United States
Environmental Protection
Agency

Emergency Response Plan Guidance for Small and Medium Community Water Systems

to Comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002

This page intentionally left blank

Office of Water (4601M)
EPA 816-R-04-002
www.epa.gov/safewater/security
April 2004

Disclaimer: This document is provided as guidance only. It contains nationally recognized standards on the types of information that should be contained in an Emergency Response Plan (ERP). EPA recognizes that sections of this guidance may not be applicable to every Community Water System (CWS) and all potential situations may not be identified. It is each CWS's responsibility to evaluate the potential vulnerabilities related to their system and determine the appropriate responses. As site-specific needs dictate, this guidance can be modified.

Table of Contents

This page intentionally left blank

Introduction

What is the purpose of this document?

The purpose of this document is to provide guidance on developing or revising Emergency Response Plans (ERPs) for small- and medium-sized community drinking water systems. An ERP is a documented plan that describes the actions that a Community Water System (CWS) would take in response to various major events. A major event refers to:

- Credible threats, indications of terrorism, or acts of terrorism;
- Major disasters or emergencies such as hurricanes, tornadoes, storms, earthquakes, fires, flood, or explosion regardless of cause; and
- Catastrophic incidents that leave extraordinary levels of mass casualties, damage, and disruption severely affecting the population, infrastructure, environment, economy, and government functions.

On June 12, 2002, President Bush signed into law the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107-188, referred to as the Bioterrorism Act). In the Bioterrorism Act, Congress recognizes the need for drinking water systems to undertake a more comprehensive view of water safety and security. The Act amends the Safe Drinking Water Act and specifies actions CWSs and the U.S. Environmental Protection Agency (USEPA) must take to improve the security of the Nation's drinking water infrastructure.

CWS characteristics vary greatly, so CWSs should apply the information contained in this document to meet their particular needs and circumstances. This document should be used as a flexible template.

Why should a CWS develop or revise an ERP?

Protecting public health is the primary goal of community drinking water systems, and having an up-to-date and workable ERP helps achieve this goal in any crisis situation. The Bioterrorism Act amends the Safe Drinking Water Act (SDWA) by adding, among other requirements, section 1433. Section 1433(b) requires community water systems serving populations greater than 3,300 to either prepare or revise an ERP that incorporates the results of its Vulnerability Assessment (VA). The ERP must include "plans, procedures, and identification of equipment that can be implemented or utilized in the event of a terrorist or other intentional attack" on the CWS. The ERP also must include "actions, procedures, and identification of equipment which can obviate or significantly lessen the impact of terrorist attacks or other intentional actions on the public health and the safety and supply of drinking water provided to communities and individuals."

Who should use this document?

In using the terms "small and medium-sized" within this document, USEPA is referring to CWS which serve populations from 3,301 to 99,999. A CWS serving a population from 3,301 to 99,999 should use this document to either develop or revise its ERP and address findings from its VA. A VA is also a requirement for a CWS serving a population greater than 3,300 under the Bioterrorism Act. Completing a VA is a necessary step before a comprehensive ERP can be developed or revised.

Note: Any reference to "CWS," "you," or "I" in this document is a reference to a CWS serving a population from 3,301 to 99,999 unless otherwise noted.

How do I use this document?

This document is divided into five sections that will assist you in developing or revising your ERP. The sections are:

I. **Before You Begin Developing or Revising Your ERP:** Describes steps and actions you would need to complete before you could successfully develop or revise your ERP.

II. **Emergency Response Plan—Eight Core Elements:** Describes core elements that are universal to any ERP. If you are beginning to develop your ERP, you should use this section as a general template. If you have an existing ERP, you can use this section to check if your existing ERP is comprehensive and complete. The core ERP elements are:

- ❑ System Specific Information;
- ❑ CWS Roles and Responsibilities;
- ❑ Communication Procedures: Who, What, and When;
- ❑ Personnel Safety;
- ❑ Identification of Alternate Water Sources;
- ❑ Replacement Equipment and Chemical Supplies;
- ❑ Property Protection; and
- ❑ Water Sampling and Monitoring.

III. **Putting Your ERP Together and ERP Activation:** Describes steps and issues you need to address once you have all your core ERP elements in place and how to put these elements together into a single comprehensive plan. Additionally, you will need to understand the types of events that will trigger use of the plan. An effective ERP now needs to address intentional acts of terrorism as well as other emergencies and natural disasters. Planning for these events makes developing, updating, and deciding to activate the ERP more challenging than in the past.

IV. **Action Plans:** Describes how Action Plans (AP) are developed and used to tailor emergency response actions to specific incidents or events. Under the Bioterrorism Act, you are required to address the findings of a VA in an ERP. An AP identifies the steps to take to address specific vulnerabilities and respond to a given incident.

V. **Next Steps:** Describes steps to take after completing an ERP, for example, submitting a certification to EPA, conducting training, and updating your plan.

Will my ERP contain sensitive information?

Your ERP may contain sensitive information, so you should consider steps you need to take to ensure the security of your ERP. Sensitive information should be placed in appendices, or in sections that are not readily available to unauthorized personnel. The ERP, however, should be easily accessible to authorized personnel and should be easily identifiable during a major event. Steps taken to limit access by unauthorized persons should consider local and state Freedom of Information Act (FOIA) laws. Alternatively, you can opt to make your ERP general in nature so that everyone can use it and not include specific information about system vulnerabilities.

A secure copy of your ERP should be maintained in an off-premises location in the event that your primary copy cannot be accessed.

I. Before You Begin Developing or Revising Your ERP

What steps do I need to take before I start to develop or revise my ERP?

Before you begin to develop or revise your ERP, there are two steps that you need to take. First, you need to have completed a VA as required under the Bioterrorism Act. The findings from your VA will be addressed in your ERP through specific Action Plans (AP), which are discussed in detail in Section IV, "Action Plans."

Second, you should identify and coordinate with first responders and ERP partners who will help and assist you during a major event. As required by Section 1433(b) of the Bioterrorism Act, partners should include, to the extent possible, Local Emergency Planning Committees (LEPCs) established under the Community Right-to-Know Act such as local law enforcement departments, fire departments, health departments, local environmental agencies, hospitals, broadcast and print media, community groups, and nearby utilities. Other partners could include State and Federal agencies, and laboratories. **Figure I-1** shows local entities (in the shaded area) as well as State and Federal entities (in the white area) that may assist you during a major event. EPA strongly recommends that you consult with local and State entities as you develop your ERP. The purpose of the consultation is to form partnerships and seek advice. Through these partnerships, each party knows and understands its role and responsibilities in emergency situations. These partnerships help everyone respond better to an emergency.

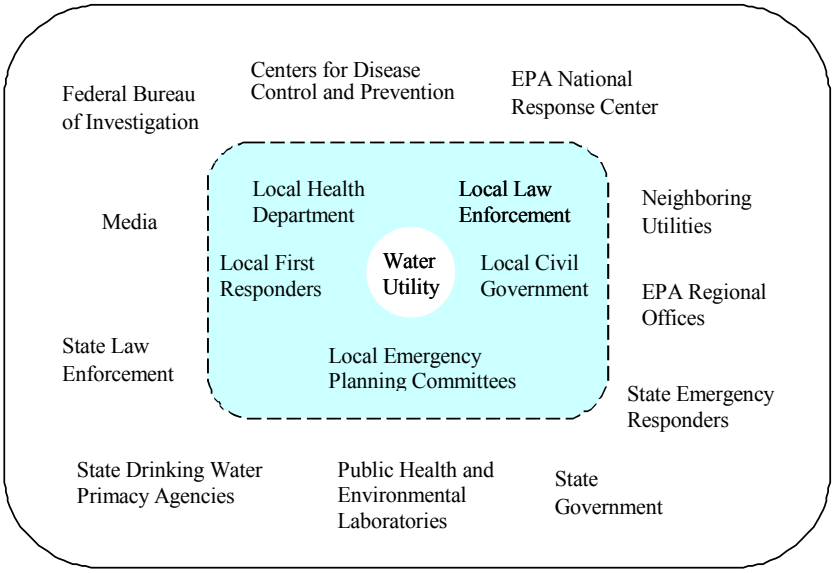

Figure I-1. Overview of ERP Partners

Are there any tools, training courses, or guides that can assist me in either developing or revising my ERP?

Emergency response has been around for quite some time, so many tools, training courses, and guides already exist on the topic of developing an ERP. Possible resources on how to develop or revise sections of your ERP include the following (see also the "References and Links" section of this document):

- ERP material from other Federal agencies [for example, Incident Command System information from the Federal Emergency Management Agency (FEMA) and the Department of Homeland Security (DHS)];

- State ERP guidance;
- Risk Management Plans as required by the Clean Air Act section 112(r) (if applicable to your CWS);
- Water association ERP guides and training courses; and
- USEPA's Response Protocol Tool Box (for water contamination incidents) http://www.epa.gov/safewater/security/index.html#emergency.

Many of the above resources address specific topics or subject areas in greater detail than this guidance document. Again, the purpose of this guidance document is to help produce a single comprehensive ERP that would meet the response needs of a variety of events. Use ERP resources available to you to help build a single and comprehensive ERP that includes response actions to terrorist or other intentional events.

II. Emergency Response Plan—Eight Core Elements

What does USEPA mean by "ERP core elements"?

Core elements form the basis, or foundation, for responding to any major event. USEPA has identified eight core elements common to an ERP that you should plan to utilize or bring to bear during water emergencies.

1. System Specific Information;
2. CWS Roles and Responsibilities;
3. Communication Procedures: Who, What, and When;
4. Personnel Safety;
5. Identification of Alternate Water Sources;
6. Replacement Equipment and Chemical Supplies;
7. Property Protection; and
8. Water Sampling and Monitoring.

If you already have an ERP in place and just need to revise it, use the following sections to check if you are missing any key information. If you are just beginning to develop your ERP, use the following sections as a general template for what should be included in your ERP. Use the following sections to develop or revise your ERP according to your needs.

A. System Specific Information (Element 1)

Why do I need to keep system-specific information on hand?

