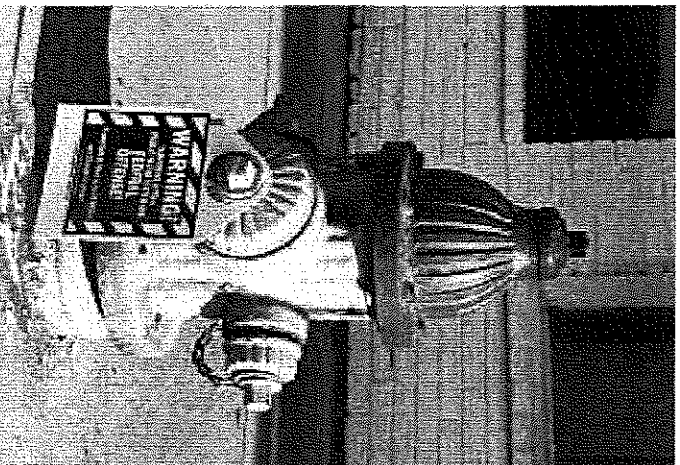




# Drinking Water Security for Small Systems Serving 3,300 or Fewer Persons

One of the Simple Tools for Effective  
Performance (STEP) Guide Series



## **Disclaimer**

The U.S. Environmental Protection Agency (EPA) prepared this guide to help you enhance the security of your water system. This document does not impose legally binding requirements on EPA, states, tribes, or the regulated community, and it may or may not be applicable to a particular situation depending on the circumstances. EPA and state decision makers retain the discretion to adopt approaches on a case-by-case basis that may differ from this guidance where appropriate. Any decisions regarding a particular community water system will be made based on the applicable statutes and regulations. Therefore, interested parties are free to raise questions and objections about the appropriateness of the application of this guide to a particular situation, and EPA will consider whether the recommendations or interpretations in this guide are appropriate in that situation based on the law and regulations. EPA may change this guidance in the future. To determine whether EPA has revised this guide or to obtain additional copies, contact the Safe Drinking Water Hotline at (800) 426-4791.

# Contents

Is This Guide for Me? .....	1
What Will I Learn? .....	2
Why Is It Important to Improve Security and Prepare for Emergencies? .....	3
What Is a Vulnerability Assessment? .....	4
What Security Improvements Can I Make Immediately? .....	12
What Is an Emergency Response Plan? .....	16
How Do I Maintain and Upgrade Security in the Long Run? .....	27
How Should I Communicate with My Customers? .....	30
Where Can I Find Additional Help? .....	34
Appendix A: Safe Drinking Water Act Primacy Agencies .....	37
Appendix B: EPA Regional Contacts .....	42
Appendix C: Other STEP Documents .....	43

# Is This Guide for Me?

This guide is designed for community water systems (CWSs) serving 3,300 or fewer persons. CWSs include all publicly and privately owned systems providing drinking water to at least 25 year-round residential customers or 15 year-round service connections. This guide may be useful for:

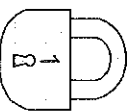
- Small town systems
- Rural water districts
- Tribal systems
- Manufactured home communities
- Homeowners' associations
- Small private systems
- Public Service Districts (PSDs)

This guide presents basic information and steps you can take to improve security and emergency preparedness at your water system. It explains why security improvements are important and discusses Vulnerability Assessments (VAs) and Emergency Response Plans (ERPs) – tools that you can use to improve security at your system.

Additional copies of this guide may be obtained by calling the Safe Drinking Water Hotline at (800) 426-4791. You may also download the guide from EPA's Water Security Web site at <http://epa.gov/safewater/watersecurity>.

Your state (see box below) can provide additional security-related material and help you implement appropriate security measures at your water system. State contact information can be found in Appendix A. Drinking water industry associations and technical assistance providers also are actively involved with water security issues. See "Where Can I Find Additional Help?" on page 34 for their contact information.

Please note that the term "state" is used in this guide to refer to your Drinking Water Privacy Agency. The Privacy Agency for most systems is the State Drinking Water Agency. However, the Privacy Agency for systems located in the Navajo Nation is the tribal office. The Privacy Agency for systems located on other tribal lands, in the State of Wyoming, or in the District of Columbia is the EPA regional office.



# What Will I Learn?

Part of providing safe drinking water is protecting your system from various threats and preparing for emergencies. Everyone involved in water system ownership, management, and operation – owners, operators, board members, and local officials – has a responsibility for water system security. If you are part of any of these groups, this guide will help you by:

- Explaining what Vulnerability Assessments (VA) and Emergency Response Plans (ERP) are
- Describing the main activities and steps involved in completing VAs and ERPs
- Identifying user-friendly tools, templates, software, and checklists that can help you work through your VA and ERP

In this guide, you will learn about drinking water security initiatives and how to take practical actions to improve security at your system. You will also learn how to help ensure that your system is prepared to handle an emergency.

## What Are Systems Serving More than 3,300 Persons Doing?

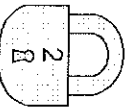
In response to the 2001 terrorist attacks, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act (Public Law 107-188) in 2002. This law requires that a CWS serving more than 3,300 persons conduct a VA. A copy of the VA must be sent to EPA according to a schedule specified in the law. CWSs serving more than 3,300 persons must also prepare or revise an ERP and certify to the EPA Administrator that the plan has been completed within 6 months of completing the VA. The ERP should incorporate the results of the VA and provide details on the actions a system will take to respond to an emergency.

Although the Act's requirements do not apply to systems serving 3,300 or fewer persons, it is important for systems of all sizes to understand their vulnerabilities and plan for emergencies. Systems serving 3,300 or fewer persons should consider completing a VA and an ERP to improve their preparedness and response capabilities.

It is important to note that some states have their own VA and ERP requirements. Be sure to check with your state to determine if there are requirements you must consider.

## Building a Team

You will need the help of everyone involved with your water system's ownership, management, and operations to improve security and emergency preparedness at your system. Build a team made up of water system operators, board members, and owners and make a team commitment to improving security and emergency preparedness at your water system.



# Why Is It Important to Improve Security and Prepare for Emergencies?

There are many threats that may put at risk your ability to provide a reliable and safe supply of water to your customers. Your system may face various man-made threats, both intentional and accidental, such as:

- Accidents (e.g., construction, traffic)
- Backflow
- Fire/arson
- Hazardous material releases
- Terrorism
- Vandalism

The idea that your system could be the target of terrorism may seem far-fetched to you. Man-made threats, however, are only some of many potential causes of emergencies at water systems. Natural disasters that might cause an emergency at your system include:

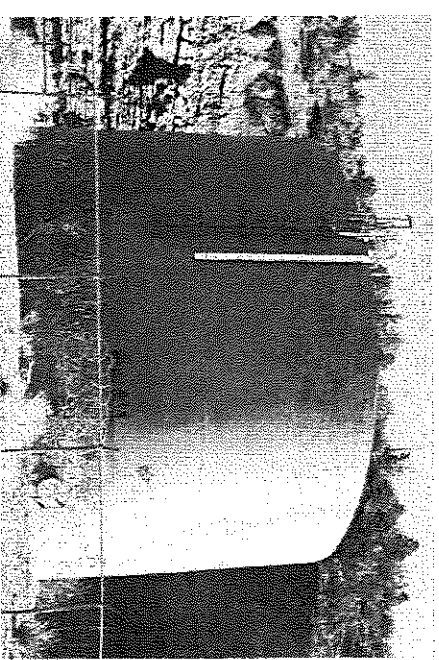
- Earthquakes
- Floods
- Forest and brush fires
- Hurricanes
- Severe cold weather/ice storms
- Tornadoes
- Waterborne disease outbreaks

Your responsibility is to protect your customers from the negative outcomes of these threats.

These outcomes could include:

- A shortage of drinking water
- Illnesses or deaths
- Public panic and fear of drinking the water from your system
- Costs of rehabilitating, rebuilding, or decontaminating your water system
- Long-term contamination of your water supply
- Interruption of firefighting capability
- Interruption of sanitary services

To deliver safe drinking water to your customers, you should have appropriate security measures in place, and you should know how to respond to an emergency. If your system is vulnerable to any threat, the health of your customers is at risk. If you are not prepared to respond to a crisis, the negative effects of the emergency will be magnified. Ignoring vulnerabilities and failing to properly plan for emergencies jeopardizes the safety of the water you deliver and the health of the people who depend on it. On the other hand, if you act now, you and your customers will have more confidence and peace of mind knowing that you are improving your system's security and emergency-response capability.



You will see this key throughout the guide. Pay special attention to these "key points," which highlight critical information for you and your system.



# What Is a Vulnerability Assessment?

A VA is a step-by-step evaluation of your system and its operations that assesses your ability to reduce the risk of different threats. A VA identifies weaknesses in your system's security and focuses on the types of possible threats that could keep you from providing a safe and reliable supply of water to your customers. Once your VA is completed, you should know which of your system's components might be vulnerable, and you will have begun to identify and prioritize the security upgrades and operational changes that will reduce risks to your system.

## HOW DO I CONDUCT A VULNERABILITY ASSESSMENT?

Identifying potential security threats and completing a VA might seem like an overwhelming challenge. You might think that you need an expert to properly evaluate your system's security. This section, however, outlines a few basic steps that will allow YOU to examine the risks facing your system. Using this approach, along with available tools, you can evaluate your system's security and begin to address any problems or needed improvements – without the help of outside consultants or security experts. Build a team made up of the water system operator, board members, and owners. This team will help you develop a complete VA.

It is important to note that some states have their own VA requirements. Be sure to check with your state to determine if there are requirements you must consider. Your state can also be a good source of assistance if you have questions about VAs.

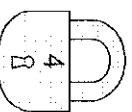
How you perform your VA is completely up to you and should reflect the needs and characteristics of your system. That said, there are six basic steps that everyone should follow when conducting a VA of their system (see the figure below).<sup>1</sup> The steps described in this section offer a general overview that will help you understand the activities necessary for an effective VA. Completing these steps will help you take a thorough look at the security risks your system faces.



To complete your VA, follow the six steps on the following pages. The graphic below will help you track the steps as you move from page to page. There are a number of worksheets, checklists, and other aids that can help you conduct a VA and accomplish these six basic steps; these tools are listed in "Where Can I Find Additional Help?" on page 34.

