause catastrophic results). When prioritizing the potential water system vulnerabilities and consequences factor into the decision process the critical facilities, services, and single points in the system that if debilitated could result in significant disruption of vital community services or health protection. To help identify priorities for your system, the table on page 7 provides a column where you can categorize the assets that you consider critical into one of three categories – high (H), medium (M), or low (L).

When evaluating a system's potential vulnerability, systems should attempt to determine what type of assailants and threats they are trying to protect against. Systems should contact their local law enforcement office to see if they have information indicating the types of threats that may be likely against their facility. Systems should also refer to the U.S. EPA "Baseline Threat Information for Vulnerability Assessments of Community Water Systems" to help assess the most likely threats to their water system. This document is available to CWSs serving greater than 3,300 people. If your system has not yet received instructions on how to receive a copy of this document, then contact your Regional U.S. EPA Office immediately. You will be sent instructions on how to securely access it via the Water Information Sharing and Analysis Center (ISAC) website or obtain a hard copy that can be mailed directly to you. Some of the typical threats to your facility may be vandalism, an insider (i.e. disgruntled employee), a terrorist, or a terrorist working with a system employee.

## **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. 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.

<b>Name:</b>	_____
<b>Title:</b>	_____
<b>Area of Responsibility:</b>	_____
<b>Water System Name:</b>	_____
<b>Water System PWSID:</b>	_____
<b>Address:</b>	_____
<b>City:</b>	_____
<b>County:</b>	_____
<b>State:</b>	_____
<b>Zip Code:</b>	_____
<b>Telephone:</b>	_____
<b>Fax:</b>	_____
<b>E-mail:</b>	_____
<b>Date Completed:</b>	_____
<b>Date Revised:</b>	_____
<b>Signature:</b>	_____
<b>Date Revised:</b>	_____
<b>Signature:</b>	_____
<b>Date Revised:</b>	_____
<b>Signature:</b>	_____
<b>Date Revised:</b>	_____
<b>Signature:</b>	_____
<b>Date Revised:</b>	_____
<b>Signature:</b>	_____

## Inventory of Small Water System Critical Components

Component	Number & Location (if applicable)	Description	Critical Asset or Single Point of Failure (H/M/L)
<b>Source Water Type</b>			
Ground Water			
Surface Water			
Purchased			
<b>Treatment Plant</b>			
Buildings			
Pumps			
Treatment Equipment (e.g., basin, clear well, filter)			
Process Controls			
Treatment Chemicals and Storage			
Laboratory Chemicals and Storage			
<b>Storage</b>			
Storage Tanks			
Pressure Tanks			
<b>Power</b>			
Primary Power			
Auxiliary Power			
<b>Distribution System</b>			
Pumps			
Pipes			
Valves			
Appurtenances (e.g., flush hydrants, backflow preventers, meters)			
Other Vulnerable Points			
<b>Offices</b>			
Buildings			
Computers			
Files			
Transportation/ Work Vehicles			
Personnel			
<b>Communications</b>			
Telephone			
Cell Phone			
Radio			
Computer Control Systems (SCADA)			
<b>Critical Facilities Served</b>			
Power Plant Facilities			
Hospitals			
Schools			
Waste Water Treatment Plants			
Food/Beverage Processing Plants			
Nursing Homes			
Prisons/Other Institutions			

## Security Vulnerability Self-Assessment for Small Water Systems

*The first 15 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 "	<p>Under the provisions of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 you are required to develop and/or update an ERP within six months after completing this assessment. If you do not have an ERP, you can obtain a sample from your state drinking water primacy agency. As a first step in developing your ERP, you should develop your Emergency Contact List (see Attachment 2).</p> <p>A plan is vital in case there is an incident that requires immediate response. Your plan should be reviewed at least annually (or more frequently if necessary) to ensure it is up-to-date and addresses security emergencies including ready access to laboratories capable of analyzing water samples. You should coordinate with your LEPC.</p> <p>You should designate someone to be contacted in case of emergency regardless of the day of the week or time of day. This contact information should be kept up-to-date and made available to all water system personnel and local officials (if applicable).</p> <p>Share this ERP with police, emergency personnel, and your state primacy agency. Posting contact information is a good idea only if authorized personnel are the only ones seeing the information. These signs could pose a security risk if posted for public viewing since it gives people information that could be used against the system.</p>	
2. Have you reviewed U.S. EPA's Baseline Threat Information Document?	Yes "    No "	<p>The U.S. EPA baseline threat document is available through the Water Information Sharing and Analysis Center at <a href="http://www.waterisac.org">www.waterisac.org</a>. It is important you use this document to determine potential threats to your system and to obtain additional security related information. U.S. EPA should have provided a certified letter to your system that provided instructions on obtaining the threat document.</p>	
3. 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 "	<p>You should restrict or limit access to the critical components of your water system to authorized personnel only. This is the first step in security enhancement for your water system. Consider the following:</p> <ul style="list-style-type: none"> <li>◆ Issue water system photo identification cards for employees, and require them to be displayed within the restricted area at all times.</li> <li>◆ Post signs restricting entry to authorized personnel and ensure that assigned staff escort people without proper ID.</li> </ul>	



QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
4. Are all critical facilities fenced, including wellhouses and pump pits, and are gates locked where appropriate?	Yes " No "	<p>Ideally, all facilities should have a security fence around the perimeter.</p> <p>The fence perimeter should be walked periodically to check for breaches and maintenance needs. All gates should be locked with chains and a tamper-proof padlock that at a minimum protects the shank. Other barriers such as concrete "jersey" barriers should be considered to guard certain critical components from accidental or intentional vehicle intrusion.</p>	
5. Are all critical doors, windows, and other points of entry such as tank and roof hatches and vents kept closed and locked?	Yes " No "	<p>Lock all building doors and windows, hatches and vents, gates, and other points of entry to prevent access by unauthorized personnel. Check locks regularly. Dead bolt locks and lock guards provide a high level of security for the cost.</p> <p>A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place.</p> <p>Doors and hinges to critical facilities should be constructed of heavy-duty reinforced material. Hinges on all outside doors should be located on the inside.</p> <p>To limit access to water systems, all windows should be locked and reinforced with wire mesh or iron bars, and bolted on the inside. Systems should ensure that this type of security meets with the requirements of any fire codes. Alarms can also be installed on windows, doors, and other points of entry.</p>	
6. Is there external lighting around all critical components of your water system?	Yes " No "	<p>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.</p>	
7. 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 "	<p>Warning signs are an effective means to deter unauthorized access.</p> <p>"Warning - Tampering with this facility is a federal offense" should be posted on all water facilities. These are available from your state rural water association.</p> <p>"Authorized Personnel Only," "Unauthorized Access Prohibited," and "Employees Only" are examples of other signs that may be useful.</p>	
8. Do you patrol and inspect all source intake, buildings, storage tanks, equipment, and other critical components?	Yes " No "	<p>Frequent and random patrolling of the water system by utility staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol.</p> <p>All systems are encouraged to initiate personal contact with the local law enforcement to show them the drinking water facility. The tour should include the identification of all critical components with an explanation of why they are important. Systems are encouraged to review, with local law enforcement, the NRWA/ASDWA Guide for Security Decisions or similar state document to clarify respective roles and responsibilities in the event of an incident. Also consider asking the local law enforcement to conduct periodic patrols of your water system.</p>	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
9. Is the area around all 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).	
10. Are the entry points to all of your water system easily seen?	Yes "    No "	<p>You should clear fence lines of all vegetation. Overhanging or nearby trees may also provide easy access. Avoid landscaping that will permit trespassers to hide or conduct unnoticed suspicious activities.</p> <p>Trim trees and shrubs to enhance the visibility of your water system's critical components.</p> <p>If possible, park vehicles and equipment in places where they do not block the view of your water system's critical components.</p>	
11. Do you have an alarm system that will detect unauthorized entry or attempted entry at all critical components?	Yes "    No "	<p>Consider installing an alarm system that notifies the proper authorities or your water system's designated contact for emergencies when there has been a breach of security. Inexpensive systems are available. An alarm system should be considered whenever possible for tanks, pump houses, and treatment facilities.</p> <p>You should also have an audible alarm at the site as a deterrent and to notify neighbors of a potential threat.</p>	
12. Do you have a key control and accountability policy?	Yes "    No "	<p>Keep a record of locks and associated keys, and to whom the keys have been assigned. This record will facilitate lock replacement and key management (e.g., after employee turnover or loss of keys). Vehicle and building keys should be kept in a lockbox when not in use.</p> <p>You should have all keys stamped (engraved) "DO NOT DUPLICATE."</p>	
13. 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.	
14. Do you have an updated operations and maintenance manual that includes evaluations of security systems?	Yes "    No "	Operation and maintenance plans are critical in assuring the on-going provision of safe and reliable water service. These plans should be updated to incorporate security considerations and the on-going reliability of security provisions – including security procedures and security related equipment.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
15. 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 1-15), 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
16. 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.	
17. 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.	
18. 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.	
19. 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
20. 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.	