During a major event, you need to have basic technical information readily available for your personnel, first responders, repair contractors/vendors, the media, and others. The information needs to be clearly documented and readily accessible so your staff can find and distribute it quickly to those who may be involved in responding to the major event. The location of critical documents, such as distribution maps, detailed plan drawings, site plans, source water locations, and operations manuals, should be identified and readily available during a major event. You should have located and reviewed much of this information while conducting your VA, so the ERP should only need to identify it.

What basic information do I need to have?

Basic information that may be presented in an ERP includes:

1. Public Water System (PWS) ID, Owner, Administrative Contact Person, Alternate Administrative Contact Person;
2. Population Served and Service Connections;
3. Distribution Map;
4. Pressure Boundary Map;
5. Overall Process Flow Diagrams;
6. Site Plans and Facility "As-Built" Engineering Drawings
    a) Pumping and Storage Facilities
    b) Reservoirs and Retention Facilities
    c) Water Treatment Facilities
    d) Booster Pump Stations
    e) Pressure-Regulating Valve (PRV) Sites
    f) Distribution System Process and Instrumentation Diagrams (P&ID)
    g) Equipment and Operations Specifications
    h) Emergency Power and Light Generation
    i) Maintenance Supplies
7. Operating Procedures and System Descriptions including back-up systems and interconnections with other systems;
8. Supervisory Control and Data Acquisition (SCADA) System/Process Control Systems Operations;
9. Communications System Operation;
10. Site Staffing Rosters and Employees' Duties and Responsibilities; and
11. Chemical Handling and/or Storage Facilities and Release Impact Analyses (i.e., chemical releases into air or water).

It is important to note that not all of this technical information may be needed to document how you operate. The level of technical documentation should reflect the complexity of your CWS.

B. CWS Roles and Responsibilities (Element 2)

What roles and responsibilities do I need to define?

You should designate an Emergency Response Lead (ER Lead) and Alternate ER Lead. The ER Lead will be the main point of contact and decision-maker during a major event. This person will have responsibility for evaluating incoming information, managing resources and staff, and deciding on appropriate response actions. This person will also have the responsibility of coordinating emergency response efforts with first responders. The ER Lead should be heavily involved in forming the partnerships described in Section I, "Before You Begin Developing or Revising Your ERP."

You should also identify an Alternate ER Lead who would step in should the ER Lead be unavailable. The ER Lead and the Alternate ER Lead need to be reachable 24 hours a day, seven days a week. A clear chain of command, or command structure, should also be established so that personnel and staff know their individual roles and responsibilities. If you have the resources and staff, you may consider forming an ER team that uses a well-defined command structure. At a minimum, your ERP should include the following basic information:

Name of ER Lead		Name of Alternate ER Lead	
Work Telephone No.		Work Telephone No.	
Home Telephone No.		Home Telephone No.	
Cell Phone No.		Cell Phone No.	
Pager No.		Pager No.	
Radio Call No.		Radio Call No.	

I saw a reference to a Water Utility Emergency Response Manager (WUERM) in another USEPA document. What is a WUERM?

A WUERM is basically your ER Lead. An ER Lead can have a variety of titles but the basic role and responsibility of the ER Lead does not change. Do not get confused or bogged down with titles and terminology. The main contact person and decision-maker during a major event is the ER Lead, regardless of job title.

What is an Incident Command System (ICS)? Do I need to have ICS?

Briefly, ICS is the model tool for command, control, and coordination of an emergency response and provides a means to coordinate the efforts of first responders as they work toward the common goal of stabilizing a major event and protecting life, property, and the environment. ICS uses a well-defined command structure in order to specify roles and responsibilities in responding to a major event. In ICS, the main contact person and decision-maker is the Incident Commander. At the CWS level, the ER Lead has the role of Incident Commander, unless the incident is of such significance that local, State, or Federal officials take over the command. You could use ICS to help organize yourself and your ER team, whether the team consists of staff from your CWS or other emergency responders. You do not need to have a complex command structure in place, but one that reflects your capabilities and also works effectively.

First responders may use ICS when responding to a major event. Your State may also have adopted ICS to respond to major events, and you may be required to abide by this command structure. If you are not required to use ICS, you should be familiar with ICS terms and command structure at a minimum. Other first responders may take over the role and responsibilities of Incident Commander in the latter stages of a major event, and you should know how this affects your role and responsibilities. You (or more appropriately the ER Lead) should address roles, responsibilities, and the command structure when forming the partnerships described in Section I, “Before You Begin Developing or Revising Your ERP.”

More information on ICS can be obtained from FEMA at http://training.fema.gov/EMIWeb/IS/is195.asp. Federal departments and agencies use an ICS under the National Incident Management System (NIMS)(http://www.dhs.gov/dhspublic/interweb/assetlibrary/NIMS-90-web.pdf).

C. Communication Procedures: Who, What, and When (Element 3)

What communication procedures do I need to have in place?

Appropriate and timely communication is essential during an emergency. The ERP should identify clear communication channels for CWS staff and personnel, external non-CWS entities, and the public/media. As part of your ERP, you should maintain internal and external notification lists that contain information on all appropriate entities to be contacted, including their names, titles, mailing addresses, e-mail addresses, all applicable land line and cellular phone numbers, and pager numbers. These lists should

be updated as necessary. In a major event (e.g., a terrorist attack), it may not be possible to use normal channels of communication. Provisions need to be made for an efficient and fail-safe form of communication to be available during conditions when the use of normal means may not be possible. Communication procedures with the public and media may already be part of your day-to-day operations, but these procedures need special attention during a major event in order to provide the public and media with timely, accurate, and complete information.

1. Internal Notification List

Who should be on my internal notification list?

The ER Lead and the Alternate ER Lead should be the first persons notified, because responding to a major event is their primary responsibility. If you have an ER team, then team members should be notified as well. Your ER team should consist of essential CWS personnel to be notified during an emergency. You should notify CWS management. Your internal notification list also should clearly identify all appropriate staff and personnel to be notified. Internal notification lists should include the name of the employee, work and home telephone numbers, and any other numbers at which the employee can be reached, such as cell phone, pager, or radio phone.

2. External Non-CWS Notification List

Who should be on my external non-CWS notification list?

Your external non-CWS notification list should ensure that all appropriate first responders and affected customers or critical users are notified. Procedures should also be established as to who should be notified, when they should be notified, and who is responsible to make the notifications from your CWS.

Below is a short list of possible first responders. These organizations are not listed in any particular order of preference.

- ❑ Local
  - Local 911
  - Police
  - Fire
  - Local Emergency Planning Committee (LEPC)
  - Elected Officials
  - Power Utility
  - Hazardous Materials (HAZMAT) personnel
- ❑ State
  - Drinking Water Primacy Agency
  - Department of Health
  - State 24-hr Emergency Communications Center Telephone
  - State Office of Homeland Security
  - HAZMAT
  - State Police
- ❑ Federal
  - FBI
  - EPA Headquarters and Regional Office
  - Department of Homeland Security (DHS)
  - Department of Health and Human Services (HHS)
  - National Response Center (800-424-8802, http://www.nrc.uscg.mil/)
- ❑ Other
  - Water Information Sharing & Analysis Center (http://www.waterisac.org/)

When you are identifying the list of groups to be notified during a major event, critical users (e.g., hospitals) and commercial and industrial customers such as those that incorporate water into their product (e.g., bottling and canning companies), should also be considered. You should maintain a list of critical users as part of your ERP. Some of these users should be given priority notification due to their public health mission and because they may serve customers considered "sensitive sub-populations" (e.g., senior residential housing, child care centers, medical facilities). Specific notification procedures should be developed for these groups.

3. Public/Media Notification: When and How to Communicate

What special items or issues do I need to consider when communicating with the public and media?

Effective public and media communications is a key element of your ERP. You should designate in advance who the CWS spokesperson will be during a major event. The spokesperson should be someone who is knowledgeable and credible, has good communication skills, and, if possible, is not a key person needed for implementing ERP response actions during the major event. In communicating with the media, the lead spokesperson may be someone external to the CWS if another organization has taken over the role of lead agency or Incident Commander (e.g., a representative from the health department or the State Drinking Water Primacy Agency). You should consider having both field and office staff respectfully defer questions to the designated spokesperson.

You can plan now for public and media notification needs by developing a communication plan or strategy for the spokesperson to follow. The communication plan or strategy should be a set of general guidelines for the spokesperson to follow in order to craft clear and concise messages for the public and to also deal with the media. The communication plan or strategy should be targeted to reach several audiences, such as your customers (both residential and business), local health professionals, and others. You can draft press releases and public water restriction notices in advance. The key to remember is that your message should be clear, accurate, and easily understood by your audience. Appendix A presents additional guidance on recommended communications plans or strategies.

D. Personnel Safety (Element 4)

Why do I need to address personnel safety in my ERP?

Protecting the health and safety of everyone in your CWS as well as the surrounding community is a key priority during an emergency. During an emergency, personnel may be at risk of harm, injury, or even death. This section of your ERP should provide direction personnel on how to safely implement a variety of response actions.

What procedures should the plan describe to provide for personnel safety?

When considering personnel safety the following factors should be taken into account:

- ***Evacuation Planning***: Develop a CWS evacuation policy and procedures.
- ***Evacuation Routes and Exits***: Designate primary and secondary evacuation routes and ensure that they are clearly marked, well lit, unobstructed at all times, and unlikely to expose evacuating personnel to additional hazards.

- ***Assembly Areas and Accountability***: Obtaining an accurate account of personnel requires planning and practice. Designate assembly areas where personnel should gather after an evacuation and specify procedures for taking a head count and identifying personnel.

- ***Shelter***: In some major events, the best means of protection is to take shelter (also known as shelter in place) either within the CWS or away from the CWS in another building.

- ***Training and Information***: Train staff and personnel in evacuation, shelter, and other safety procedures.

- ***Emergency Equipment***: Consider developing written procedures for using and maintaining your emergency response equipment. This should apply to any emergency equipment relevant to a response involving a toxic chemical, including all detection and monitoring equipment, alarms and communications systems, and Personal Protective Equipment (PPE) not used as part of normal operations.