1. Evaluate System → 2. Identify Threats → 3. Consider Consequences → 4. Assess Likelihood → 5. Evaluate Measures → 6. Plan Action


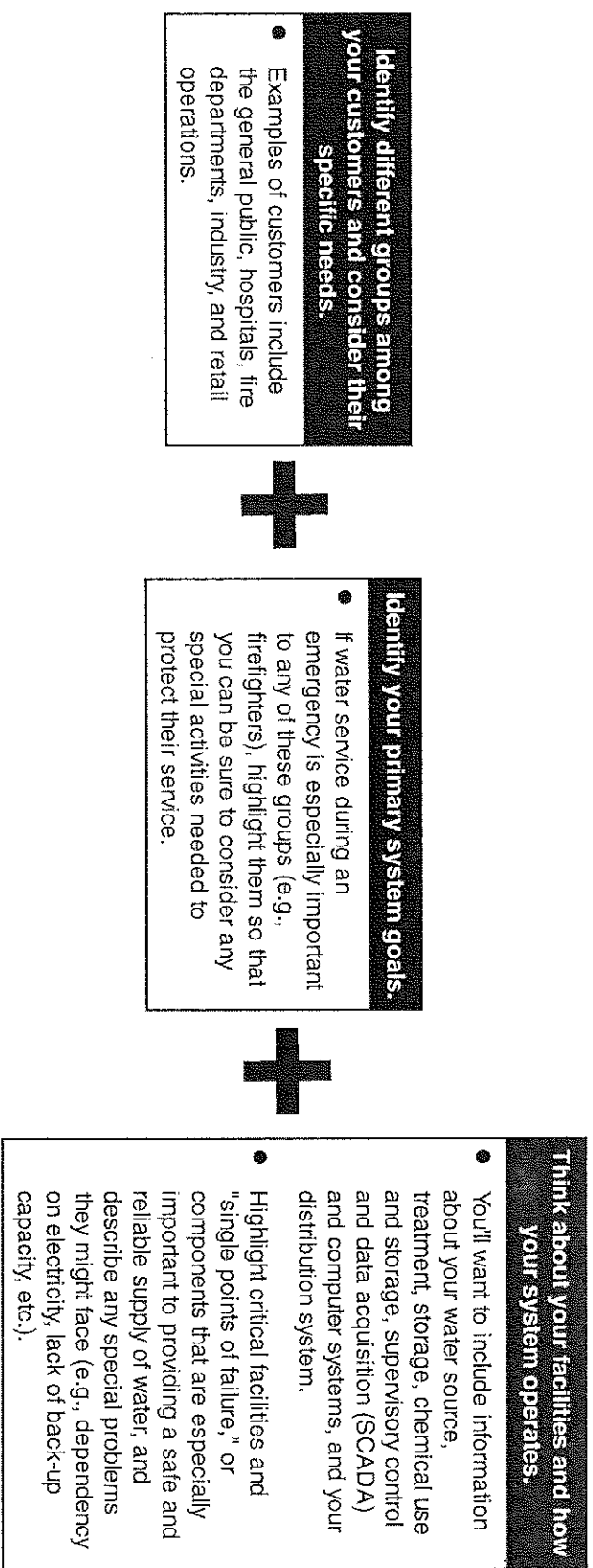
<sup>1</sup> These six steps are based on the six basic elements listed in *Vulnerability Assessment Factsheet*, EPA Office of Water (EPA 816-F-02-005), November 2002.



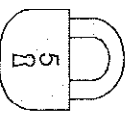
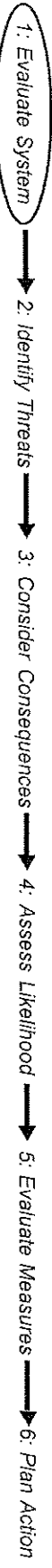
# VA Step 1

## YOUR SYSTEM AND ITS COMPONENTS – KNOWING AND EVALUATING CRITICAL RELATIONSHIPS

In this step you should think about your entire water system, including your primary goals, the customers you serve, and your system's components. To tackle this step, you should:



Although you may feel that you already are familiar with your system and how it works, evaluating each system component (including system personnel and water source) both independently and as part of overall system operations is the key to identifying its possible weaknesses. It is important to identify "single points of failure" in the system, or system components or processes that, if they failed, would interrupt the system's ability to supply reliable, safe water. It is also especially important for you to identify your critical customers (e.g., hospitals, fire departments), services, and components to help you prioritize your activities. It is important to provide yourself with an accurate picture of your system in this step. The rest of the VA process relies on this information!





## VA Step 2

### IDENTIFY POSSIBLE THREATS TO YOUR SYSTEM

The second step of your VA gives you the chance to identify the types of threats that could disrupt your system's ability to provide a reliable and safe supply of water. To complete this step, you should:

Look at the critical system facilities and components that you identified in VA Step 1 and think about whether a threat could realistically harm each of them. At a minimum, you should consider the following components in your assessment:

- Source water
- Physical barriers
- Treatment facilities
- Storage facilities
- Distribution and transmission pipes
- Computers or other automated systems (e.g., SCADA)
- Use, handling, and storage of chemicals
- Knowledge base (e.g., water system operator)
- Operations and maintenance practices



Consider each possible threat and which part(s) of the system it would affect. Consider all types of threats, including:

- Physical damage to the system
- Contamination of water at any point in the system
- Release of chemicals
- Interruption of electricity
- Loss or destruction of critical information (e.g., stolen system schematics)
- Loss of computers or SCADA systems



Take the time necessary to think through all of the potential threats that could affect your system. Work with law enforcement officials to get a better idea of the threats you may face. By coming up with the most complete list you can, you will ensure that your VA considers as many risks as possible. Making sure you really understand where and how your system is vulnerable will help you tackle VA Step 3.

1: Evaluate System



2: Identify Threats



3: Consider Consequences



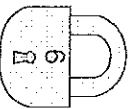
4: Assess Likelihood



5: Evaluate Measures



6: Plan Action



## VA Step 3

### CONSIDER POSSIBLE CONSEQUENCES

There are numerous negative outcomes that can result from threats against your system, and it's important for you to understand the possibilities. To complete this step, you should:

Look at the types of threats you identified in VA Step 2. Carefully consider:

- The type of threat (e.g., physical damage, water contamination)
- The critical component(s) or "single point(s) of failure" it could affect



Consider how each threat you identified could affect your system, from the smallest possible impact to the worst-case scenario. Include these factors in your thinking:

- Customers who will be affected and for how long
- The potential for illnesses or deaths
- The potential cost of the emergency (including repair, decontamination, or replacement costs for damaged components and revenue lost during a service outage)
- The impact of the emergency on public confidence in your system
- The long-term problems resulting from the emergency



Focus on the threats that would most harm your system's ability to provide a reliable and safe supply of water. You should be as thorough as possible in thinking about the possible consequences of any threat. The plans that you make to reduce risk in VA Step 6 will aim to prevent or reduce the likelihood of these consequences. The more thorough you are, the better your plan will be.

1: Evaluate System → 2: Identify Threats → 3: Consider Consequences → 4: Assess Likelihood → 5: Evaluate Measures → 6: Plan Action



## VA Step 4

### ASSESS THE LIKELIHOOD OF NEGATIVE CONSEQUENCES

This task can be very difficult because often there is too little information to make a good assessment. To help you do the best job you can, you should:

Contact your state, local law enforcement office, and public health officials to determine whether they have information on the types of threats that are most likely in your area.



Contact nearby water utilities to see what types of threats they might have faced.



Review your own incident reports from the past few years to better understand past security problems at your system.



Assessing the likelihood of specific intentional acts (as opposed to natural or accidental events) and their consequences will be challenging, but remember that figuring out which threats are most likely will determine how your system will reduce risk and plan for emergencies. Take advantage of all of the information you have and make sure you continuously re-evaluate the likelihood of specific acts and their consequences. Additional tools for gathering information are discussed in "Where Can I Find Additional Help?" beginning on page 34.

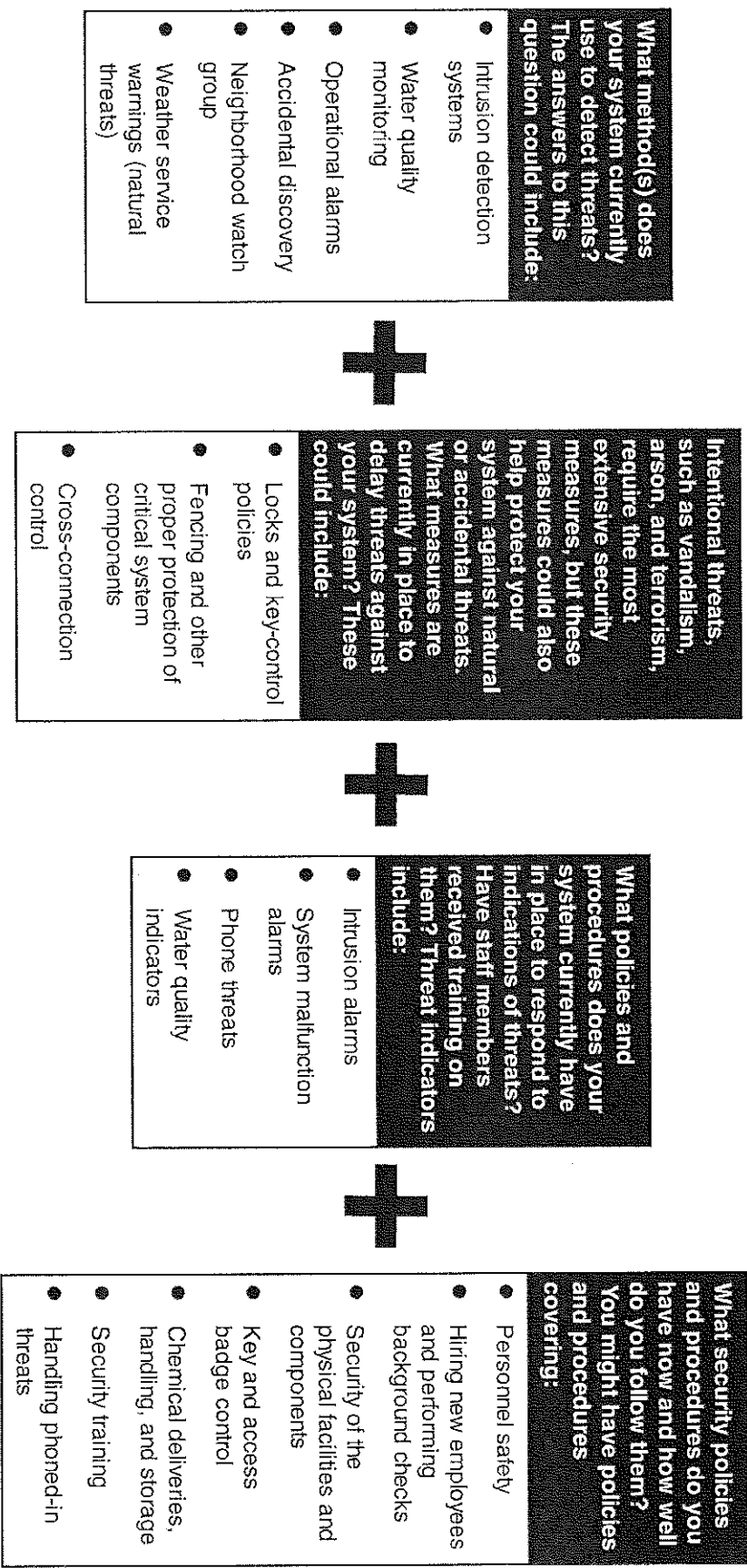
1: Evaluate System → 2: Identify Threats → 3: Consider Consequences → 4: Assess Likelihood → 5: Evaluate Measures → 6: Plan Action



# VA Step 5

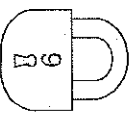
## EVALUATE EXISTING MEASURES

Before you can decide what additional measures need to be taken, you should evaluate the effectiveness of what you already do to protect your system. To complete this step, you should answer the following questions:



In answering these questions, you probably found that some system components are already adequately protected, while others are not. This information will help you prioritize the steps you take to protect your system. Be sure to distinguish between measures that are properly executed and well maintained and those that provide little or no protection because they are poorly executed or maintained. It is important that you do not overlook vulnerabilities caused by inadequate security measures or lack of knowledge about existing policies and procedures.