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

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
26. Can you isolate the storage tank from the rest of the system?	Yes " No "	<p>A water system should be able to take its storage tank(s) out of operation or drain its storage tank(s) if there is a contamination problem or structural damage. Install shut-off or bypass valves to allow you to isolate the storage tank in the case of a contamination problem or structural damage.</p> <p>Consider installing a sampling tap on the storage tank outlet to test water in the tank for possible contamination.</p>	

### ***Distribution***

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

QUESTION	ANSWER	COMMENT	ACTION/NEEDED TAKEN
27. Do you control the use of hydrants and valves?	Yes " No "	<p>Your water system should have a policy that regulates the authorized use of hydrants for purposes other than fire protection. Require authorization and backflow devices if a hydrant is used for any purpose other than fire fighting.</p> <p>Consider designating specific hydrants for use as filling station(s) with proper backflow prevention (e.g., to meet the needs of construction firms). Then, notify local law enforcement officials and the public that these are the only sites designated for this use.</p> <p>Flush hydrants should be kept locked to prevent contaminants from being introduced into the distribution system, and to prevent improper use.</p>	
28. 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.	
29. 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.*

<b>QUESTION</b>	<b>ANSWER</b>	<b>COMMENT</b>	<b>ACTION NEEDED/TAKEN</b>
30. 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 "	<p>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.</p> <p>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.</p>	
31. Are your personnel issued photo-identification cards?	Yes " No "	<p>For positive identification, all personnel should be issued water system photo-identification cards and be required to display them at all times.</p> <p>Photo identification will also facilitate identification of authorized water system personnel in the event of an emergency.</p>	
32. 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.	
33. 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.	
34. Have water system personnel been advised to report security vulnerability concerns and to report suspicious activity?	Yes " No "	<p>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.</p> <p>Periodic meetings of authorized personnel should be held to discuss security issues.</p>	
35. Do your personnel have a checklist to use for threats or suspicious calls or to report suspicious activity?	Yes " No "	<p>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.</p> <p>Also consider installing caller ID on your telephone system to keep a record of incoming calls.</p>	

## 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
<p>36. 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?</p>	<p>Yes " No "</p>	<p>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 side of the computer and reviewed and updated periodically.</p> <p>Also consider contacting a virus protection company and subscribing to a virus update program to protect your records.</p> <p>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.</p>	
<p>37. Is there information on the Web that can be used to disrupt your system or contaminate your water?</p>	<p>Yes " No "</p>	<p>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.</p> <p>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.</p>	
<p>38. Are maps, records, and other information stored in a secure location?</p>	<p>Yes " No "</p>	<p>Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only.</p> <p>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.</p>	
<p>39. Are copies of records, maps, and other sensitive information labeled confidential, and are all copies controlled and returned to the water system?</p>	<p>Yes " No "</p>	<p>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.</p>	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
40. Are vehicles locked and secured at all times?	Yes " No "	<p>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.</p> <p>Water system vehicles should be locked when they are not in use or left unattended.</p> <p>Remove any critical information about the system before parking vehicles for the night.</p> <p>Vehicles also usually contain tools (e.g., valve wrenches) and keys that could be used to access critical components of your water system. These should be secured and accounted for daily.</p>	

### **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
41. 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 "	<p>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.</p>	
42. Does your water system have a procedure to deal with public information requests, and to restrict distribution of sensitive information?	Yes " No "	<p>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.</p> <p>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.</p>	
43. 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 "	<p>It is critical to be able to receive information about suspected problems with the water at any time and respond to them quickly. Written procedures should be developed in advance with your state drinking water primacy agency, local health agencies, and your local emergency planning committee and reviewed periodically.</p>	



QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
44. Do you have a procedure in place to advise the community of contamination immediately after discovery?	Yes "    No "	<p>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.</p> <p>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.</p>	
45. 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 Serving Populations Between 3,300 and 10,000,” 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 Serving Populations Between 3,300 and 10,000,” 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. You can rank your priorities in numerical order or based on the categories of high, medium, and low.

Use the following information and the information you have generated by completing this assessment to prioritize and rank the most important security vulnerabilities to your system:

1. Any information from local law enforcement office about the likelihood of a terrorist attack or other threats.
2. The U.S. EPA “Baseline Threat Document” to determine the most likely types of threats to protect against.
3. The primary mission of your system (i.e. serve potable water, sufficient water for fire protection, etc.).
4. Single points of failure (i.e. disabling pump) that severely limit your capability to conduct your primary mission.
5. Critical customers – such as hospitals, power plants, schools or waste water treatment facilities.
6. The vulnerabilities identified by completing this assessment.