- ***First Aid***: Discuss proper first aid and emergency medical treatment for employees and others who are onsite at the CWS. This should include standard safety precautions for victims as well as more detailed information for medical professionals. Indicate also who is likely to be responsible for providing the appropriate treatment (i.e., an employee with specialized training or a medical professional).

Are there other sources of information that can help me with developing personnel safety procedures?

You should focus on standard Occupational Safety and Health Administration (OSHA), Spill Prevention Control and Countermeasures (SPCC), Risk Management Program (RMP), and State procedures to define your own personnel safety procedures. Your staff should understand when to evacuate, when and how to use PPE, and how to rapidly locate additional safety information, such as chemical-specific Material Safety Data Sheets (MSDS). You also could consult with other utilities and water organizations.

E. Identification of Alternate Water Sources (Element 5)

What should I consider when identifying alternate water sources in my ERP?

You should consider the amount of water needed to address short-term (hours to days) and long-term (weeks to months) outages. As part of your ERP, you should identify the alternate water supplies available to you during both types of outages. To do this, you need to have a comprehensive understanding of your current water supply, your water distribution system, and your water system demand requirements. You should clearly understand the location and capabilities of other regional CWS, including available excess capacity and ease of connection to your distribution system. In addition, you should also understand the interconnection agreements your partners have in place and potential issues that could arise if multiple CWS are affected. These are important issues that should be addressed when you are forming the partnerships described in Section I, “Before You Begin Developing or Revising Your ERP.”

What should I consider for short-term outages?

Short-term outages might be due to contamination or electrical power outages. If your CWS has been contaminated, a public health notification such as “boil water,” “do not drink,” or “do not use,” may be issued by the drinking water primacy agency. If a “boil water” notice is issued, no alternative water source is needed. If a “do not drink” order is issued, then the suspect water can still be used for other

activities that do not involve ingestion of the water. In this situation, it will only be necessary to provide an alternate drinking water supply for consumption and related activities such as food preparation.

A “do not use” order is much more restrictive. You will need sufficient alternate water sources to supply water for consumption, hygiene, and emergency needs. A “do not use” notice may also have implications with respect to water used for firefighting. Although a prohibition on use of water for firefighting is likely to occur only if the water is contaminated with certain substances, an alternate source of firefighting water, such as a pond, river, or stream, may be necessary in this event.

As part of your ERP, you should consider the potential effects of a power outage. Your utility could be without power due to a major event, and it may take several days for power to be restored. Your plan should include contingencies for back up power generation and alternative power sources.

As part of your ERP, you also should identify agencies or private companies that could provide water supplies (bottled or bulk) in the event of a major event and establish mutual aid agreements with surrounding communities, industries, contractors and related utilities as appropriate. Your source list should be maintained to include accurate information on points of contacts for the alternate sources. Possible short-term alternate water supply options include (but are not limited to) the following:

- Bottled water provided by outside sources;
- Bottled water provided by local retailers;
- Bulk water provided by certified water haulers;
- Bulk water transported or provided by military assets (i.e., National Guard or U.S. Army Corps of Engineers (USACE));
- Bulk water provided by neighboring water utilities by truck or via pipeline;
- Bulk water from hospitals, universities, and local industry that maintain backup water supplies for consumption;
- Interconnections with nearby public water systems;
- Water treated by plant and hauled to distribution centers (i.e., in the case of water distribution system contamination);
- Water pumped from surface water sources, treated at the plant or nearby plants, and hauled to distribution centers;
- Water for firefighting from Federal agencies such as the USACE and FEMA; and
- Water from unaffected wells owned by local citizens and businesses.

Additional equipment may be available from:

- Local businesses such as dairies, well drillers, irrigation supply firms, or distributors that may have tank trucks that can be made suitable for carrying water, chlorinators or generators that can be used for emergency disinfection, and pipe that can be used to extend water supply lines.
- Other water utilities in the area that may have spare parts (such as valves, pumps, and pipe) available for use in an emergency.
- FEMA, USACE, and the U.S. Forest Service that may be able to provide firefighting equipment.

You may also want to plan for water conservation measures to be used if a major event causes a reduction in service or a “do not use” notice is issued. For example, if a major event causes a reduction in service, you could limit water use by advising customers not to do laundry, run the dishwater, or water the garden and to limit the duration of showers. To plan for a “do not use” notice, you could advise consumers to maintain an emergency supply of water, such as keeping a certain amount of bottled water in their homes.

What should I consider for long-term water outages?

If your CWS will need extensive cleaning, or if portions of the system have been destroyed, you will need a long-term alternate water supply. The following are examples of possible long-term water supply options:

- Connection of the water distribution system to an existing municipal or private water supply (assumes existing water treatment plant and distribution system is intact and useable);
- Connection of the water distribution system with a new uncontaminated groundwater or surface water source (assumes existing water treatment plant and distribution system is intact and useable);
- Development of new water distribution system (assumes existing water treatment plant and source water is uncontaminated and useable); and
- Development of oversized community storage facilities to compensate for loss of existing system capacity.

F. Replacement Equipment and Chemical Supplies (Element 6)

What pieces of equipment and chemical supplies do I need to identify in my ERP?

Your ERP should identify equipment that can significantly lessen the impact of a major event on public health and protect the safety and supply of drinking water. You should maintain an updated inventory of:

- Current equipment (e.g., pumps);
- Repair parts;
- Chemical supplies for normal maintenance and operations; and
- Information on mutual aid agreements.

Based on the findings of your VA, you should identify how and where to find the equipment, repair parts, and chemicals that you would need to respond adequately to a particular vulnerability. You should consider establishing mutual aid agreements with other CWS to address any deficiencies. These agreements should identify the equipment, parts, and chemicals available to you under the agreement.

G. Property Protection (Element 7)

Why do I need to address property protection in my ERP?

Protecting CWS facilities, equipment and vital records is essential to restoring operations once a major event has occurred. Your ERP should identify measures and procedures that are aimed at securing and protecting your CWS following a major event. Items that should be considered include:

- “Lock down” procedures;
- Access control procedures;
- Establishing a security perimeter following a major event;
- Evidence protection measures for law enforcement (should the major event also be declared a crime scene);
- Securing buildings against forced entry; and
- Other property protection procedures and measures.

H. Water Sampling and Monitoring (Element 8)

What water sampling and monitoring issues do I need to address in my ERP?

Water sampling and monitoring should be an integral part of your ERP and not an afterthought. How else can you determine whether the drinking water that you supply is safe for public consumption and use? During the stage of forming partnerships described in Section I, "Before You Begin Developing or Revising Your ERP," you should consult with your State Drinking Water Primacy Agency on the issues of water sampling and monitoring. In your ERP you will need to identify and address special water sampling and monitoring issues that may arise during and after a major event. Some water sampling and monitoring issues to consider include:

- Identifying proper sampling procedures for different types of contaminants;
- Obtaining sample containers;
- Determining the quantity of required samples;
- Identifying who is responsible for taking samples;
- Identifying who is responsible for transporting samples (in time sensitive situations);
- Confirming laboratory capabilities and certifications; and
- Interpreting monitoring or laboratory results.

For a more detailed discussion on water sampling and monitoring issues, please see USEPA's Response Protocol Tool Box Module 3, "Site Characterization and Sampling Guide" (EPA-817-D-03-003) at http://www.epa.gov/safewater/security/pdfs/guide_response_module3.pdf and Module 4, "Analytical Guide" (EPA-817-D-03-004) at http://www.epa.gov/safewater/security/pdfs/guide_response_module4.pdf

III. Putting Your ERP Together and ERP Activation

A. Putting All Your Core ERP Elements Into a Single Comprehensive Plan

I have addressed all my core ERP elements. What do I do next?

You now want to organize and document all the information that you gathered or produced while addressing your core ERP elements. Your goal is to produce a single comprehensive ERP document that is accessible to appropriate personnel, and that can be updated or modified as the need arises. Your ERP document may be organized into:

- Overall ERP polices;
- General ERP procedures;
- Any mutual aid agreements;
- Reference documents; and
- Action Plans (see Section IV, "Action Plans," for more details).

How you ultimately organize and document your ERP is up to you and can depend on whether you are developing an ERP from scratch, or are revising an existing ERP. Other Federal and State requirements may also influence how you organize and document your ERP. The Bioterrorism Act requires that you maintain a copy of your ERP for five years after you have sent your ERP certification to USEPA (see also Section V, "Next Steps"). A secure copy of your ERP should also be maintained in an off-premises location in the event that your copy cannot be accessed.

B. ERP Activation

What is "ERP Activation" and why is it important?

Knowing when to activate or set your ERP in motion is as important as having a prepared and documented ERP. In the past, emergency response mostly dealt with emergencies such as natural disasters and accidents. The definition of a "major event" in this guidance includes a major disaster or other emergency as well as a terrorist attack. Being prepared to respond to a terrorist attack requires special attention. This section discusses ways in which you may learn about a threat, the threat decision process, and activation of your ERP.

What things should I pay special attention to before activating my ERP?

You should pay attention to any "threat warning." The Homeland Security Advisory System shown in **Figure III-1** contains five threat condition levels. Low Condition (Green) is declared when there is a low risk of terrorist attacks. Guarded Condition (Blue) is declared when there is a general risk of terrorist attacks. Elevated Condition (Yellow) is declared when there is a significant risk of terrorist attacks. High Condition (Orange) is declared when there is a high risk of terrorist attacks. Finally, Severe Condition (Red) reflects a severe risk of terrorist attacks. EPA has issued supplemental guidance for water utilities to increase security based on threat conditions described by the five-tiered Homeland Security Advisory System (see Appendix B).

Figure III-1. Threat Condition Levels

A "threat warning" is an occurrence or discovery that indicates a threat of a malevolent act and triggers an evaluation of the threat. These warnings should be evaluated in the context of typical CWS activity and previous experience in order to avoid false alarms. The threat warnings presented in **Figure III-2** and described below are intended to be inclusive of those most likely to be encountered, but this listing is by no means comprehensive of all possibilities.