1: Evaluate System → 2: Identify Threats → 3: Consider Consequences → 4: Assess Likelihood → 5: Evaluate Measures → 6: Plan Action



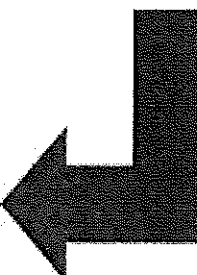
# VA Step 6

## PLAN TO REDUCE RISKS

Based on the assessment you've worked through in VA Steps 1 through 5, you can now develop a plan to reduce the risks facing your system. The analysis that you've done should allow you to identify your most urgent security needs and develop a plan that addresses these needs first. To develop your plan you should:

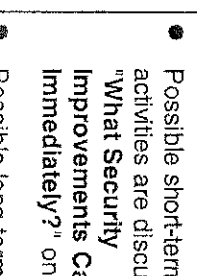
**Develop a list of recommended actions that will reduce your system's vulnerability to threats. Specific actions are discussed in more detail in later sections of this guide. In general, these actions fall into three categories:**

- Sound business practices, including changes to policies, procedures, and training
- System upgrades, including changes in equipment, infrastructure, or the way you operate your system
- Security upgrades, including changes that improve your ability to detect, delay, or deter threats against your system



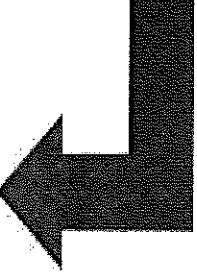
**Rank the actions by the urgency of the need that each action addresses.**

- Does it address a threat that is very likely or severe?
- Does it address an inadequate but critical existing security measure?



**Consider short- and long-term solutions to each of the vulnerabilities you identified in your assessment.**

- Possible short-term activities are discussed in "What Security Improvements Can I Make Immediately?" on page 12
- Possible long-term activities are discussed in "How Do I Maintain and Upgrade Security in the Long Run?" on page 27

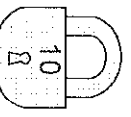
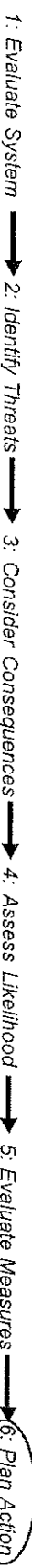


**Try to identify actions that will produce multiple benefits for your system or that can be made as part of other planned system upgrades, for example:**

- Improved treatment processes can reduce system vulnerabilities and enhance the day-to-day operation of your system



Take the time to review the work you did in VA Steps 1 through 5. This will help to ensure that your plan considers all possible weaknesses and vulnerabilities. One final word of caution: your VA contains a lot of important and sensitive information—keep it secure, and keep a second copy in a safe offsite location.



# What's Next?

Your VA has identified a number of system vulnerabilities, and you have begun to address those vulnerabilities with a plan to reduce risk. The next two sections of this guide provide more details on the two methods you can use to reduce risk:

1. You can enhance your system's security by taking direct measures that improve your ability to detect, deter, or delay threats to your system. The next section briefly describes these concepts and offers basic security improvements that can address vulnerabilities.
2. The results of a VA should be included in your system's ERP so that you can respond effectively should vulnerable parts of your system be threatened. "What Is an Emergency Response Plan?" on page 16 describes an ERP and takes you through a step-by-step process for preparing one.



# What Security Improvements Can I Make Immediately?

This section will help you develop a prioritized list of improvements that will reduce your system's vulnerability to threats. Although security improvements vary in complexity and cost, you will see in this section relatively inexpensive, practical changes that can be implemented immediately. You may not have to hire consultants or invest in top-of-the-line technology to act right now and increase the protection of your customers at a very reasonable cost.

The basic security measures described in this section will help improve your ability to **DETECT**, **DETER**, and **DELAY** security threats (see circles below).

Because many water systems share common vulnerabilities, there are a number of solutions that most systems should consider. Several common security actions are described on the pages that follow. These security actions tend to focus on intentional threats or acts, but some improvements can produce several benefits and make your system more secure against other threats (e.g., accidents, natural disasters) as well.



Remember that some of the measures suggested on the following pages may not be needed at your system. Some might be more complex than you need; others might address vulnerabilities that you've already remedied. Look at your VA and choose the actions that remedy your system's highest priority security needs.

## Detect

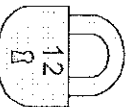
Know your water system and keep an eye on your facilities so you know when your security has been breached (e.g., patrol your water system perimeter, check locks and other points of entry for signs of tampering, establish a neighborhood watch program).

## Delay

Have multiple security measures in place to slow down anyone who is trying to harm your system (e.g., lock and alarm all points of entry, install "Jersey barriers," install security fences around facilities). Delaying an intruder gives you more time to detect a problem and more time to respond.

## Deter

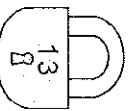
Make it very clear that your facilities are secure and closely watched and that the penalty for trespass is severe (e.g., require staff to display photo IDs at all times, post signs restricting entry to authorized personnel).



**Restrict access to critical water system components to authorized personnel only:**

One of the quickest and least expensive ways to dramatically increase the security of your system is to deny unauthorized personnel access to critical system components and "single points of failure." Supervised guests may be allowed, but unsupervised or uninvited guests could cause major problems, even if they do not intend to. And remember, disgruntled former employees have sabotaged systems in the past.

1. Require staff to display current photo IDs at all times.
2. Post signs restricting entry to authorized personnel.
3. Record who has keys and stamp keys "DO NOT DUPLICATE."
4. Change locks and access codes regularly.
5. Require personnel to wear uniforms or other identifying clothing.
6. Identify all system vehicles prominently.
7. Require vehicles to be locked at all times.
8. Remove critical information (e.g., source water maps, plans) from vehicles before parking them overnight.
9. Require terminated employees to return photo IDs, keys, access codes, and uniforms.
10. Install security fences around facilities.
11. Lock and consider alarming all points of entry: doors, windows, hatches, vents, and gates.
12. Lock all access points to finished water, even those within a locked or manned building.
13. Consider installing "Jersey Barriers" to block vehicle access to system facilities.
14. Remove objects that could be used to aid an intruder, such as ladders, overgrown shrubs, and large rocks, near windows and other points of entry.
15. Block access to elevated storage tanks by putting physical barriers around supports.





**Increase monitoring and oversight:**

Once access to your system is restricted and tight, back up that security by patrolling and monitoring your facilities so that you can detect any threats and intrusions. All water system personnel should know and practice their roles in protecting your system.

1. Patrol fence perimeters and the water system (periodically and randomly).
2. Check locks and other points of entry for evidence of tampering.
3. Check critical system components regularly.
4. Install adequate exterior lighting around critical components.
5. Clear fence lines of vegetation and overhanging branches.
6. Do not park vehicles where they will block your view of critical components.
7. Update your O&M manual to include evaluation of security systems.
8. Establish a neighborhood watch program with nearby neighbors.
9. Consider expanding monitoring parameters for raw and treated water (e.g., pH, color, odor). Develop and maintain a baseline value for each monitored parameter.

**Communicate and coordinate with local law enforcement:**

Local law enforcement is a very important resource that you should use to make your system more secure, but most police officers are not familiar with water system facilities or processes. A police presence might deter someone from threatening your system.

1. Give police officers a tour of your water system to familiarize them with key processes and equipment.
2. Arrange for periodic patrols of your facilities. Educate police about the types of suspicious activities that could take place throughout the water system.
3. Document suspicious calls and activities. Sample checklists and forms for documenting suspicious calls and activities are included in some of the tools found in "Where Can I Find Additional Help?" on page 34.

**Improve communication and security when dealing with vendors and suppliers:**

Even if you improve the security at your own facilities, chemical suppliers and repair persons are potential sources of vulnerability. The chemicals delivered and stored at your system deserve special attention because of the risk that they pose to system staff and the public if improperly handled or released. Safeguards will delay and deter threats to these dangerous chemicals.

1. Verify that your suppliers take precautions to ensure their products are not contaminated.
2. Ensure that all deliveries are made in the presence of water system personnel.
3. Keep a delivery log.
4. Store all chemicals in a secure area designated for storage only.
5. Keep tools and equipment needed to respond to an emergency onsite.
6. Accept only deliveries scheduled in advance.
7. Require drivers to show vendor-issued ID.
8. Verify IDs of communication company employees who have access to water supply structures for maintenance and repair of antennas and related equipment.

**Upgrade computer and records security:**

If your water system uses computers for operations or to store sensitive information, you should take some of these steps to make sure that information is protected and backed-up. By safeguarding your computers and paper records, you are delaying possible acts of sabotage.

1. Password-protect and virus-protect all computers. Change passwords and update virus protection programs regularly.
2. Back-up files, programs, and computers regularly.
3. Ensure that no sensitive information about your system is available on Web sites.
4. Store maps, records, and other important documents in a secure location.
5. Store backup copies of maps, records, and other important documents in a secure, off-site location.
6. Label all sensitive information "confidential" and require its return after projects are completed.
7. Keep a record of employees who accessed sensitive information and the dates on which they accessed the information.



Don't be intimidated by the length of these lists. Any security improvements you make will decrease the risks your system faces and will protect the health of your customers. By detecting, deterring, and delaying threats, you are reducing your system's vulnerabilities. Any risks you can't minimize through security measures should be addressed as part of your ERP, which is discussed in the next section.

# What Is an Emergency Response Plan?

An ERP is a written, well-thought-out series of planned actions that help you respond to emergencies of all types. An effective ERP for a small drinking water system makes use of the system's VA (see "What Is a Vulnerability Assessment?" on page 4) by addressing possible consequences of vulnerabilities identified in the VA. An ERP presents clear and logical steps to take in response to possible emergencies, designates persons responsible for specific actions, provides for training and planned practice exercises, and ensures effective coordination with first responders, law enforcement, and health officials.

If your water system does not have an ERP, you should prepare one. An ERP will help you organize your response to emergencies **before** they happen. An emergency can happen at any time, and any problem with the drinking water supply will become a top priority for you and the affected members of your community. An emergency could generate tremendous and immediate pressures on system operators, emergency response professionals, law enforcement, local health officials, and the public. A system that has an ERP and has practiced organized emergency response exercises will have a much better chance of minimizing the effects of emergencies. Therefore, having a well-planned system response to foreseeable emergencies makes good sense.