Question Number	Needed Action	Scheduled Completion	Priority/Ranking

## Attachment 2. Emergency Contact List

All community water systems serving populations greater than 3,300 and less than 10,000 must adopt an emergency response plan (ERP) based on their vulnerability assessment. Emergency response 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.” Although, it can be an essential part of your ERP, **this will not satisfy the Bioterrorism Act requirement to develop or update your emergency response plan based on your vulnerability assessment.** 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. You should also 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 – Update regularly and display clearly next to telephones**

**Responders**

<b>ORGANIZATION</b>	<b>CONTACT NAME/TITLE</b>	<b>PHONE (DAY)</b>	<b>PHONE (NIGHT)</b>	<b>E-MAIL</b>
Fire Department				
Police Department				
FBI Field Office (for terrorism or sabotage)				
Emergency Medical Service				
Local Health Department				
National Spill Response Center	24 Hour Hotline	<b>1 (800) 424-8802</b>		
State Spill Hotline	24 Hour Hotline			
Local Hazmat Team (if any)				
Local/Regional Laboratory				
Water System Operators				

### Local Notification List

<b>ORGANIZATION</b>	<b>CONTACT NAME/TITLE</b>	<b>PHONE (DAY)</b>	<b>PHONE (NIGHT)</b>	<b>E-MAIL</b>
Government Officials				
Emergency Planning Committee				
Hospitals				
Pharmacy				
Nursing Homes				
Schools				
Prisons				
Neighboring Water Systems				
Critical Industrial/Commercial Water Users				
Others				

### Service/Repair Notification List

<b>ORGANIZATION</b>	<b>CONTACT NAME/TITLE</b>	<b>PHONE (DAY)</b>	<b>PHONE (NIGHT)</b>	<b>E-MAIL</b>
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				
Equipment Repairman (Chlorinator)				
Radio/Telemetry Repair Service				
Bottled Water Source				
Bulk Water Hauler				
Pump Supplier				
Well Drillers				
Pipe Supplier				
Chemical Supplier				

**State Notification List**

<b>ORGANIZATION</b>	<b>CONTACT NAME/TITLE</b>	<b>PHONE (DAY)</b>	<b>PHONE (NIGHT)</b>	<b>E-MAIL</b>
Drinking Water Primacy Agency				
Department of Environmental Protection (or state equivalent)				
Department of Health				
Emergency Management Agency				
Hazmat Hotline				

**Media Notification List**

<b>ORGANIZATION</b>	<b>CONTACT NAME/TITLE</b>	<b>PHONE (DAY)</b>	<b>PHONE (NIGHT)</b>	<b>E-MAIL</b>
Designated Water System Spokesperson				
Newspaper - Local				
Newspaper – Regional/State				
Radio				
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 local Emergency Management Agency, Health Department representative, or your Local Emergency Planning Committee (LEPC) 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.

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



# Attachment 3: Threat Identification Checklists

## Water System Telephone Threat Identification Checklist

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

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

<p><b>10. Is the Caller's Voice (check all that apply):</b></p> <p> <input type="checkbox"/> Soft                      <input type="checkbox"/> Calm                      <input type="checkbox"/> Angry                      <input type="checkbox"/> Slow                      <input type="checkbox"/> Rapid  <input type="checkbox"/> Slurred                      <input type="checkbox"/> Loud                      <input type="checkbox"/> Laughing                      <input type="checkbox"/> Crying                      <input type="checkbox"/> Normal  <input type="checkbox"/> Deep                      <input type="checkbox"/> Nasal                      <input type="checkbox"/> Clear                      <input type="checkbox"/> Lispering                      <input type="checkbox"/> Stuttering  <input type="checkbox"/> Old                      <input type="checkbox"/> High                      <input type="checkbox"/> Cracking                      <input type="checkbox"/> Excited                      <input type="checkbox"/> Young  <input type="checkbox"/> Familiar (who did it sound like?)  <input type="checkbox"/> Accented (which nationality or region?) </p>																			
<p><b>11. Is the Connection Clear? (Could it have been a wireless or cell phone?)</b></p>																			
<p><b>12. Are There Background Noises?</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;"><input type="checkbox"/> Street noises (what kind?)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Machinery (what type?)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Voices (describe)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Children (describe)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Animals (what kind?)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Computer Keyboard, Office</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Motors (describe)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Music (what kind?)</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Other</td> <td></td> </tr> </table>		<input type="checkbox"/> Street noises (what kind?)		<input type="checkbox"/> Machinery (what type?)		<input type="checkbox"/> Voices (describe)		<input type="checkbox"/> Children (describe)		<input type="checkbox"/> Animals (what kind?)		<input type="checkbox"/> Computer Keyboard, Office		<input type="checkbox"/> Motors (describe)		<input type="checkbox"/> Music (what kind?)		<input type="checkbox"/> Other	
<input type="checkbox"/> Street noises (what kind?)																			
<input type="checkbox"/> Machinery (what type?)																			
<input type="checkbox"/> Voices (describe)																			
<input type="checkbox"/> Children (describe)																			
<input type="checkbox"/> Animals (what kind?)																			
<input type="checkbox"/> Computer Keyboard, Office																			
<input type="checkbox"/> Motors (describe)																			
<input type="checkbox"/> Music (what kind?)																			
<input type="checkbox"/> Other																			
<p><b>13. Call Received By (Name, Address, and Telephone Number):</b></p> <p><b>Date Call Received:</b></p> <p><b>Time of Call:</b></p>																			
<p><b>14. Call Reported to:</b></p>	<p><b>Date/Time</b></p>																		
<p><b>15. Action(s) Taken Following Receipt of Call:</b></p>																			