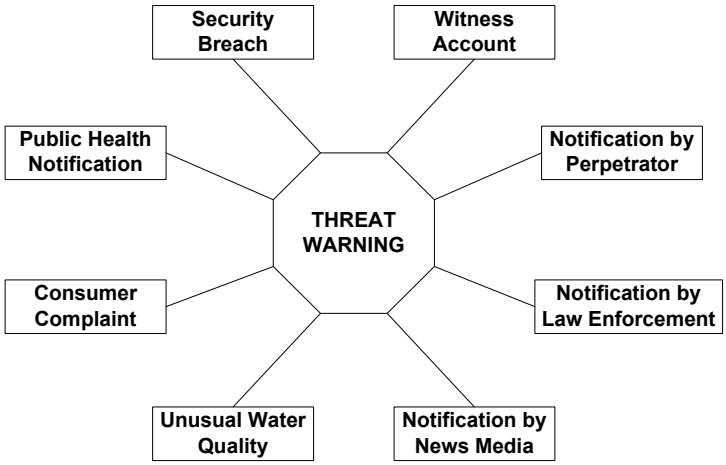

Figure III-2. Summary of Potential Threat Warnings

- ***Security Breach***. Physical security breaches caused by lax operations such as unsecured doors or criminal acts such as trespassing are probably the most common threat warnings.

- ***Witness Account***. You or your neighbors may see suspicious activity, such as trespassing, breaking and entering, and other types of tampering.

- ***Notification by Perpetrator***. A threat may be made directly to you, either verbally or in writing. Historical incidents indicate that verbal threats made over the phone are more common than written threats.

- ***Notification by Law Enforcement***. You may receive notification about a threat directly from law enforcement, whether it is county, local, State, or Federal. Such a threat could be a result of a report of suspicious activity or through information gathered by law enforcement.

- ***Notification by News Media***. A threat might be delivered to the news media, or the media may discover a threat. A conscientious reporter would immediately report such a threat to the law enforcement and either the reporter or law enforcement would immediately contact the CWS.

- ***Unusual Water Quality***. You should investigate possible causes of unusual water quality (i.e., changes from baseline). You want to rule out unusual results that can be explained or those that are due to known causes.

- ***Consumer Complaint***. An unexplained or unusually high incidence of consumer complaints about the aesthetic qualities of drinking water may indicate a potential threat. Many chemicals can impart a strong odor or taste to water, and some may discolor the water.

- ***Public Health Notification***. The first indication that a water-related incident has occurred may involve victims showing up in local emergency rooms and health clinics. An incident triggered by a public health notification is unique in that at least a segment of the population has been exposed to a harmful substance.

What do I do once I discover a threat warning?

Once a threat warning is received, the threat decision (or threat evaluation) process begins. The ER Lead or Alternate ER Lead should be notified immediately because they will be involved in this decision process and make decisions about who else (e.g., other emergency responders) should be involved. The threat decision process is considered in three successive stages: 'possible', 'credible', and 'confirmed'. As the situation escalates through these three stages, the actions that might be considered also change. The following describes the stages, actions that might be considered, and activation of your ERP.

- **Stage 1: "Is the threat 'possible'?"** If you are faced with a threat, you should evaluate the available information to determine whether or not the threat is possible (i.e., could something have actually happened?). If the threat is possible, immediate operational response actions might be implemented. Knowing the findings from your VA could help you determine whether a certain threat is possible or not.

- **Stage 2: "Is the threat 'credible'?"** There must be information to corroborate the threat in order for it to be considered credible. For example, your information source may be highly credible, hospitals may be reporting a potential incident, or your may have monitoring results that are unusual. At this stage, you may activate additional portions of your ERP, such as initiating internal and external notifications, conducting water sampling and analysis, or issuing public health advisories. At this stage, you're not sure whether a major event has occurred but are preparing to respond should the threat actually lead to a major event.

- **Stage 3: "Has the incident been 'confirmed'?"** Confirmation implies that definitive evidence and information has been collected to establish that an incident has occurred. Confirmation of an incident may be obvious, such as structural damage to a CWS; in such a case, Stages 1 and 2 would be omitted. Upon confirmation of the incident, you should fully implement your ERP. Your ERP should contain Action Plans (see Section IV) that address specific major events, and these Action Plans should be implemented immediately.

The application of this threat decision process will vary significantly with the circumstances. The ER Lead should work through the threat decision process and implement the ERP as needed. In summary, judgment must be exercised when determining how to appropriately manage a specific threat or incident.

IV. Action Plans

What are Action Plans?

Action Plans (APs), also known as Response Guidelines, are tailored ERPs that address specific major events. APs describe response actions to take for events that you think might occur at your facility based on the specific vulnerabilities identified in your VA.

An AP should provide a quick approach for responding to a specific major event and it complements actions already initiated under the ERP. You may only need one to two pages to cover specific response information since you have already addressed basic emergency response steps in the core elements of your ERP. An AP should be an accessible (i.e., "rip and run") document that can be detached and taken to the field by the ER Lead or Alternate ER Lead. An AP should include the following basic information:

- Any special notification requirements;
- Special response steps to be taken upon ERP activation; and
- Recovery actions to bring the CWS back into operation.

A. Response to Vulnerability Assessment Findings

How do I go about developing Action Plans for my VA findings?

The Bioterrorism Act requires that prepared or revised ERPs incorporate the results of completed VAs. During the VA process, you should have determined your high priority vulnerabilities. An Action Plan defines the specific actions you would take to respond to events where your high priority vulnerabilities have been compromised. In addition, we recommend that you develop APs for certain high consequence events regardless of whether these are among your high-priority vulnerabilities. Events and threats of events that should be considered in APs include the following:

- Contamination of the Drinking Water;
- Structural Damage/Physical Attack;
- SCADA, Computer, or Cyber Attack; and
- Intentional Hazardous Chemical Release (e.g., release of chlorine or ammonia from storage).

Even if your VA did not identify any vulnerabilities, you are encouraged to consider contingency planning for the possibility of these events.

Example Action Plans for the four intentional events listed above are included in Appendix C. Each AP goes through the threat decision process described in Section III.B, "ERP Activation." It should be noted

that these simplified examples are for discussion purposes only and that you should develop "Action Plans" specific to the needs of your water system and surrounding community. You also could consult EPA's Response Protocol Toolbox, http://www.epa.gov/safewater/security/index.html#emergency, as an aid in developing APs for contamination events.

So, what about all of the sensitive information in my Action Plans referring to my vulnerabilities?

APs should be easily accessible to authorized personnel and should be easily identifiable during a major event. However, you may want to limit access to APs containing sensitive information and specifics related to intentional events. Again, steps taken to limit such access should consider local and state Freedom of Information Act (FOIA) laws. Alternatively, you can opt to make your APs general in nature so that everyone can use them and place sensitive information in the ERP appendices, or in sections that are not readily available to unauthorized personnel.

B. Natural Disasters and Other Significant Events

How should my ERP deal with natural disasters and other emergencies?

If you already have an ERP in place to address other major events, you may want to tailor response actions in light of discussions in this section. You may wish to develop individual Action Plans for other major events that are not terrorist-related. A similar approach to that described above could be used to plan for natural disasters and other significant events. Natural disasters and other significant events include:

- Fire;
- Flood;
- Hurricane and/or Tornado;
- Severe Weather (snow, ice, temperature, lightning, drought);
- Earthquake;
- Electrical Power Outage;
- Mechanical Failure;
- Water Supply Interruption;
- Contaminated Water Treatment Chemicals;
- Accidental Hazardous Chemical Spill/Release;
- Construction Accidents;
- Personnel Problems (Loss of operator, medical emergencies);
- Vandalism; and
- Unintentional Contamination of the Water Supply (e.g., waterborne disease outbreak, accidental cross connections, etc.).

V. Next Steps

What do I do once my ERP is completed or revised?

Once you prepare or revise your ERP, you are required under the Bioterrorism Act to submit a written certification stating that the plan has been completed by a certain deadline date. (Do not submit a copy of the ERP to EPA.) USEPA has produced a separate document that addresses ERP certification submittal entitled *Instructions to Assist Community Water Systems in Complying with The Public Health Security and Bioterrorism Preparedness and Response Act, Title IV*. Please consult this document to answer your specific questions about submittal procedures and deadline dates. This document can be

found at http://www.epa.gov/safewater/security/community.html. A copy of the ERP certification is presented at the end of this section.

Additionally, as required under Section 1433(c) of the Bioterrorism Act you must maintain a copy of your ERP for five (5) years after you submit your ERP certification to USEPA.

Where do I send my signed ERP Certification?

We recommend that you submit the ERP certification using an express or courier service such as Federal Express, United Parcel Service, Airborne, etc., which provides tracking and certification of delivery. Using one of these services will ensure that the submission is delivered directly to the persons authorized to receive and process these items.

Use the following address for express or courier service deliveries to USEPA. This location is open for deliveries between 8:30am and 4:30pm Eastern Time. Call the number under the address below before attempting delivery outside of those hours.

U.S. Environmental Protection Agency
Water Resource Center (WSD-RAR)
Room 1119 EPA West Building
1301 Constitution Ave., NW
Washington DC 20004

Couriers are to use phone number 202-566-1729.

As stated above, more detailed guidance on preparing and submitting the ERP certification can be found at http://www.epa.gov/safewater/security/community.html.

What additional State requirements must I meet?

Depending on your State, you may be required to provide a copy of your ERP to State authorities or certify that you have completed or revised your ERP. You should coordinate with your State Drinking Water Primacy Agency to determine what requirements apply to your CWS.

When should I update my ERP?

It is important to note that an ERP is a "living" document that you should update periodically (i.e., at least annually or if there is a major change to your CWS configuration). The ER Lead and appropriate CWS management staff should approve the ERP and identify the time period for routinely updating the ERP (e.g., annually). Updates should occur if there are changes in CWS staff, internal and external contacts, roles and responsibilities of anyone involved in response, or there are changes made in infrastructure.

If you update your ERP, you are not required to resubmit a written ERP certification to the USEPA.

What type of training is appropriate?