Preparing an ERP can take some effort. You should build an internal team of water system operators, board members, and owners to develop a complete ERP. The steps below can help you prepare a new ERP (or update your existing ERP). Keep in mind that the most effective ERP for your system will build on the findings of your VA. And remember that your state can be a good source of assistance should you have questions or need help in developing your ERP. Finally, because every system is different, you may need to modify the ERP development process described below to make it work for you.

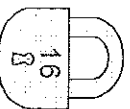
It is important to note that some states may have their own ERP requirements. Make sure you check with your state to see whether it has established specific requirements that you must address.

Keep in mind that the steps that follow offer only a general overview of the activities you should undertake to complete an ERP. There are a number of resources that offer detailed worksheets or other tools to help you. They are listed in "Where Can I Find Additional Help?" on page 34.



To complete your ERP, follow the five steps listed on the following pages. The graphic below will help you track the steps as you move from page to page.

1: Preparation → 2: Core Elements → 3: Putting it Together → 4: Action Plans → 5: Next Steps



# ERP Step 1

## ERP PREPARATION

In developing an ERP, you should identify and form partnerships with the people and organizations whose help your system will need in an emergency, including:

- Local police and fire departments
- Public health officials
- Local Emergency Planning Committees
- Local government/city managers
- State and federal agencies
- Nearby water utilities (for developing interconnections and mutual aid agreements)
- Health care providers
- Equipment suppliers
- News media

Forming effective partnerships with these organizations and individuals will help you better develop the core elements of your ERP and better coordinate emergency activities when the ERP is put into action. The partnerships also will help everyone become better prepared for emergency response.

Many communities have Local Emergency Planning Committees (LEPCs). A typical LEPC is made up of representatives of the municipal government, fire department, hospitals, environmental organizations, citizen groups, law enforcement and other emergency response officials, industry, and other interested parties. EPA maintains a database of over 3,000 LEPCs and their contact information. Visit <http://www.epa.gov/ceppo/lepclist.htm> to see whether your community has an LEPC. If it does, you should work especially closely with the LEPC when developing your ERP. Doing so will help ensure that your response to any emergency is coordinated as efficiently as possible.



Reach out to potential partners, describe your plans and objectives to them, and solicit their input and assistance. Helping your partners understand your goals and including your partners in the development of your ERP will improve your plan and help you develop more effective relationships with your partners.

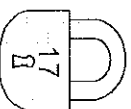
1: Preparation

2: Core Elements

3: Putting it Together

4: Action Plans

5: Next Steps



## ERP Step 2

### THE EMERGENCY RESPONSE PLAN – CORE ELEMENTS

A number of core elements should be included in any ERP, including yours. These elements will help ensure that your ERP and emergency response capabilities enable you to respond to any kind of emergency or threat. At the same time, the elements are flexible enough to ensure that your ERP meets the specific needs of your system. The core elements are discussed below.

#### Core Element 1: System-Specific Information

In an emergency, you should be able to provide basic technical information to personnel who will provide emergency assistance. In most cases, the organizations providing assistance will be those with which you formed partnerships under ERP Step 1. To ensure that you can provide the necessary system-specific information quickly and accurately, it is important that you include it as an easily accessible part of your ERP.



The basic information that you should include in this section of your ERP is:

- Owner name, operator name(s), and Public Water System Identification (PWSID) number, which identifies your system to your state and to EPA
- Population served and number of service connections
- Key information about critical system components (e.g., source water, treatment plant, water and chemical storage, and distribution system)
- How to isolate parts of your system when the need arises

1: Preparation



2: Core Elements



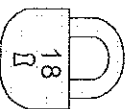
3: Putting it Together



4: Action Plans



5: Next Steps



## ERP Step 2 (Continued)

### Core Element 2: Roles and Responsibilities

You should specify roles and responsibilities for yourself and for your partners from outside of your system. First, you should designate an Emergency Response Leader (and a back-up) who will be the main point of contact and the primary decision maker during an emergency. Other system personnel and your partners also should understand their roles, responsibilities, and place in the chain of command. While it is important not to get bogged down in terminology and titles, it is also important that you and your Emergency Response Leader make sure all parties are clear about their roles.

Everyone also should be familiar with what is known as "command structure language." The Federal Emergency Management Agency (FEMA) and other federal agencies are using the National Incident Management System (NIMS) to coordinate emergency efforts. Your state and local government may also have adopted NIMS. The NIMS Incident Command System (ICS) is the standard organizational structure for all major domestic incidents. It helps to coordinate the efforts of many emergency responders. NIMS will enable responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size, or complexity. You can obtain more information on NIMS and the NIMS ICS from FEMA at <http://www.fema.gov/nims>.



At a minimum, your ERP should include the following basic information for your Emergency Response Leader and one back-up point of contact:

- Name
- Cell phone number (if applicable)
- Work telephone number
- Pager number (if applicable)
- Home telephone number
- Address

You should also identify other key individuals and partners and describe their roles, responsibilities, and places in the chain of command. Remember to communicate this information to your partners verbally and in writing.

1: Preparation

2: Core Elements

3: Putting it Together

4: Action Plans

5: Next Steps



## ERP Step 2 (Continued)

### Core Element 3: Communication Procedures - Who, What, and When

Timely communication with a variety of audiences is an essential component of your ERP. You should plan to notify three groups of people: system personnel, emergency response partners, and the public/news media.

- System personnel – Your Emergency Response Leader or backup should be the first person notified of an emergency. Other appropriate personnel should then be contacted.
- Emergency partners – These are the partners you identified in ERP Step 1. They should be contacted as necessary depending on the type of emergency.
- Public and news media – You should designate in advance a spokesperson who will handle public and media communications during an emergency. This spokesperson should not be the Emergency Response Leader. You should also develop a plan that your spokesperson can follow in communicating with the media and the public. This plan will help your spokesperson maintain a message that is clear, accurate, and easily understood by your audience. For more information about communicating with your water consumers, see “How Should I Communicate with My Customers?” on page 30.



Your ERP should include contact information for all individuals and organizations that fall into the groups discussed above. The list should include contact names, addresses, and all phone numbers for each contact. Update this list regularly to ensure that information is current and organize it to ensure that the highest priority calls are made first. States and technical assistance providers may have sample contact list templates you can use.

1: Preparation



2: Core Elements



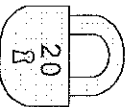
3: Putting it Together



4: Action Plans



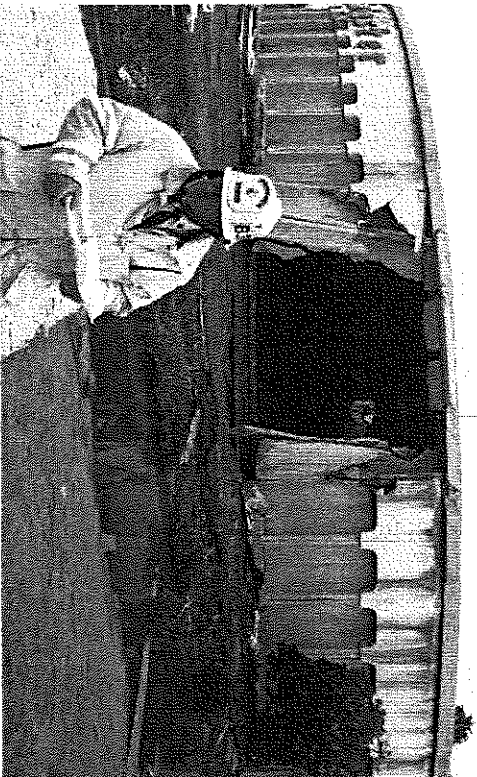
5: Next Steps



## ERP Step 2 (Continued)

### Core Element 4: Personnel Safety

Protecting the health and safety of your personnel is an important part of your ERP. In your ERP, you should write out basic safety precautions, identify the location of first aid supplies, and identify locations where personnel should meet in the event of an emergency. You should also make sure that your personnel are regularly trained in all of your safety procedures.



The personnel safety section of your ERP should, at a minimum, include the following:

- Directions for proper first aid and medical treatment
- Procedures for using and maintaining emergency response equipment
- Identification of evacuation routes and evacuation procedures
- Identification of assembly areas and procedures for locating all personnel



1: Preparation



2: Core Elements



3: Putting it Together



4: Action Plans



5: Next Steps



## ERP Step 2 (Continued)

### Core Element 5: Identification of Alternate Sources of Water

Your ERP should identify alternate sources of water that can address short-term (hours to days) and long-term (weeks to months) outages. There are a number of different options for short-term and long-term water supplies. Short-term options include bottled water from outside sources or retailers and bulk water from a variety of sources. Long-term options may include connecting your distribution system to a neighboring system. These alternate sources should be clearly identified in your ERP, and the agreements or arrangements for accessing the alternate sources should be clearly spelled out. Your source list and the agreements with these sources should be kept up to date.

You should also plan for the impact of various public health notifications, including "boil water," "do not drink," and "do not use" notices. The different steps you may need to take to deal with each of these notifications should be addressed clearly in your ERP. See "**How Should I Communicate with My Customers?**" on page 30 for guidance on notifying your customers and providing them with instructions on how to protect themselves.



The important thing to remember is to identify short-term and long-term alternate water sources in your ERP and to establish agreements with these partners before an emergency occurs. Your ERP should list your alternate water sources, along with the relevant contact information. You should also file copies of your agreements with your ERP.

### Core Element 6: Equipment and Chemical Supplies

Using the results of your system's VA, you should identify in your ERP where to find the equipment, repair parts, and chemicals needed in the event of an emergency.



This section of your ERP should include an updated list of:

- Current equipment
- Repair parts
- Chemical supplies
- Agreements with nearby systems to share portable generators and spare parts
- Contact information for any partners who can assist you with equipment and chemical supplies

1: Preparation



2: Core Elements



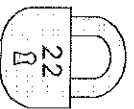
3: Putting It Together



4: Action Plans



5: Next Steps



22

1

## ERP Step 2 (Continued)

### Core Element 7: Property Protection

Protecting your facilities, equipment, and records is very important for getting your system running again after an emergency. Your ERP should clearly describe procedures to secure and protect important assets.



In this section of your ERP, you should consider describing how you will lock down your facilities, how you will control access to your facilities, and the steps you will take to protect other crucial property and records.