## Water System Report of Suspicious Activity

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

<b>1. Types of Suspicious Activity:</b>				
<input type="checkbox"/> Breach of security systems (e.g., lock cut, door forced open)	<input type="checkbox"/> Changes in water quality noticed by customers (e.g., change in color, odor, taste) that were not planned or announced by the water system			
<input type="checkbox"/> Unauthorized personnel on water system property.	<input type="checkbox"/> Other (explain)			
<input type="checkbox"/> Presence of personnel at the water system at unusual hours				
<b>2. Water System Identification:</b>				
Name:				
Address:				
Telephone:				
PWS Owner or Manager's Name:				
<b>3. Alternate Water Source Available: Yes/No</b>	<b>If yes, give name and location:</b>			
<b>4. Location of Suspicious Activity:</b>				
<input type="checkbox"/> Distribution Line	<input type="checkbox"/> Water Storage Facilities	<input type="checkbox"/> Treatment Plant	<input type="checkbox"/> Raw Water Source	<input type="checkbox"/> Treatment Chemicals
<input type="checkbox"/> Other (explain):				

**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:**

# Certification of Completion of Assessment

A final step in completing the "Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000" 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.

- **DO NOT** send the completed vulnerability assessment (VA) to your state primacy agency unless your state requires VA submittals.
- **DO** send the completed VA to U.S. EPA by June 30, 2004 to satisfy the requirements of the Federal Bioterrorism Act. You must also certify to U.S. EPA that you have developed or updated your emergency response plan based on your VA within six months of submitting your VA to the U.S. EPA.

- **Mailing and Delivery Instructions**

U.S. EPA recommends that you **DO NOT** use the U.S. Postal Service.

To ensure proper tracking and delivery, you should send your VA and certification using an express shipping or courier service such as Federal Express, United Parcel Service, or Airborne, to the address below. The phone number for couriers to use is (202) 566-1729.

**U.S. EPA Water Resource Center (WSD-RAR)**

Room 1119 EPA West Building  
1301 Constitution Ave., NW  
Washington, DC 20004

**For More Mailing Information**

<http://www.epa.gov/safewater/security/util-inst.pdf>  
Safe Drinking Water Hotline (800) 426-4791  
Reference document number 810-B-02-001

**System PWS ID No:** \_\_\_\_\_

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

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

**Town/City:** \_\_\_\_\_ **State:** \_\_\_\_\_

**ZIP Code:** \_\_\_\_\_

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

**Email:** \_\_\_\_\_

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

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

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

**Town/City:** \_\_\_\_\_ **State:** \_\_\_\_\_

**ZIP Code:** \_\_\_\_\_

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

**Email:** \_\_\_\_\_

## 24 Hour Emergency Contact Information for Your System:

**Contact Person:** First Name: \_\_\_\_\_ Last Name: \_\_\_\_\_

**Daytime Phone:** \_\_\_\_\_ **Fax:** \_\_\_\_\_

**Emergency Phone:** \_\_\_\_\_ **E-mail:** \_\_\_\_\_

**Cell Phone:** \_\_\_\_\_

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** \_\_\_\_\_

## **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 assume any liability resulting from the use or reliance upon any information, guidance, suggestions, conclusions, or opinions contained in this document.