You should make sure that your staff is trained on their ERP responsibilities. Training can include briefing sessions, classroom sessions, or mock exercises. You should also remember to do "refresher" training on a regular basis. Training should include testing of the ERP. Drills and exercises that challenge the information in the ERP should be conducted at least annually. There are many sources (State, Federal, and industry specific) that describe what should be included in emergency training. These typically include the following four types of training:

- **Orientation Sessions**: Orientation sessions work well for basic instruction and explaining ERP procedures. Written tests may be employed to ensure some level of comprehension by the attendees.

- **Table-Top Workshop**: Table-top workshops involve developing scenarios that describe potential problems and provides certain information necessary to address the problems. The idea is to present staff and emergency response officials with a fabricated event, have them verbally respond to a series of questions, and then evaluate whether the responses match what is written in the ERP.

- **Functional Exercises**: The Functional Exercise is considered the most effective training tool, next to a real emergency, because a team of simulators is trained to develop a realistic major event. By using a series of pre-scripted messages, the simulation team sends information in to personnel assigned to carry out the ERP procedures. Both the simulators and personnel responding to the simulation are focused on carrying out the procedures to test the validity of the ERP.

- **Full Scale Drills**: These are the most costly and time-consuming training programs but can be extremely effective. In a full-scale drill, emergency response personnel and equipment are mobilized to a scene, an emergency scenario is presented, and they respond as directed by the ERP.

The bottom line is that time, resources, and personnel need to be dedicated to accomplishing the training. Use the training to identify lessons learned, debrief staff of lessons learned to enhance future response and recovery efforts, and update plans to incorporate lessons learned.

Reproduction of ERP Certification

CERTIFICATION OF COMPLETION
OF AN EMERGENCY RESPONSE PLAN

Public Water System ID number:_____

System Name:_____

City where system is located:_____

State :_____

Printed Name of Person Authorized to Sign
this Certification on Behalf of the System:_____

Title:_____

Address :_____

City:_____

State and ZIP Code:_____

Phone:_____**Fax:**_____**Email:**_____

I certify to the Administrator of the U.S. Environmental Protection Agency that this community water system has completed an Emergency Response Plan that complies with Section 1433(b) of the Safe Drinking Water Act as amended by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law 107-188,Title IV — Drinking Water Security and Safety).

I further certify that this document was prepared under my direction or supervision. I am aware that there are significant penalties for submitting false information (Safe Drinking Water Act (42 U.S.C.300f *et seq.*)).

The emergency response plan that this community water system completed incorporates the results of the vulnerability assessment completed for the system and includes "plans, procedures, and identification of equipment that can be implemented or utilized in the event of a terrorist or other intentional attack " on this community water system. The emergency response plan also includes "actions, procedures, and identification of equipment which can obviate or significantly lessen the impact of terrorist attacks or other intentional actions on the public health and the safety and supply of drinking water provided to communities and individuals."

This CWS has coordinated, to the extent possible, with existing Local Emergency Planning Committees established under the Emergency Planning and Community Right-to-Know Act (42 U.S.C.11001 et seq) when preparing this emergency response plan.

Signed:_____ **Date:**_____

Primary contact person that EPA can call if there are questions about this Certification:

Name:_____

Address (if different than that of the Authorized Representative):_____

_____

Phone:_____

Email Address:_____

Alternate Contact Person:

Name:_____

Address (if different than that of the Authorized Representative): _____

_____

Phone:_____

Email Address:_____

References and Links

The following is a list of references and Internet links that may be useful to you in preparing your Emergency Response Plan.

Department of Homeland Security (DHS): DHS is the overall lead agency for homeland security issues. DHS will become involved in incident response if needed. General information about DHS is available at http://www.dhs.gov/dhspublic. DHS administers the National Incident Management System (NIMS), which provides a nationwide template to enable Federal, State, local, and tribal governments and private-sector and nongovernmental organizations to work together to prepare for, prevent, respond to, and recover from domestic incidents, including terrorism. Information on the NIMS can be found at http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf.

Environmental Protection Agency: EPA has numerous resources available in addition to this guidance. The following are key sources:

- Water Infrastructure Security information, guidance, and training information can be found at http://www.epa.gov/safewater/security/index.html.
- More information on Local Emergency Planning Committees (LEPCs) can be found at http://www.epa.gov/ceppo/lepclist.htm.

The Center for Disease Control and Prevention (CDC): The CDC develops resources to assist hospital staff, clinics, and physicians in diagnosing diseases related to terrorism, reporting incidences of disease, and controlling the spread of infection. Information on emergency preparedness and response can be found at http://www.bt.cdc.gov.

- To assist in the development of a Public Health Response Plan, the CDC published a planning document entitled *The Public Health Response to Biological and Chemical Terrorism: Interim Planning Guidance for State Public Health Officials (July 2001)*, which can be found at http://www.bt.cdc.gov/Documents/Planning/PlanningGuidance.pdf.
- *Interim Recommended Notification Procedures for Local and State Public Health Department Leaders in the Event of a Bioterrorist Incident* can be found at http://www.bt.cdc.gov/EmContact/Protocols.asp.

Federal Emergency Management Agency (FEMA): On March 1, 2003, FEMA became part of the U.S. Department of Homeland Security. FEMA's mission is to reduce loss of life and property and protect our nation's critical infrastructure from all types of hazards through a comprehensive, risk-based, emergency management program of mitigation, preparedness, response and recovery. General information can be found at http://www.fema.gov. In addition, several online training courses relevant to emergency management are available on-line from FEMA at http://training.fema.gov/EMIWeb/IS/crslist.asp.

The American Water Works Association (AWWA): EPA training developed through partnership with AWWA covers security issues including assessing vulnerabilities, emergency response plans and risk communication. AWWA information can be accessed at their website, http://www.awwa.org. Specific AWWA resources can be found at http://www.awwa.org/communications/offer/secureresources.cfm.

The Association of State Drinking Water Administrators (ASDWA): ASDWA has information on water security planning, training, and links to State programs and other information sources. Go to the security link at http://www.asdwa.org.

National Rural Water Association (NRWA): NRWA developed the "Security and Emergency Management System" (SEMS) Software Program, which can be loaded on a personal computer. It is based on NRWA/ASDWA's *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000*. You can find more information at http://www.nrwa.org.

Glossary

Definitions in this glossary are specific to the Emergency Response Plan Guidance but have been conformed to common usage as much as possible.

Action Plans: specific plans designed to be used during the response to a threat or incident. Action plans should be easy to use and contain forms, flow charts, and simple instructions to support staff in the field or decision officials during management of a crisis.

Bioterrorism Act: the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

Chain of Command: a clear and definitive structure of authority.

'Confirmed': a stage in the threat evaluation process in which there is definitive evidence and information to establish that an incident or major event has occurred.

'Credible': a stage in the threat evaluation process in which there is information to corroborate a threat.

Drinking Water Primacy Agency: the agency that has primary enforcement responsibility for national drinking water regulations, namely those promulgated under the Safe Drinking Water Act as amended. Drinking water primacy for a particular State may reside in one of a variety of agencies such as the State Health Agency, the State Environmental Agency, or the USEPA regional office.

Emergency Response (ER) Lead: the pre-designated main point of contact and decision-maker for a CWS during a major event.

Incident Command System: a standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries.

Jurisdiction: the range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority for incident mitigation. Jurisdictional authority at an incident can be political/geographic (e.g., city, county, State, or Federal boundary lines) or functional (e.g., police department, health department, etc.).

Local Emergency Planning Committee (LEPC): established by the Emergency Planning and Community Right-to-Know Act, LEPCs have the job of increasing community hazardous materials safety through public education, emergency planning, responder training, conducting exercises, and reviewing actual responses to releases.

Major Event: a domestic terrorist attack, major disaster, or other emergency (from Homeland Security Presidential Directive/HSPD-8) (http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html)

Notification: the process of communicating information to interested parties.

Personal Protective Equipment (PPE): equipment and supplies designed to protect employees from serious injuries or illnesses resulting from contact with chemical, radiological, biological, or other hazards. PPE includes face shields, safety glasses, goggles, laboratory coats, gloves, and respirators.

'Possible': a stage in the threat evaluation process in which available information indicates there is an opportunity for an incident (i.e., the threat is possible).

Response Decisions: part of the threat management process in which decisions are made regarding appropriate response actions that consider 1) the conclusions of the threat evaluation, 2) the consequences of the suspected incident, and 3) the impacts of the response actions on drinking water customers and the utility.

Security Breach: an unauthorized intrusion into a secured facility that may be discovered through direct observation, an alarm trigger, or signs of intrusion (e.g., cut locks, open doors, cut fences). A security breach is a type of threat warning.

Spokesperson: the individual responsible for interfacing with the public and media or with other agencies requiring information directly from the incident. Under the ICS, there is only one spokesperson per incident.

Technical Assistance Provider: any organization or individual that provides assistance to drinking water utilities in meeting their mission to provide an adequate and safe supply of water to their customers.

Threat: an indication of possible violence, harm, or danger.

Threat Evaluation: part of the threat management process in which all available and relevant information about the threat is evaluated to determine if the threat is 'possible' or 'credible', or if an incident has been 'confirmed.' This is an iterative process in which the threat evaluation is revised as additional information becomes available. The conclusions from the threat evaluation are considered when making response decisions.

Threat Warning: an occurrence or discovery that indicates a threat of a malevolent act and triggers an evaluation of the threat.

Vulnerability Assessment (VA): a systematic process for evaluating the susceptibility of critical facilities to potential threats and identifying corrective actions that can reduce or mitigate the risk of serious consequences associated with these threats.

Appendix A: Public Communications Strategy

Developing a Public Communications Strategy

Developing a public communications strategy will prepare you to effectively communicate with the public and media at the time of an emergency or crisis. As a CWS, you should remember that any public notification or communication will have an immediate and direct impact on your customers and consumers. Consumers may be instructed to boil water, limit their water uses to activities that do not involve consumption, or not use the water at all. A good public communications strategy will help you get your message out effectively and outline who needs to do what and when. Items that should be considered in a public communication strategy include:

- Designating a spokesperson and any alternate spokespersons (should the main spokesperson be unavailable);
- Organizing basic facts about the CWS and the situation the CWS is facing;
- Having a method in place to develop key messages to use with the media that are clear, brief, and accurate;
- Making sure the messages are carefully planned and have been coordinated with other appropriate officials and organizations;
- Making sure the messages are targeted to reach different audiences such as residential and business customers, local health professionals, etc.; and
- Having methods in place for delivering messages;
- Determining how to reach the largest number of customers and key stakeholders by selecting delivery methods that are likely to produce the best results. The reach and impact of the message and information will increase if the same message is distributed via different delivery methods more than one time.