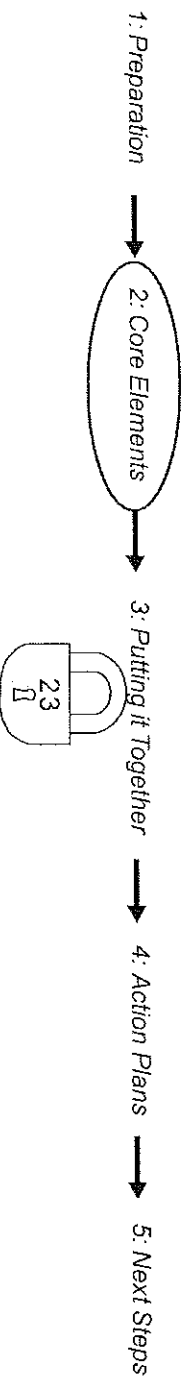
### Core Element 8: Water Sampling

Sampling is critical to determining whether the water your system produces is safe for your customers to drink and use. In your ERP, you should address water sampling and monitoring issues that could arise during an emergency. Water sampling and analysis is critical during the detection of an incident and during recovery from an incident. When developing your ERP, you should consult with your state on water sampling and monitoring requirements, including responsibility for water quality monitoring, during an emergency. Make sure you know what to do in an emergency before an emergency occurs.



You should include the following information in this section of your ERP:

- Proper sampling procedures
- The location and number of required samples
- Who is responsible for taking samples
- Contact information for laboratories or partners who will help analyze the samples and explain the results



## ERP Step 3

### PUTTING YOUR ERP TOGETHER AND KNOWING WHEN TO PUT IT INTO ACTION

Now that you've addressed the core elements of your ERP, you should organize and document that information in a useful way. If you have an existing ERP or other emergency management documents, now is the time to update all of them with the work you've done in ERP Steps 1 and 2. The goal, of course, is to produce a single, complete ERP that is accessible and easy to use. How you organize and document your ERP is up to you and should reflect the specific needs of your system; however, you should check with your state to see whether it has any requirements that might affect your finished ERP.

During this step you should also develop procedures for deciding when to put your ERP into action. Knowing when to use your ERP is as important as preparing and documenting it. In a natural emergency such as a tornado, earthquake, or flood, the decision to put your ERP into action is obvious. This type of emergency is easy to confirm.

It is more difficult to decide when to put your ERP into action when it comes to intentional acts. Here, the decision is critically important. While it is essential that you pay attention to any threat, you need to carefully think through and document a process to screen out hoaxes and avoid false alarms. During each threat incident, it is critical that you or your Emergency Response Leader consider three key questions:

- Is the threat possible?
- Is the threat credible?
- Has the incident been confirmed?



Remember, the answers to these questions will most likely differ with each incident and will probably determine what parts of your ERP need to be implemented. You or your Emergency Response Leader should exercise judgment when determining how to respond to a specific threat. More information about assessing threats is offered in some of the tools listed in "Where Can I Find Additional Help?" on page 34.

1: Preparation



2: Core Elements



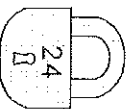
3: Putting it Together



4: Action Plans



5: Next Steps



# ERP Step 4

## ACTION PLANS – RESPONDING TO DIFFERENT TYPES OF EMERGENCIES

An Action Plan provides your system with quick approaches for responding to specific types of emergencies. The Action Plans that you develop should complement the general activities outlined in the core elements of your ERP and should be tailored to specific events (e.g., floods, tornadoes). Action Plans should be short and concise “rip and run” documents that can be detached from your ERP and taken into the field by emergency responders. The activities listed in the Action Plans should complement actions already initiated under your ERP. You should develop Action Plans for intentional acts and for natural disasters and other significant events.

### Intentional Acts

Action Plans should cover the following incidents and threats of such incidents (e.g., hoaxes):

- Contamination
- Structural damage/physical attack
- Intentional hazardous chemical release
- SCADA, computer, or cyber attack

### Natural Disasters and Other Significant Events

You may want to incorporate or modify existing plans to deal with a variety of natural disasters and other significant events. If you don't have existing plans, it makes sense to develop new plans to cover such events that may affect your system, including:

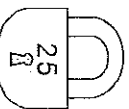
- Fire
- Flood
- Hurricane and tornado
- Severe weather (snow, ice, temperature, lightning, drought)
- Earthquake
- Electrical power outage
- Mechanical failure
- Water supply interruption
- Contaminated water treatment chemicals
- Accidental hazardous spill/release
- Construction accidents
- Personnel problems (loss of operator, medical emergencies)

Remember, your Action Plans should be clear, concise, and accessible. They should be well organized to make sure that the proper Action Plan can be found quickly by the staff members who need it. Your Action Plans should include the following basic information:

- Special notification requirements
- Special response steps necessary for the specific type of emergency
- Recovery actions to bring your system back into operation
- Remediation actions needed to make sure your system is fully restored



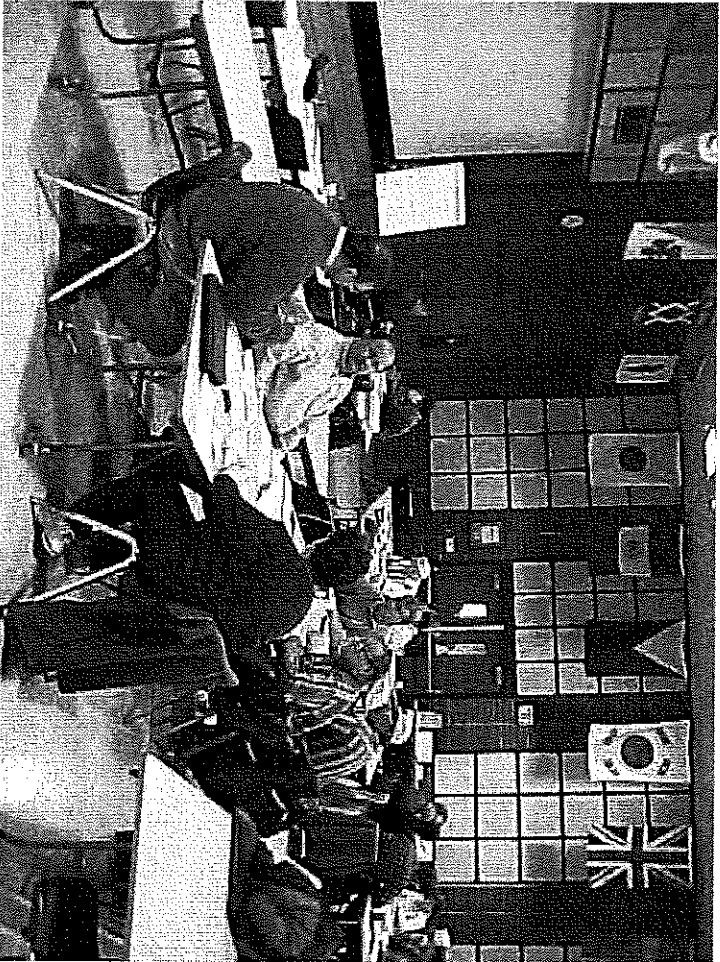
1: Preparation → 2: Core Elements → 3: Putting it Together → 4: Action Plans → 5: Next Steps



## ERP Step 5

### NEXT STEPS

Completing your written ERP is only the first step in making sure that your system is prepared to deal with an emergency. Your ERP should be a "living" document that you review and update regularly to make sure that all of your information is correct and up to date. Training in how to use your ERP is just as important as developing and updating it; even the best ERP will be difficult to implement during an emergency if people do not know their responsibilities. You should regularly practice implementing your ERP. Orientation exercises, table-top workshops, functional exercises, and full-scale drills are all ways in which you can help to make sure that your well-planned ERP is executed properly and efficiently when a real emergency arises. You can find more information about these training exercises in the tools listed in "Where Can I Find Additional Help?" on page 34.



1: Preparation



2: Core Elements



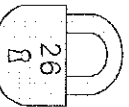
3: Putting it Together



4: Action Plans



5: Next Steps



# How Do I Maintain and Upgrade Security in the Long Run?

Completing your VA and ERP does not mean you have reached the finish line; a lapse in security and preparedness can be disastrous. You should continually assess your weaknesses, upgrade your system's security, and plan for unforeseen events. You should regularly reassess your vulnerabilities and revise your ERP as threats and personnel change. Remember to regularly practice implementing your ERP, especially if you make changes to it.

## Re-examine Your Vulnerabilities

Part of your long-term security strategy should be to re-evaluate your vulnerabilities. Ask your state if it has changed any of its security requirements. Your state is also a great resource for finding the latest information available on system vulnerability and security. Perhaps a new threat has emerged in your area, a new security measure is available, or new funding programs have been created. In addition, you should continue to train staff members so they understand the system's vulnerabilities and their roles in keeping the system secure.

## Neighborhood Watch Program

From "BexarMet Recruits Customers for Community Watch Program," *Willson County News*, February 12, 2003:

In February 2003, The Bexar Metropolitan Water District (BexarMet) in Texas began asking customers who live near water facilities to keep a watchful eye on any unusual activity. Participants were asked to call BexarMet any time of the day or night if they observed suspicious activity around a water facility.

Customers of BexarMet who live near water facilities received a letter requesting their assistance. The letters outlined the program and identified situations when residents should call 911 or BexarMet dispatchers. In addition, volunteers were given magnets with the phone number of BexarMet dispatchers. Pablo and Angelita Gallegos were the first volunteers. They live near a water storage tank and see the program as a good step forward. "We're here all the time," said Pablo Gallegos, "and whenever I see something, I'll call because we like to help."

## Upgrade Your Security

Besides keeping your understanding of your system's vulnerabilities current, you might continue to reduce risks by implementing security upgrades that are more costly or take more time to put in place. As your vulnerabilities change, you might need new security upgrades. The table below lists some long-run security measures that can detect, deter, and delay threats.

Remember that upgrading your security may also benefit other areas of your system operation. For example, properly sealed wells provide source water protection, backflow prevention programs improve the quality of water you deliver to your customers, and increased knowledge of your system can lead to improved technical, financial, and managerial capacity.

### Upgrade Security Policies:

1. Screen all potential employees through a job application, professional references, and a background check.
2. Develop a procedure to deal with public information requests.
3. Develop a procedure to receive notifications of suspected disease outbreaks immediately after their discovery by local health agencies.
4. Create a procedure to advise the community of contamination immediately after its discovery.
5. Put in place a procedure to respond immediately to customer complaints about a new taste, odor, color, or other detectable change in water quality.
6. Implement policies regarding access to critical information.
7. Develop and implement computer security policies.
8. Use security warnings and bulletins provided by state, federal, and non-governmental agencies or organizations.

### Upgrade Physical Security:

1. Replace critical doors and hinges that aren't constructed of heavy-duty reinforced material.
2. Make sure hinges on exterior doors are located on the inside of the building.
3. Make sure windows are bolted and reinforced with wire mesh or iron bars.
4. Require authorization and backflow prevention assemblies if a hydrant is used for any purpose other than fire fighting.
5. Implement a backflow prevention program.
6. Properly seal wellheads.
7. Make sure vents and caps are properly installed and cannot be removed.
8. Cap all abandoned wells.
9. Install fencing around your surface water source(s).
10. Install valves that allow you to isolate your storage tank.
11. Lock priority fire hydrants to deter contamination (should be done in consultation with fire department).
12. Install a sampling tap on each storage tank to detect contamination.
13. Monitor and maintain positive pressure in your distribution system.
14. Properly protect your computer equipment.
15. Keep your system illuminated.