While it may seem that developing a public communications strategy may be a lot of work and effort, you should already have experience with public and media communication through your compliance with the public notification requirements of the 1996 Safe Drinking Water Act (SDWA) amendments. In fact, many of the suggestions found in this appendix on developing and implementing a public communication strategy are excerpts from the "Public Notification Handbook" (EPA 816-R-00-010, 2000) (http://www.epa.gov/safewater/pws/pn/handbook.pdf). For example, the sample public notices shown on the following pages are taken from the handbook. Additionally, other publications and tools are available that can assist you in developing and implementing a public communications strategy not only in response to major events, but also in improving your public and media communications in general.

Making Public and Media Communications Work

Making public and media communications work involves implementing your public communications strategy effectively. This takes practice and a lot of work BEFORE any notice or communication is issued. Below are some tips and suggestions that would help make your public communications strategy work. Please note that these tips and suggestion are not all inclusive. Many are taken directly from USEPA's "Public Notification Handbook" (EPA 816-R-00-010, 2000).

Communication Tips and Suggestions:

- Any decision to issue a public notification should be made in consultation with your Drinking Water Primacy Agency. You also should make arrangements with your local health department and/or other appropriate organizations prior to a major event in order to establish clear lines of communication and ensure access to decision officials on a 24/7 basis.
- Typical press releases and notices should be ready beforehand to save hours of time and possibly prevent serious health problems for water users. In your press release or notice you should explain to the media what information you are trying to communicate and why. The most important

information, including a description of the situation, populations at risk, instructions to consumers, and potential health effects, should be near the beginning of any press release or notice. Be sure to include a contact name and telephone number so that the media can call you for more information.

- ❑ Remember to avoid technical or confusing language in your press releases and notices.
- ❑ When you send a press release or notice to the media, write "PRESS RELEASE FOR PUBLIC SAFETY" at the top to emphasize its importance.
- ❑ Work with the media ahead of time and develop an ongoing relationship. Explain to them what constitutes a major event and what your needs will be during a crisis. Hold an annual media day where you can explain how your CWS operates, including any improvements you may be implementing. The more informed the members of the media are about your CWS then the more accurate and effective they are helping get your message out to the public. The box below provides some general tips when directly working with the media.
- ❑ Establish contacts with institutions and people who can translate press release and notices into other languages for you and who can help you target non-English speaking populations.
- ❑ If you are going to provide bottled water, you should confirm ahead of time and periodically reconfirm that available bottled water supplies meet the Food and Drug Administration or State safety standards.
- ❑ Consider beforehand which communication delivery methods would work best, particularly during a major event. Delivery methods during a major event could include:

  - Broadcast media (radio and television);
  - Government access channels;
  - Web site (local government and others);
  - Listserve e-mail;
  - Newspaper;
  - Phone banks;
  - Broadcast phone messages ("reverse 911" messaging);
  - Broadcast faxes;
  - Posting in conspicuous locations;
  - Mass distribution through partners (e.g., churches, retailers, restaurants);
  - Hand delivery;
  - Door-to-door canvassing; and
  - Direct notification to critical users (e.g., schools, hospitals, nursing homes, prisons, etc.).

General Tips on Working with the Media

- Be truthful and up-front.
- Answer questions as well as you can, but don't be afraid to say that you need to check on something if there is a question you can't answer (once you find the information, quickly report back on what you've found).
- Keep in mind that reporters are not familiar with State or Federal requirements for safe drinking water – avoid technical jargon!
- Provide additional sources of information (for instance, referrals to State contacts).
- Be sensitive to the fact that reporters may be working on tight deadlines.
- Provide a list of the elements that should be addressed.
- Don't be upset if a newspaper article or news report isn't exactly as you would want it, but politely tell a reporter if a significant piece of information is wrong or missing.
- Don't be defensive when answering questions.

Example Boil Water Notice

WARNING

BOIL YOUR WATER BEFORE USING

[The Holly County Water System] water is contaminated with [fecal coliform/E. coli]

[Fecal coliform or E. coli] bacteria were found in the water supply on [November 5]. These bacteria can make you sick and are a particular concern for people with weakened immune systems.

What should I do?

- DO NOT DRINK THE WATER WITHOUT BOILING IT FIRST. Bring all water to a boil, let it boil for ten minutes, and let it cool before using, or use bottled water. Boiled or bottled water should be used for drinking, making ice, brushing teeth, washing dishes, and preparing food until further notice. Boiling kills bacteria and other organisms in the water.

- Fecal coliform and E. coli are bacteria whose presence indicates that the water may be contaminated with organisms that can cause illness in humans. These organisms can cause diarrhea, cramps, nausea, headaches, or other symptoms. They may pose a special health risk for infants, young children, some of the elderly, and people with severely compromised immune systems.

- Organisms in drinking water are not the only cause of the symptoms above. If you experience any of these symptoms and they persist, you may want to seek medical advice. People at increased risk should seek advice about drinking water from their health care providers.

What happened? What is being done?

The water distribution system was contaminated with fecal coliform. We are working with law enforcement and the public health department to investigate/resolve this issue. We are currently increasing the chlorination levels at the treatment plant as well as at the chlorine booster stations throughout the system. In addition, we are evaluating all available information and conducting tests to confirm the extent of the contamination of the system. We will inform you when tests show no bacteria and you no longer need to boil your water. We anticipate resolving the problem within the next 48 hours.

For more information, please contact [Joseph Smith] at [555-555-6789]. General guidelines on ways to lessen the risk of infection by microbes are available from the EPA Safe Drinking Water Hotline at 1-800-426-4794 and [the Public Health Department Hotline at 1-800-123-4567].

Please share this information with all the other people who drink this water, especially those who may not have received this notice directly (for example, people in apartments, nursing homes, schools, and businesses). You can do this by posting this notice in a public place or distributing copies by hand.

This notice is being sent to you by [Holly County Water System]. State Water System ID# [10001]. Date distributed: [November 6, 2003]

Example Do Not Drink Notice

WARNING

DO NOT DRINK THE WATER

[Cyanide] found in the [City of Rolling Brook] water supply on [October 10th]

Bottled water can be obtained at [Islington Station High School and Penn Road High School 24 hours per day].

What should I do?

- Do NOT drink the water.
- Symptoms associated with cyanide include dry mouth, itchy throat, headache, sweating, flushed skin, muscle rigidity, fever, confusion, lethargy, seizures, loss of consciousness, coma, and death.
- If you or someone you know exhibits any of these symptoms, immediately contact your health care provider. In addition, please notify the public health department at 1-800-123-4567.

What happened? What is being done?

On October 10th, the water distribution system was contaminated with cyanide. We are working with law enforcement and the public health department to investigate/resolve this issue. We have tested the water in various parts of the distribution system to verify the extent of the cyanide contamination. Based on these tests, we have isolated the portion of the system located north of Aspen Street and east of River Road. Everyone in this portion of the system **should not drink the water**. We have implemented additional security procedures to protect the system against further contamination. Additional information will be provided 24 hours/day on Channel 57- the local government television channel.

For more information, please contact [Joseph Smith] at [555-555-6789]. More information is also available from the EPA Safe Drinking Water Hotline at 1-800-426-4794 and [the Public Health Department Hotline at 1-800-123-4567].

Please share this information with all the other people who drink this water, especially those who may not have received this notice directly (for example, people in apartments, nursing homes, schools, and businesses). You can do this by posting this notice in a public place or distributing copies by hand.

This notice is being sent to you by [City of Rolling Brook Water System]. State Water System ID#[50005]. Date distributed: [October 10, 2003]

Example Do Not Use Notice

WARNING

DO NOT USE THE WATER

[Lyonelle Water System] water is contaminated with [parathion]

Bottled water can be obtained at [Murray High School and Central High School 24 hours per day].

Parathion was found in the water supply on [November 14]. This chemical can make you sick and may result in death.

What should I do?

- DO NOT USE THE WATER. You should ***not*** use the water for drinking, making ice, brushing teeth, washing dishes, washing clothes, bathing, food preparation, or watering lawns. Bottled water should be used for all of the above necessities until further notice.

- Parathion is a chemical usually used to kill insects. It can cause constriction of the pupils, blurred vision, muscle and abdominal cramps, excessive salivation, sweating, nausea, vomiting, dizziness, headaches, convulsions, diarrhea, weakness, labored breathing, wheezing, and unconsciousness. Exposure can even lead to death.

- If you or someone you know exhibits any of these symptoms, immediately contact your health care provider. In addition, please notify the public health department at 1-800-123-4567.

What happened? What is being done?

The water distribution system was contaminated with parathion. We are working with law enforcement and the public health department to investigate/resolve this issue. We have tested the water in various parts of the distribution system to verify the extent of the parathion contamination. Based on these tests, we have isolated the portion of the system located north of Lincoln Avenue and east of Maple Road. Everyone in this portion of the system **should not use the water**. We have implemented additional security procedures to protect the system against further contamination. Additional information will be provided 24 hours/day on Channel 57- the local government television channel.

For more information, please contact [Joseph Smith] at [555-555-6789]. More information is also available from the EPA Safe Drinking Water Hotline at 1-800-426-4794 and [the Public Health Department Hotline at 1-800-321-4567].

Please share this information with all the other people who drink this water, especially those who may not have received this notice directly (for example, people in apartments, nursing homes, schools, and businesses). You can do this by posting this notice in a public place or distributing copies by hand.

This notice is being sent to you by [Lyonelle Water System]. State Water System ID# [90008]. Date distributed: [November 14, 2003]

Appendix B: GUARDING AGAINST TERRORIST AND SECURITY THREATS

Suggested Measures for Drinking Water and Wastewater Utilities (Water Utilities)

United States Environmental Protection Agency

Mid-Atlantic Region covering Delaware, Maryland, Pennsylvania, Virginia, West Virginia and the District of Columbia **April 2003**

GUARDING AGAINST TERRORIST AND SECURITY THREATS

Suggested Measures for Drinking Water and Wastewater Utilities (Water Utilities)

The Department of Homeland Security (DHS) established a five-tiered Homeland Security Advisory System to provide a national framework for notification about the nature and degree of terrorist threats. The system establishes a set of graduated levels that change in response to increases or decreases in terrorist threats. The threat levels are colored coded, beginning with green, and increasing in severity through blue, yellow, orange, and red. While the threat may not be specific to water utilities, the water sector, as one of the thirteen critical sectors identified by DHS, may consider themselves potential targets.

Why is EPA offering these suggestions?

Water utilities are in the forefront of ensuring that our nation's water systems are protected against terrorist threats. Many utilities have already developed safeguards. This document provides model guidelines for water utilities to increase security based on threat conditions described by the five-tiered Homeland Security Advisory System. Please note that the attached document is a guide; it is a not a requirement under any regulation or legislation.

This document provides suggested steps water utilities should consider implementing in the areas of detection, preparedness, prevention, and protection. The suggested measures are additive in that higher threat levels should also include those measures outlined in the document for lower threat levels. These suggestions are based on practices employed by various systems across the nation. The ability to implement them at the system level will vary. Note that these general recommendations should be adapted by the utility depending on the system size, status of emergency response planning at the utility, and identified system vulnerabilities. These suggestions should not be viewed as a complete source of information on protecting water utilities. Facility managers and utility security directors should consider the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.

Based on strong recommendations from the water sector, EPA is making this document available to water utilities and to the secure WaterISAC (www.waterisac.org). EPA is also providing this document to the state drinking water administrators. Some state homeland security and emergency response programs have issued suggestions to their critical infrastructures, including water. State drinking water administrators are encouraged to coordinate with state homeland security and emergency response programs and modify these suggested measures as appropriate to ensure consistency.

CONDITION	CONSIDER ADOPTING THESE MEASURES	
LOW (GREEN) **Low Risk of Terrorist Attack** **Signifies a *low risk* of terrorist attacks. Protective measures should focus on ongoing facility assessments; and the development, testing, and implementation of emergency plans. In addition to THREAT LEVEL GREEN, there are four higher threat levels: blue, yellow, orange, and red. (Please refer to the other fact sheets for information on suggested steps to be taken during other threat condition levels.)**	Detection	▪ Monitor water quality at the source water, leaving the plant, and in distribution and storage systems. Establish baseline results. Review operational and analytical data to detect unusual variations. ▪ Follow-up on customer complaints concerning water quality and/or suspicious behavior on the facilities. ▪ Confirm communication protocol with public health officials concerning potential waterborne illnesses.
	Preparedness	▪ Post emergency evacuation plans in accessible, but secure, location near entrance for immediate access by law enforcement, fire response, and other first responders. ▪ Inventory spare parts and on-hand chemicals. Check if sufficient. ▪ Identify sensitive populations within the service area (e.g., hospitals, nursing homes, daycare centers, schools, etc.) for notification, as appropriate, in the event of a specific threat against the utility. ▪ Back-up critical files such as plans and drawings, as-builts, sampling results, billing, and other critical information. ▪ Conduct appropriate background investigations of staff, contractors, operators, and others with access to the facility. ▪ Prepare vulnerability assessments and revise to incorporate changes made (e.g., assets added/replaced or new countermeasures implemented). ▪ Ensure that employees understand appropriate emergency notification procedures.
	Prevention	▪ Train staff in safety procedures, such as handling hazardous materials and maintaining and using self-contained breathing apparatus. ▪ Secure equipment such as vehicles and spare parts. ▪ Monitor requests for potentially sensitive information.
	Protection	▪ Check all chemical deliveries for driver identification and verification of load. ▪ Maintain vigilance and be alert to suspicious activity. Inspect buildings in regular use for suspicious packages and evidence of unauthorized entry. Report any suspicious activity to appropriate authorities. ▪ Prosecute intruders, trespassers, and those detained for tampering to the fullest extent possible under applicable laws. ▪ Review request for tours and identify protocols for managing the tour. ▪ Implement controls for construction activities at critical sites. ▪ Maintain disinfectant residuals as required by regulations. ▪ Implement best management practices for optimizing drinking water treatment.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
GUARDED (BLUE) **General Risk of Terrorist Attacks** **Signifies a *guarded risk* of terrorist attacks. Protective measures should focus on activating employee and public information plans; exercising communication channels with response teams and local agencies; and reviewing and exercising emergency plans.**	Detection	▪ Test security alarms and systems for reliability.
	Preparedness	▪ Reaffirm communication and coordination protocols (embedded in the utility's emergency response plan) with local authorities such as police and fire departments, HAZMAT teams, hospitals, and other first responders. ▪ Prepare and/or revise emergency response plans associated communication protocols. Include appropriate local officials concerned with law enforcement, emergency response and public health. ▪ On a regular basis post employee reminders about events that constitute security violations and ensure employees understand notification protocol in the event of a security breach. ▪ Prepare draft press releases, public notices and other communications for a variety of incidents. Route through appropriate channels of review to ensure pieces are clear and consistent.
	Prevention	▪ Secure buildings, rooms, and storage areas not in regular use. Maintain a list of secured areas or facilities and monitor activity in these areas.
	Protection	▪ Control access to mission critical facilities.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
ELEVATED (YELLOW) **Significant Risk of Terrorist Attack** Signifies an **elevated risk** of terrorist attacks. Protective measures should focus on increasing surveillance of critical facilities; coordinating response plans with allied utilities and response teams and local agencies; and implementing emergency plans, as appropriate.	Detection	▪ To the extent possible, increase the frequency and extent of monitoring activities and review results against baseline. ▪ Increase review of operational and analytical data (including customer complaints) with an eye toward detecting unusual variability (as an indicator of unexpected changes in the product). Variations due to natural or routine operational variability should be considered first. ▪ Increase surveillance activities in source and finished water areas.
	Preparedness	▪ Review and update emergency response procedures and communication protocols. ▪ Establish unannounced security spot checks (e.g., verification of personal identification and door security) at access control points for critical facilities. ▪ Increase frequency for posting employee reminders of the threat situation and about events that constitute security violations. ▪ Ensure employees understand notification protocol in the event of a security breach. ▪ Conduct security audit of physical security assets, such as fencing and lights, and repair or replace missing/broken assets. Remove debris from along fence-lines that could be stacked to facilitate scaling. ▪ Maximize physical control of all equipment and vehicles inoperable when not in-use, (e.g., lock steering wheels, secure keys, chain and padlock on front-end loaders, etc.). ▪ Review draft communications on potential incidents, brief media relations personnel of potential for press contact and/or issuance of release. ▪ Review and update list of sensitive populations within the service area, such as hospitals, nursing homes, daycare centers, schools, etc., for notification, as appropriate, in the event of a specific threat against the utility. ▪ Contact neighboring water utilities to review coordinated response plans and mutual aid during emergencies. ▪ Review whether critical replacement parts are available and accessible.
	Prevention	▪ Carefully review all facility tour requests before approving. If allowed, implement security measures to include list of names prior to tour, request identification of each attendee prior to tour, prohibit backpacks/duffle bags, cameras and identify parking restrictions. ▪ On a daily basis, inspect the interior and exterior of buildings in regular use for suspicious activity or packages, signs of tampering, or indications of unauthorized entry. ▪ Implement mailroom security procedures. Follow guidance provided by the United States Postal Service.
	Protection	▪ Verify the identity of all personnel entering the water utility. Mandate visible use of identification badges. Randomly check identification badges and cards of those on the premises. ▪ At the discretion of the facility manager or security director, remove all vehicles and objects (e.g., trash containers) located near mission critical facility security perimeters and other sensitive areas. ▪ Verify the security of critical information systems (e.g., Supervisory Control and Data Acquisition (SCADA), Internet, email, etc.) and review safe computer and internet access procedures with employees to prevent cyber intrusion. ▪ Consider steps needed to control access to all areas under the jurisdiction of the water utility.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
HIGH **(ORANGE)** **High Risk of Terrorist Attack** Signifies a **high risk** of terrorist attacks. Protective measures should focus on limiting facility access to essential staff and contractors, and coordinating security efforts with local law enforcement officials and the armed forces, as appropriate.	Detection	▪ Increase the frequency and extent of monitoring activities. Review results against baseline. ▪ Confirm that county and state health officials are on high alert and will inform water utilities of any potential waterborne illnesses. ▪ If a neighborhood watch-type program is in place, notify the community and request increased awareness.
	Preparedness	▪ Confirm emergency response and laboratory analytical support network are ready for deployment 24 hours per day, 7 days a week. ▪ Reaffirm liaison with local police, intelligence, and security agencies to determine likelihood of an attack on the water utility personnel and facility and consider appropriate protective measures (e.g., road closing, extra surveillance, etc.). ▪ Practice communications protocol with local authorities and others cited in the facility's emergency response plan. ▪ Post frequent reminders for staff and contractors of the threat level, along with a reminder of what events constitute security violations. ▪ Ensure employees are fully aware of emergency response communication protocols and have access to contact information for relevant law enforcement, public health, environmental protection, and emergency response organizations. ▪ Inspect and practice activation of available emergency interconnections with neighboring water agencies. ▪ Have alternative water supply plan ready to implement (e.g., bottled water delivery).
	Prevention	▪ Discontinue tours and prohibit public access to all operational facilities. ▪ Consider requesting increased law enforcement surveillance, particularly of critical assets and otherwise unprotected areas.
	Protection	▪ Evaluate need to staff water treatment/production facility at all times. ▪ Consider the need to prohibit recreational use of surface water reservoirs. ▪ Increase security patrol activity to the maximum level sustainable and ensure tight security in the vicinity of mission critical facilities. Vary the timing of security patrols. ▪ Request employees change password on critical information management systems.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
SEVERE (RED) **Severe Risk of Terrorist Attack** **Signifies a *severe risk* of terrorist attacks. Protective measures should focus on the decision to close specific facilities and the redirection of staff resources to critical operations.**	Detection	▪ Ensure that list of sensitive populations (e.g., hospitals, nursing homes, daycare centers, schools, etc.) within the service area is accurate and shared with appropriate public health officials. ▪ Reconfirm that county and state health officials are on high alert and will inform water utilities of any potential waterborne illnesses.
	Preparedness	▪ Post daily notices to staff regarding threat level and appropriate security practices ▪ Where appropriate, place back-up operational capacity on-line (water treatment plant filters, turbines, etc.). ▪ Ensure key utility personnel are on duty. ▪ Where appropriate, provide public notification for citizens to store emergency water supply or to implement other preparatory measures. ▪ Evaluate the need for opening an emergency operations center.
	Prevention	▪ As appropriate, request increased law enforcement and/or security agency surveillance, particularly of critical assets and otherwise unprotected areas (e.g., consider if National Guard assistance is needed and make appropriate request). ▪ Limit access to facilities and activities to essential personnel. ▪ Consider whether mail and packages should go to a central, secure location and be inspected before distribution. Remind mailroom personnel of the need for heightened awareness when sorting and distributing all incoming mail.
	Protection	▪ Ensure existing security policies, procedures, and equipment are effectively implemented. ▪ Recheck security of all on-site chemical storage and utilization areas. ▪ Implement frequent and staggered inspections of the exterior of buildings (to include roof areas) and parking areas. ▪ Re-check the security of critical information systems (e.g., SCADA, Internet, email, etc.) and have staff change computer passwords. ▪ Consider placing staff at remote (typically unmanned) facilities.