## Update Your ERP

In addition to minimizing the risks posed to your customers, you should continue to prepare for emergencies. You should re-examine your ERP, especially as your system and its vulnerabilities change, so that you can respond to a crisis. Make sure that you do not let the relationships and communication channels that you've built deteriorate over time. If possible, you should conduct drills regularly to make certain that your system is as prepared as it can be for an emergency.

### Threat Response

From Daniel Borunda, "Utilities Take Steps to Protect Water Supplies," *El Paso Times*, November 23, 2003:

In September 2003, system managers at Las Cruces Water Utilities (TX) emptied a city water tank after an alarm signaled a break-in. Lacking a means to quickly determine if the water was contaminated, operators elected to drain the entire storage tank.

The system flushed and refilled the tank, returning it to service the following day. In the meantime, the system used backup tanks to supply users.

"Our system worked very well," Water Resources Administrator Gilbert Morales said. "There were a couple of areas that we found where our system could have been better, but this helped us identify those shortcomings and will help us respond more quickly in the future." The system was able to isolate the problem to the tank, and its customers were not at risk.

Remember that your VA and ERP contain sensitive information and should be stored in a safe place. In addition, copies should be kept in a secure off-site location. Access to your security information should be limited to staff members and to local and state officials on a need-to-know basis only.





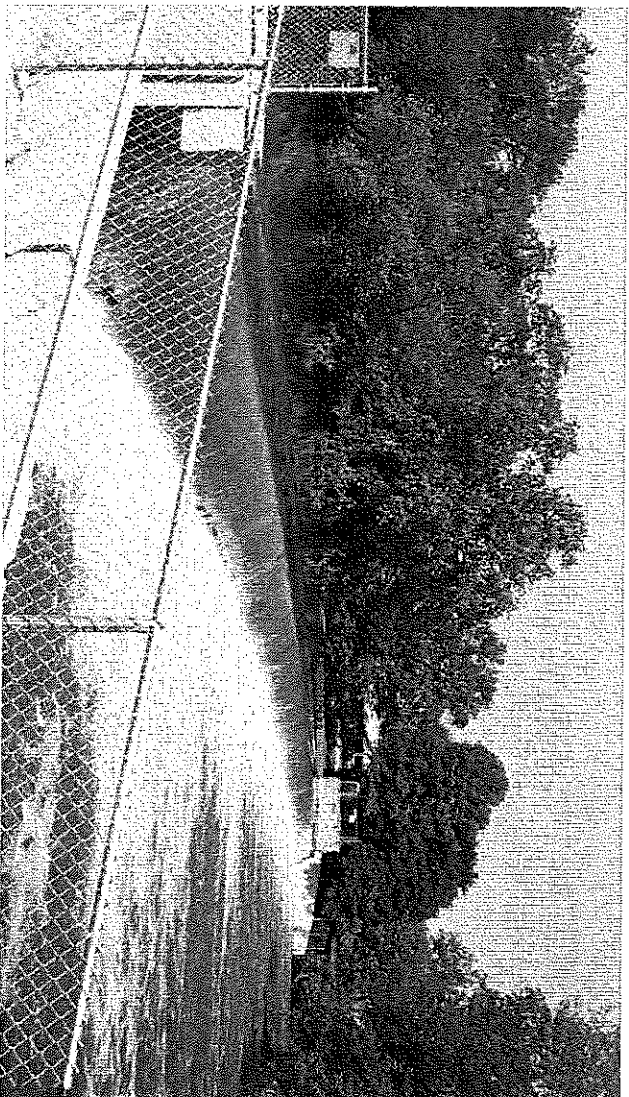
# How Should I Communicate with My Customers?

Good communication with your customers is an important part of your emergency response efforts. The people who depend on you for drinking water will need immediate, clear, and honest information during an emergency. Without this information, your customers may erroneously assume your water is unsafe and stop drinking it. Even worse, your customers may continue to drink contaminated tap water because they have not received the message that it is unsafe.

This section will help you develop a plan for communicating with your customers during an emergency or other crisis. There are several steps. The first step is to identify your critical customers, the customers who could be most affected by a problem with their water supply. The second step is to establish relationships with different groups in your community that could help you get your message out when you need to. The third step is to prepare a plan for notifying your customers during an emergency. The relationships you built during the second step will help you do so quickly and efficiently.

## CRITICAL CUSTOMERS

In the event of an emergency, your critical customers will need to be alerted quickly and may require an alternate supply of water. Critical customers are those most vulnerable to poor-quality water and insufficient quantities of water. Among them are children, the elderly, and the sick, as well as important institutions such as fire departments, hospitals, and power plants. You should establish communication channels with these customers now so they can be alerted at the first sign of an emergency.



## BUILDING RELATIONSHIPS FOR EFFECTIVE COMMUNICATION

Once you better understand whom you need to notify, you should build relationships and plan how you will distribute critical public health information during an emergency or other crisis. These decisions can and should be made long before you face an emergency so that you are prepared to act quickly and effectively. Your emergency communication will only be as strong as the relationships you build before a crisis.

You should build relationships with local media outlets, including radio stations, television stations, and newspapers. Your local media are important because they may be the easiest and quickest way for your system to notify the public. They are also less likely to exaggerate or misreport an event if they understand the issues ahead of time. You should designate a spokesperson in advance who will handle media relations during an emergency. This spokesperson should NOT be the Emergency Response Leader. Even before an emergency arises the system spokesperson should meet with local media representatives to determine exactly what information they will need, how best to get it to them, and when they will need it to meet their deadlines. Using this input, you should develop a plan for communicating with the media that your spokesperson can follow during an emergency.

Existing community networks, such as homeowners' associations, can also help you efficiently notify your customers during an emergency. It is important that you identify and test these networks before a threat or other emergency occurs. You might want to consider developing an e-mail distribution list or a calling chain so that you can notify the lead contact in each network as quickly as possible.

### Helpful Tips for Working with the Media

- At the top of the press release, write "PRESS RELEASE FOR PUBLIC SAFETY" to emphasize its importance.
- Answer questions as well as you can, and don't be defensive or afraid to say that you need to check on something if there is a question you cannot answer.
- Be sensitive to the fact that media representatives may have tight deadlines and other pressing needs.
- Monitor local media to check whether they are reporting the information accurately.
- Don't be upset if media coverage is not exactly as you would want. Politely inform the media outlet if important information is wrong or missing.
- If a media outlet will not publish or air your warning, you might need to buy ad space.

The information in this section is taken from EPA's "Public Notification Handbook" (EPA 816-R-00-010-2000). You can find more information on public notification in the handbook, available for downloading at <http://www.epa.gov/safewater/pn.html> or from the Safe Drinking Water Hotline at (800) 426-4791.

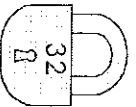
## PLAN FOR EMERGENCY NOTIFICATION

All of the preparation and relationships discussed to this point are important because they allow you to communicate quickly and effectively with your customers during an emergency. Don't forget that you might be communicating with your customers to minimize overreaction by reassuring them that their water is safe to drink despite the crisis. Here are some practical rules you should keep in mind when communicating with your customers:

- Be truthful and up-front
- Use simple language that everyone can understand
- Make notifications "short and sweet"
- Translate alerts for non-English speakers
- Clearly identify the name of your system and your service area, especially if your community is served by more than one water system
- Explain the exact nature of the emergency, the population at risk, actions that consumers should take, and alternative sources of water (if necessary)
- Provide a telephone number for more information
- Limit written warnings to one page designed to catch your customers' attention (bright colors and large text)

There are many ways you can communicate with your customers. The method you choose depends on which of your customers you are trying to reach, your available resources, and the urgency of the threat. Keep in mind that you will probably need to use a mixture of communication tools, since you may not reach all of your customers using only one method (e.g., some customers may not listen to the radio, watch TV, or read a newspaper). The options available to you make it that much more important that you plan ahead so that you are not overwhelmed during an emergency. A partial list of the communication outlets that you might use is found on page 33.

**!** **WARNING:** When communicating with customers, keep in mind that you want to provide enough information to enable them to act appropriately, but not so much that you increase the system's vulnerability to a threat. For instance, most customers will know if they live down the street from a water treatment facility, but they do not need to be informed of that facility's particular vulnerabilities.



## COMMUNICATION OUTLETS

**BROADCAST MEDIA** – Television and radio, if available in your community, may be the quickest way to inform the most customers. Check with your state to determine whether you can broadcast an alert over the federal Weather Radio alert system. See the box on page 31 for more tips on dealing with the media.

**NEWSPAPERS** – Depending on the urgency of the situation, you might want to work with the local paper. This outlet can be especially helpful when you need to keep customers updated during a prolonged crisis.

**POSTINGS** – Signs can be delivered to each business and residence or posted in public places. For instance, a campground may post signs in restrooms and at park entrances. If you have the time and staff, you can combine postings with word of mouth by trying to talk to customers as you post the alert. Remember to make the notices from materials that will hold up against wind and rain.

**PERSONAL NOTIFICATION** – Word of mouth is the oldest and potentially most time-consuming method. You may call, e-mail, and go door-to-door to notify customers. E-mail might be particularly effective in a university or office park, while calling may be the quickest method to notify a homeowners' association. Some systems may use an automatic dialing service to systematically call every customer and play a recorded message. Though more time-consuming, going door-to-door might be the best way to make sure that all your customers receive the alert.

In addition, you should use any other methods of communicating with your customers that you think will work well for your system. For example, broadcasting a public health warning from moving vehicles (such as a police vehicle) can be effective if your customers are at home or in a concentrated area, such as a beach. You should use whatever means you need to communicate with all your customers as quickly as possible.



# Where Can I Find Additional Help?

While improving the security and preparedness of your system takes a lot of work, it's an important step in protecting your system and your customers. Fortunately, many resources are available to help you accomplish the activities outlined in this STEP Guide. This section provides an overview of some of these sources of assistance. They include your state, EPA, drinking water associations, and technical assistance providers.

The first place you should look for help is your state (see Appendix A for contact information). States and EPA have been working together to identify ways to help systems address their security vulnerabilities and implement ERPs. Many state efforts, such as sanitary surveys, optimization programs, source water protection activities, and capacity development, enable the state to provide you with security technical assistance and possibly even funding. For instance, the state inspector conducting a sanitary survey of your system might be able to help you identify some of your system's vulnerabilities. Since many states consider security an essential part of technical and managerial capacity, you might also be able to take advantage of state financial and technical assistance programs.

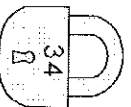
EPA can also be a source of information and assistance. The Agency has established a water system security page on its Web site (<http://epa.gov/safewater/watersecurity>). EPA provides an updated, comprehensive list of publications, information, and other resources for small and large drinking water systems. In addition, the Web site includes security resources geared specifically towards small system security, public involvement in water system security, and information sharing between water systems and public and private sector organizations.