Appendix C: Example Action Plans

*Water System Contamination**

Threat Warning Stage

Threat Warning Received	Special actions and notifications to be taken: • Notify ER Lead or Alternate ER Lead • Record and document all information pertaining to the threat warning • Do not disturb site if the threat warning could be a possible crime scene • Return to normal operations if no further action is required (i.e., the threat warning can be explained) • Begin the "Threat Decision Process" if the threat warning cannot be explained

↓

Threat Decision Process Stage

Is the Threat Possible? (Stage 1)	Special actions and notifications to be taken: • Notify local law enforcement • Notify State Drinking Water Primacy Agency • Evaluate threat warning and make decisions in consultation with State Drinking Water Primacy Agency and local law enforcement • Initiate basic precautionary measures: 1. Alert staff and personnel about threat warning 2. Prepare additional notification lists if the situation escalates to the "Is the Threat Credible?" stage

↓

If the threat is not possible, then return to normal operations. Otherwise, proceed to "Is the Threat Credible" stage.

Is the Threat Credible? (Stage 2)	Special actions and notifications to be taken: • Activate notification and personnel safety portions of ERP • Evaluate whether the threat is credible in consultation with assisting agencies • Visually inspect physical evidence and determine whether there is a change in normal system operating parameters (i.e., chlorine residuals, turbidity, odor, color, pH, etc.) • Conduct actions and testing as recommended by monitoring and sampling experts

↓

If the threat is not credible, then return to normal operations. Otherwise, proceed to "Has the Threat been Confirmed" stage.

Has the Incident Been Confirmed? (Stage 3)	Special actions and notifications to be taken: • Initiate full ERP activation • Follow State Incident Command System • Isolate portion of system or backflush • Shut down system if obvious or confirmed contamination warrants • Issue public notice and issue follow-up media press releases • Continue sampling and water monitoring • Assess need to remediate storage tanks, filters, sediment basins, solids handling, etc.

*This is a simplified Action Plan example that includes the threat decision process to determine if the major event is just a threat or actual event. You should develop this "Action Plan" specific to the needs of your CWS and surrounding community.

*Structural Damage/Physical Attack to Water System or Facility(ies)**

Threat Warning Stage

Threat Warning Received	Special actions and notifications to be taken: • Notify ER Lead or Alternate ER Lead • Record and document all information pertaining to the threat warning • Do not disturb site if the threat warning could be a possible crime scene • Return to normal operations if no further action is required (i.e., the threat warning can be explained) • Begin the "Threat Decision Process" if the threat warning cannot be explained

Threat Decision Process Stage

Is the Threat Possible? (Stage 1)	Special actions and notifications to be taken: • Notify local law enforcement • Notify State Drinking Water Primacy Agency • Evaluate threat warning and make decisions in consultation with State Drinking Water Primacy Agency and local law enforcement • Initiate basic precautionary measures: 1. Alert staff and personnel about threat warning 2. Heighten security at critical facilities 3. Prepare additional notification lists if the situation escalates to the "Is the Threat Credible?" stage

If the threat is not possible, then return to normal operations. Otherwise, proceed to "Is the Threat Credible" stage.

Is the Threat Credible? (Stage 2)	Special actions and notifications to be taken: • Activate notification and personnel safety portions of ERP • Physically secure water system facilities • Evaluate whether the threat is credible in consultation with assisting agencies

If the threat is not credible, then return to normal operations. Otherwise, proceed to "Has the Threat been Confirmed" stage.

Has the Incident Been Confirmed? (Stage 3)	Special actions and notifications to be taken: • Initiate full ERP activation • Follow State Incident Command System • Deploy damage assessment team • Isolate damaged facility from rest of water system • Coordinate alternative water supply, as needed, or consider alternate (interim) treatment schemes • Issue public notice and issue follow-up media press releases • Repair damaged facilities • Assess need for additional protection/security measures

*This is a simplified Action Plan example that includes the threat decision process to determine if the major event is just a threat or actual event. You should develop this "Action Plan" specific to the needs of your CWS and surrounding community.

*Cyber Attack on SCADA or Operational Computer System**

Threat Warning Stage

Threat Warning Received	Special actions and notifications to be taken: • Notify ER Lead or Alternate ER Lead • Record and document all information pertaining to the threat warning • Do not disturb site if the threat warning could be a possible crime scene • Return to normal operations if no further action is required (i.e., the threat warning can be explained) • Begin the "Threat Decision Process" if the threat warning cannot be explained

Threat Decision Process Stage

Is the Threat Possible? (Stage 1)	Special actions and notifications to be taken: • Notify local law enforcement • Notify State Drinking Water Primacy Agency • Evaluate threat warning and make decisions in consultation with State Drinking Water Primacy Agency and local law enforcement • Initiate basic precautionary measures: 1. Alert staff and personnel about threat warning 2. Temporarily shut down SCADA system and go to manual operation using established protocol 3. Prepare additional notification lists if the situation escalates to the "Is the Threat Credible?" stage

If the threat is not possible, then return to normal operations. Otherwise, proceed to "Is the Threat Credible" stage.

Is the Threat Credible? (Stage 2)	Special actions and notifications to be taken: • Activate notification and personnel safety portions of ERP • Continue manual operation using established protocol • Consider whether to isolate source water • Consider whether to shut down system and provide alternate water • Evaluate whether the threat is credible in consultation with assisting agencies • Conduct actions/testing recommended by monitoring and sampling experts

If the threat is not credible, then return to normal operations. Otherwise, proceed to "Has the Threat been Confirmed" stage.

Has the Incident Been Confirmed? (Stage 3)	Special actions and notifications to be taken: • Initiate full ERP activation • Follow State Incident Command System • Continue manual operation, source water isolation, or system shut down and alternate water supply, as appropriate • Issue public notice and issue follow-up media press releases • Make image copy of all system logs to preserve evidence • With law enforcement assistance, check for implanted backdoors and other malicious code before restarting SCADA system • Install safeguards before restarting SCADA system • Bring SCADA system up and monitor system • Assess/implement additional precautions for SCADA system

*This is a simplified Action Plan example that includes the threat decision process to determine if the major event is just a threat or actual event. You should develop this "Action Plan" specific to the needs of your CWS and surrounding community.

*Hazardous Chemical Release from Water System Facility(ies)**

Threat Warning Stage

Threat Warning Received	Special actions and notifications to be taken: • Notify ER Lead or Alternate ER Lead • Record and document all information pertaining to the threat warning • Do not disturb site if the threat warning could be a possible crime scene • Return to normal operations if no further action is required (i.e., the threat warning can be explained) • Begin the "Threat Decision Process" if the threat warning cannot be explained

↓

Threat Decision Process Stage

Is the Threat Possible? (Stage 1)	Special actions and notifications to be taken: • Notify local law enforcement • Notify State Drinking Water Primacy Agency • Evaluate threat warning and make decisions in consultation with State Drinking Water Primacy Agency and local law enforcement • Initiate basic precautionary measures: 1. Alert staff and personnel about threat warning 2. Post full-time operations personnel at the chemical treatment areas of the facility 3. Verify that monitoring, leak detection, and personal protection equipment are fully operational 4. Prepare additional notification lists if the situation escalates to the "Is the Threat Credible?" stage

↓

If the threat is not possible, then return to normal operations. Otherwise, proceed to "Is the Threat Credible" stage.

Is the Threat Credible? (Stage 2)	Special actions and notifications to be taken: • Activate notification and personnel safety portions of ERP • Physically secure water system facilities and specifically the chemical treatment areas of the facility • Identify potentially hazardous chemical(s) to appropriate assisting agencies • Based on Risk Management program and ERP, evaluate potential extent of public evacuation or shelter in place order • Evaluate whether the threat is credible in consultation with assisting agencies

↓

If the threat is not credible, then return to normal operations. Otherwise, proceed to "Has the Threat Been Confirmed" stage.

Has the Incident Been Confirmed? (Stage 3)	Special actions and notifications to be taken: • Initiate full ERP activation • Follow State Incident Command System • Determine extent/concentration of chemical release and deploy damage assessment team • Turn off chemical treatment equipment and isolate chemical treatment areas from rest of water system • Depending on extent and concentration of release, issue evacuation or shelter in place order per Risk Management Program and ERP • Coordinate alternative water supply, as needed, or consider alternate (interim) treatment schemes • Issue public notice and issue follow-up media press releases • Repair damaged facilities • Assess need for additional protection/security measures

*This is a simplified Action Plan example that includes the threat decision process to determine if the major event is just a threat or actual event. You should develop this "Action Plan" specific to the needs of your CWS and surrounding community.