Drinking water industry associations and technical assistance providers can be very important partners in efforts to improve system security and emergency preparedness. Several organizations have produced valuable security tools, ranging from simple how-to books to sophisticated software. In addition, these organizations are valuable sources of information on the experiences (both positive and negative) of other water systems, and they may be able to provide information on and evaluations of various security technologies. These organizations also offer training opportunities, as well as meetings, conferences, and forums where you can find the latest information on water system security.

## Major Providers of Technical Assistance to Drinking Water Systems

American Water Works Association	<a href="http://www.awwa.org/">http://www.awwa.org/</a> (800) 926-7387
National Rural Water Association	<a href="http://www.nwra.org/">http://www.nwra.org/</a> (580) 252-0629
Rural Community Assistance Partnership	<a href="http://www.rcap.org/contact.html">http://www.rcap.org/contact.html</a> (888) 321-7227
National Environmental Services Center	<a href="http://www.nesc.wvu.edu/nesc/nesc_about.htm">http://www.nesc.wvu.edu/nesc/nesc_about.htm</a> (800) 624-8301

The "Helpful Links" and "Alerts and Bulletins" sections that follow are good starting points for identifying the resources available to help you understand your security vulnerabilities, reduce your risks, and prepare for an emergency. You may also find it useful to hire a consultant to evaluate your system, help you address your vulnerabilities, or assist you in developing an ERP. Contact your state or technical assistance provider for a referral to someone who can help.



## HELPFUL HINTS

EPA's Security Web site provides links to a number of security tools, training opportunities, outreach materials, and other information. Visit <http://epa.gov/safewater/watersecurity> and click on the appropriate links for a list of all materials available. The following paragraphs list some of the materials you can find through the Web site:

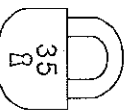
### VA Tools (click on "Vulnerability Assessments")

- **Self-Assessment Guide for Very Small (Serving Fewer than 3,300 Persons) Systems.** Developed by the Association of State Drinking Water Administrators (ASDWA) and NRWVA in consultation with EPA, this document is available from ASDWA's Web site ([www.asdwa.org](http://www.asdwa.org)). Scroll down to the middle of the page to view this document.
- **Video: Security Vulnerability Assessment for Water Systems.** EPA's Drinking Water Academy and the National Environmental, Safety, and Health Training Association (NESHTA) have produced a video for water systems serving fewer than 3,300 persons to aid in assessment of their vulnerability. You can obtain the video using the order form available at <http://www.neshta.org/PDFs/orderform.pdf>.
- **New England Water Works Association (NEWWA) Automated Security Survey and Evaluation Tool (ASSET).** The ASSET VA software is available from NEWWA by visiting [http://www.newwa.org/asset\\_software/index.php](http://www.newwa.org/asset_software/index.php).
- **Security and Emergency Management System (SEMS).** Contact an NRWVA affiliate in your area for more information on this combination VA and ERP software package.

### ERP Tools (click on "Emergency/Incident Planning")

- **Video: Emergency Response Plan for Water Systems Serving 3,301 – 10,000 persons.** NESHTA has developed a video for small water systems serving populations between 3,301 and 10,000 persons, although smaller systems may also find the video helpful. The video highlights the relationship between VA results and ERP development. You can download an order form at <http://neshta.org/Publications/Security.htm> or call (602) 956-6399 to place your order.
- **Emergency Response Tabletop CD-ROM Exercises for Drinking Water and Wastewater Systems (EPA-817-C-05-001).** This CD-based tool contains tabletop exercises to help train water and wastewater utility workers in preparing and carrying out ERPs. The exercises provided on the CD can help strengthen relationships between a water supplier and its emergency response team.

Items with EPA document numbers can be ordered through the Safe Drinking Water Hotline, (800) 426-4791.



Outreach Products (click on "Publications" and then on "Outreach Materials")

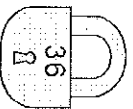
- **Water Watchers: We're All in This Together (EPA 810-F-03-006)**. This brochure for residents describes how they can help local authorities protect the water utilities in their communities.
- **Top Ten List: Water Supply Emergency Preparedness and Security for Law Enforcement (EPA 901-H-03-002)**. This list is also available as a poster (11" x 17") for display in local municipal facilities to help in coordinating the efforts of law enforcement, the water supply industry, and public health officials.
- **Water Security Posters**. EPA has developed a number of posters to help alert and educate communities about water security. In addition to the Top Ten List poster, "Report Suspicious Activity at Reservoirs, at Utilities, and at Water Mains" (EPA 810-F-03-001) and "Report Suspicious Activity - Watch Out! Help Out! Report It!" (EPA 810-F-03-002, 003, or 004), are available.

## **ALERTS AND BULLETINS**

Many states have begun implementing alert or bulletin systems to provide water systems with critical security information. Regular alerts and bulletins can be provided via e-mail or fax. Contact your state to see whether an alert or bulletin is available and to find out how you can join the system.

On a national level, the Water Security Channel (WaterSC) provides alerts and vital security information to key personnel at drinking water systems and states. WaterSC is a free e-mail notification system that can send notices to mobile devices configured to receive e-mail. WaterSC maintains a secure Web site that contains an archive of federal alerts, advisories, and bulletins. The service is free and systems can register at [www.watersc.org](http://www.watersc.org) or by calling 1-888-H2O-SC4U.

NRWA has developed a new free Rural Water Alert System (RWAS) to share security information with rural water systems. NRWA expects to launch RWAS by the end of 2005. The system will provide security information to rural water systems who may not subscribe to the WaterSC. RWAS will be comparable to the WaterSC in the type of information provided and will be accessible via the Internet. However, RWAS is not a rapid alert system. More information on RWAS is available through state NRWA affiliates.



# Appendix A: Safe Drinking Water Act Primacy Agencies

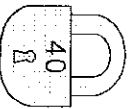
State Contact Information	Web site	Phone Number
<b>Alabama</b> Department of Environmental Management: Water Supply Branch	<a href="http://www.adem.state.al.us/WaterDivision/Drinking/DWMaint.htm">www.adem.state.al.us/WaterDivision/Drinking/DWMaint.htm</a>	(334) 271-7700
<b>Alaska</b> Department of Environmental Conservation: Drinking Water Program	<a href="http://www.state.ak.us/dec/eh/dw">www.state.ak.us/dec/eh/dw</a>	(907) 269-7647
<b>American Samoa</b> Environmental Protection Agency	<a href="http://www.asg-gov.com/agencies/epa.asg.htm">www.asg-gov.com/agencies/epa.asg.htm</a>	(684) 633-2304
<b>Arizona</b> Department of Environmental Quality: Safe Drinking Water Program	<a href="http://www.azdeq.gov/environwater/dw/index.html">www.azdeq.gov/environwater/dw/index.html</a>	(602) 771-2300
<b>Arkansas</b> Department of Health: Division of Engineering	<a href="http://www.healthylarkansas.com/eng/">www.healthylarkansas.com/eng/</a>	(501) 661-2623
<b>California</b> Department of Health Services: Division of Drinking Water and Environmental Management	<a href="http://www.dhs.ca.gov/ps/ddwem/technical/dwp/dwpiindex.htm">www.dhs.ca.gov/ps/ddwem/technical/dwp/dwpiindex.htm</a>	(916) 449-5577
<b>Colorado</b> Department of Public Health and Environment: Drinking Water Program	<a href="http://www.cdph.state.co.us/wq/drinking_water/drinking_water_program_home.htm">www.cdph.state.co.us/wq/drinking_water/drinking_water_program_home.htm</a>	(303) 692-3500
<b>Connecticut</b> Department of Public Health: Drinking Water Division	<a href="http://www.dph.state.ct.us/BRS/water/dwd.htm">www.dph.state.ct.us/BRS/water/dwd.htm</a>	(860) 509-7333
<b>Delaware</b> Health and Social Services: Division of Public Health	<a href="http://www.state.de.us/dhss/dph/about.html">www.state.de.us/dhss/dph/about.html</a>	(302) 744-4700



State Contact Information	Web site	Phone Number
<b>District of Columbia</b> Environmental Protection Agency Region 3	<a href="http://www.epa.gov/reg3wapd/drinkingwater">www.epa.gov/reg3wapd/drinkingwater</a>	(215) 814-2300
<b>Florida</b> Department of Environmental Protection: Drinking Water Program	<a href="http://www.dep.state.fl.us/water/drinkingwater/index.htm">www.dep.state.fl.us/water/drinkingwater/index.htm</a>	(850) 245-8335
<b>Georgia</b> Department of Natural Resources: Water Resources Branch	<a href="http://www.gaepd.org/">www.gaepd.org/</a>	(404) 657-5947
<b>Guam</b> Environmental Protection Agency: Water Programs Division	<a href="http://www.guamepa.govguam.net/programs/water">www.guamepa.govguam.net/programs/water</a>	(671) 475-1658
<b>Hawaii</b> Department of Health: Environmental Health Division	<a href="http://www.hawaii.gov/health/environmental/water/sdwb/index.html">www.hawaii.gov/health/environmental/water/sdwb/index.html</a>	(808) 586-4258
<b>Idaho</b> Department of Environmental Quality: Water Quality Division	<a href="http://www.deq.state.id.us/water/">www.deq.state.id.us/water/</a>	(208) 373-0194
<b>Illinois</b> Environmental Protection Agency: Bureau of Water	<a href="http://www.epa.state.il.us/water/index-pws.html">www.epa.state.il.us/water/index-pws.html</a>	(217) 785-8653
<b>Indiana</b> Department of Environmental Management: Drinking Water Branch	<a href="http://www.in.gov/dem/water/dwb/">www.in.gov/dem/water/dwb/</a>	(317) 232-8603
<b>Iowa</b> Department of Natural Resources: Water Supply Program	<a href="http://www.iowadnr.com/water/drinking/index.html">www.iowadnr.com/water/drinking/index.html</a>	(515) 725-0275
<b>Kansas</b> Department of Health and Environment: Bureau of Water	<a href="http://www.kdhe.state.ks.us/pws/">www.kdhe.state.ks.us/pws/</a>	(785) 296-5503
<b>Kentucky</b> Department for Environmental Protection: Division of Water	<a href="http://www.water.ky.gov/dw">www.water.ky.gov/dw</a>	(502) 564-3410
<b>Louisiana</b> Office of Public Health: Safe Drinking Water Program	<a href="http://www.oph.dhn.louisiana.gov/engineerservice/safewater/">www.oph.dhn.louisiana.gov/engineerservice/safewater/</a>	(225) 765-5038
<b>Maine</b> Maine Department of Health and Human Services: Drinking Water Program	<a href="http://www.state.me.us/dhs/eng/water/">www.state.me.us/dhs/eng/water/</a>	(207) 287-2070

State Contact Information	Web site	Phone Number
<b>Maryland</b> Department of the Environment: Water Supply Program	<a href="http://www.mde.state.md.us/programs/WaterPrograms/Water_Supply/index.asp">www.mde.state.md.us/programs/WaterPrograms/Water_Supply/index.asp</a>	(410) 537-3000
<b>Massachusetts</b> Department of Environmental Protection: Drinking Water Program	<a href="http://www.mass.gov/dep/brp/dws/dwshome.htm">www.mass.gov/dep/brp/dws/dwshome.htm</a>	(617) 292-5770
<b>Michigan</b> Department of Environmental Quality: Water Bureau	<a href="http://www.michigan.gov/dep">www.michigan.gov/dep</a>	(517) 373-7917
<b>Minnesota</b> Department of Health: Drinking Water Protection Section	<a href="http://www.health.state.mn.us/divs/eh/water/index.html">www.health.state.mn.us/divs/eh/water/index.html</a>	(651) 215-0770
<b>Mississippi</b> Department of Health: Water Supply Division	<a href="http://www.msdh.state.ms.us/msdhsite/index.cfm/44,0,76,html">www.msdh.state.ms.us/msdhsite/index.cfm/44,0,76,html</a>	(601) 576-7518
<b>Missouri</b> Department of Natural Resources: Water Protection and Soil Conservation Division	<a href="http://www.dnr.state.mo.us/wpscd/wpcp/index.html">www.dnr.state.mo.us/wpscd/wpcp/index.html</a>	(573) 751-1300
<b>Montana</b> Department of Environmental Quality: Public Water Supply Program	<a href="http://www.deq.state.mt.us/wqinfo/pws/index.asp">www.deq.state.mt.us/wqinfo/pws/index.asp</a>	(406) 444-4071
<b>Nebraska</b> Department of Health and Human Services: Public Water Supply Program	<a href="http://www.hhs.state.ne.us/enh/pws/index.htm">www.hhs.state.ne.us/enh/pws/index.htm</a>	(402) 471-0521
<b>Nevada</b> State Health Division: Safe Drinking Water Program	<a href="http://hndep.nv.gov/bsd/w/index.htm">http://hndep.nv.gov/bsd/w/index.htm</a>	(775) 687-6353
<b>New Hampshire</b> Department of Environmental Services: Water Division	<a href="http://www.des.state.nh.us/wseb/">www.des.state.nh.us/wseb/</a>	(603) 271-2153
<b>New Jersey</b> Department of Environmental Protection: Water Supply Administration	<a href="http://www.state.nj.us/dep/watersupply/">www.state.nj.us/dep/watersupply/</a>	(609) 292-5550
<b>New Mexico</b> Environment Department: Drinking Water Bureau	<a href="http://www.nmenv.state.nm.us/dwb/dwbtop.html">www.nmenv.state.nm.us/dwb/dwbtop.html</a>	(505) 827-1400

State Contact Information	Web site	Phone Number
<b>New York</b> New York State Department of Health: Bureau of Water Supply Protection	<a href="http://www.health.state.ny.us/nysdoh/water/main.htm">www.health.state.ny.us/nysdoh/water/main.htm</a>	(518) 402-7650
<b>North Carolina</b> Department of Environment and Natural Resources: Public Water Supply Section	<a href="http://www.denr.state.nc.us/pws/">www.denr.state.nc.us/pws/</a>	(919) 733-2321
<b>North Dakota</b> Department of Health: Division of Water Quality	<a href="http://www.health.state.nd.us/mf/">www.health.state.nd.us/mf/</a>	(701) 328-5211
<b>Ohio</b> Environmental Protection Agency: Division of Drinking and Ground Water	<a href="http://www.epa.state.oh.us/ddagw/">www.epa.state.oh.us/ddagw/</a>	(614) 644-2752
<b>Oklahoma</b> Department of Environmental Quality: Water Quality Division	<a href="http://www.deq.state.ok.us/WQDnew/index.htm">www.deq.state.ok.us/WQDnew/index.htm</a>	(405) 702-8100
<b>Oregon</b> Department of Human Services: Drinking Water Program	<a href="http://oregon.gov/DHS/ph/dwp/index.shtml">http://oregon.gov/DHS/ph/dwp/index.shtml</a>	(971) 673-0405
<b>Pennsylvania</b> Department of Environmental Protection: Office of Water Management	<a href="http://www.dep.state.pa.us/dep/deputate/watermgfwsm/WSM.htm">www.dep.state.pa.us/dep/deputate/watermgfwsm/WSM.htm</a>	(717) 772-4018
<b>Puerto Rico</b> Department of Health: Public Water Supply Supervision Program	<a href="http://www.epa.gov/region02/ceppd/prlink.htm">www.epa.gov/region02/ceppd/prlink.htm</a>	(787) 977-5870
<b>Rhode Island</b> Department of Health: Office of Drinking Water Quality	<a href="http://www.health.ri.gov/environment/dwq/index.php">www.health.ri.gov/environment/dwq/index.php</a>	(401) 222-6867
<b>South Carolina</b> Department of Health and Environmental Control: Drinking Water Program	<a href="http://www.scdhec.net/eqc/water/html/dwater.html">www.scdhec.net/eqc/water/html/dwater.html</a>	(803) 898-4300
<b>South Dakota</b> Department of Environment and Natural Resources: Drinking Water Program	<a href="http://www.state.sd.us/den/des/drinking/dwprg.htm">www.state.sd.us/den/des/drinking/dwprg.htm</a>	(605) 773-3754

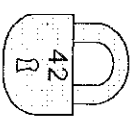


State Contact Information	Web site	Phone Number
<b>Tennessee</b> Department of Environment and Conservation: Division of Water Supply	<a href="http://www.state.tn.us/environment/dws/index.html">www.state.tn.us/environment/dws/index.html</a>	(615) 532-0191
<b>Texas</b> Texas Commission on Environmental Quality	<a href="http://www.tceq.state.tx.us/nav/utl_water/">www.tceq.state.tx.us/nav/utl_water/</a>	(512) 239-4691
<b>Utah</b> Department of Environmental Quality: Division of Drinking Water	<a href="http://www.drinkingwater.utah.gov">www.drinkingwater.utah.gov</a>	(801) 536-4200
<b>Vermont</b> Vermont Agency of Natural Resources	<a href="http://www.anr.state.vt.us/dec/watersup/wsd.htm">www.anr.state.vt.us/dec/watersup/wsd.htm</a>	(802) 241-3400
<b>Virgin Islands</b> Department of Planning and Natural Resources: Division of Environmental Protection	<a href="http://dpr.gov/vi/dep/home.htm">http://dpr.gov/vi/dep/home.htm</a>	(340) 773-1082
<b>Virginia</b> Department of Health: Office of Drinking Water	<a href="http://www.vdh.state.va.us/dw/index.asp">www.vdh.state.va.us/dw/index.asp</a>	(804) 864-7500
<b>Washington</b> Division of Environmental Health: Office of Drinking Water	<a href="http://www.doh.wa.gov/ehp/dw/">www.doh.wa.gov/ehp/dw/</a>	(360) 236-3100
<b>West Virginia</b> Bureau for Public Health: Department of Health and Human Resources	<a href="http://www.wvdhhr.org/oehs/eed/">www.wvdhhr.org/oehs/eed/</a>	(304) 558-6715
<b>Wisconsin</b> Department of Natural Resources: Bureau of Drinking Water and Ground Water	<a href="http://www.dnr.state.wi.us/org/water/dwg/">www.dnr.state.wi.us/org/water/dwg/</a>	(608) 266-0821
<b>Wyoming</b> EPA Region 8: Wyoming Drinking Water Program	<a href="http://www.epa.gov/region08/water/dw/home/wycon/wycon.html">www.epa.gov/region08/water/dw/home/wycon/wycon.html</a>	(303) 312-6812

# Appendix B: EPA Regional Contacts

To determine which region your state is in, visit <http://cfpub.epa.gov/watersecurity/stateinfo.cfm>.

US EPA Regional Contacts		
EPA Region 1	<a href="http://www.epa.gov/NE/eeco/drinkwater/dw-security.html">http://www.epa.gov/NE/eeco/drinkwater/dw-security.html</a>	(617) 918-1694
EPA Region 2	<a href="http://www.epa.gov/region2/water/">http://www.epa.gov/region2/water/</a>	(212) 637-3879
EPA Region 3	<a href="http://www.epa.gov/reg3wappd/">http://www.epa.gov/reg3wappd/</a>	(215) 814-5668
EPA Region 4	<a href="http://www.epa.gov/region4/water/">http://www.epa.gov/region4/water/</a>	(404) 562-9446
EPA Region 5	<a href="http://www.epa.gov/region5/water/">http://www.epa.gov/region5/water/</a>	(312) 886-0190
EPA Region 6	<a href="http://www.epa.gov/Arkansas/6wq/swp/security/">http://www.epa.gov/Arkansas/6wq/swp/security/</a>	(214) 665-2776
EPA Region 7	<a href="http://www.epa.gov/region7/security/index.htm">http://www.epa.gov/region7/security/index.htm</a>	(913) 551-7585
EPA Region 8	<a href="http://www.epa.gov/region8/compliance/security/secure.html">http://www.epa.gov/region8/compliance/security/secure.html</a>	(303) 312-7021
EPA Region 9	<a href="http://www.epa.gov/region9/water/">http://www.epa.gov/region9/water/</a>	(415) 947-3561
EPA Region 10	<a href="http://yosemite.epa.gov/R10/WATER.NSF/webpage/Water+Issues+in+Region+10">http://yosemite.epa.gov/R10/WATER.NSF/webpage/Water+Issues+in+Region+10</a>	(206) 553-1389



# Appendix C: Other STEP Documents

This guide is one in a series of Simple Tools for Effective Performance (STEP) documents for small drinking water systems. The STEP documents can be obtained from EPA by calling the Safe Drinking Water Hotline at (800) 426-4791 and requesting the document by its publication number. The documents can also be found at [www.epa.gov/safewater/smallsys/ssinfo.htm](http://www.epa.gov/safewater/smallsys/ssinfo.htm). Other titles in the series are:

- *Small Systems Guide to the Total Coliform Rule (TCR)*  
Publication number: EPA 816-R-01-017A  
Published: June 2001
- *Safe Drinking Water Act (SDWA) Regulation Overview Brochure for Small Systems*  
Publication number: EPA 816-R-03-017  
Published: September 2003
- *Complying With the Revised Drinking Water Standard for Arsenic: Small Entity Compliance Guide*  
Publication number: EPA 816-R-02-008A  
Published: August 2002
- *Asset Management Workbook*  
Publication number: EPA 816-R-03-016  
Published: September 2003
- *Strategic Planning Workbook*  
Publication number: EPA 816-R-03-015  
Published: September 2003
- *Taking Stock of your Water System: A Simple Asset Inventory for Very Small Systems*  
Publication number: EPA 816-K-03-002  
Published: October 2004