



**Instructions to Assist Community Water Systems
in Complying with the
Public Health Security and Bioterrorism
Preparedness and Response Act of 2002**

Office of Water
EPA 810-B-02-001
January 2003

www.epa.gov/safewater/security

Table of Contents

Sections

1. Introduction and purpose of these Instructions
2. Instructions At-A-Glance
3. What a CWS must do to comply with requirements of the Bioterrorism Act
4. Key dates for compliance with the requirements of the Bioterrorism Act
5. Determination of the size of the population the CWS serves
6. How to Submit VA Certifications, VAs, and ERP Certifications to EPA
7. Additional Information on Vulnerability Assessments (VAs)– components of a CWS the Bioterrorism Act requires a VA to cover; guidance on a VA's elements.
8. List of Acronyms

Appendices

1. Vulnerability Assessment Certification
2. Points to consider in Vulnerability Assessments
3. Mailing label to use for courier deliveries of items submitted to EPA; Recommended delivery address
4. Certification of Completion of an Emergency Response Plan

Instructions to Assist Community Water Systems in Complying With the Public Health Security and Bioterrorism Preparedness and Response Act of 2002

Long Title:

Instructions to community water systems: Guidance on how to comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 with respect to the certification and submission of Vulnerability Assessments to the US Environmental Protection Agency (EPA) and certification to EPA of completion of Emergency Response Plans.

1. Introduction and Purpose of these Instructions:

On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) into Law (PL 107-188). The Bioterrorism Act amends the Safe Drinking Water Act (SDWA) by adding section 1433. Section 1433(a) requires that certain community water systems (CWS) conduct Vulnerability Assessments (VAs), certify to EPA that the VAs were conducted, and submit a copy of the VA to EPA. Section 1433(b) requires that certain CWSs prepare or revise Emergency Response Plans (ERPs) and certify to EPA that an (ERP) has been completed.

We have prepared these *Instructions to Assist Community Water Systems in Complying With the Bioterrorism Act's* specific requirements and its deadlines for submission of VA and ERP documents.

Disclaimer: Please note that these Instructions are intended to provide information and recommendations to community water systems (CWSs) on how to comply with the Bioterrorism Act. The statutory provisions contained in the Bioterrorism Act are repeated in these Instructions and are legally binding requirements. The Instructions provided here do not substitute or expand upon these statutory requirements. Furthermore, adherence to these Instructions is not required where the discussed actions are not specifically required by the Bioterrorism Act; rather, following Instructions that are identified as suggestions are strictly voluntary for both EPA and affected CWSs. In addition, these Instructions may not apply to a particular situation based upon the circumstances. EPA decision-makers retain the discretion to adopt approaches on a case-by-case basis, which may differ from these Instructions where appropriate. Any decisions regarding a particular facility will be made based on the applicable statutory provisions. Therefore, interested parties are free to raise questions and objections about the appropriateness of the application of these Instructions to a particular situation and EPA will consider whether or not the recommendations or interpretations in the Instructions are appropriate in that situation based on the Bioterrorism Act or other relevant law. EPA may change these Instructions in the future as experience or other circumstances warrant.

2. Instructions At-A-Glance

What you, as the owner or operator of community water system should do, in brief, and where to look for additional information. (Throughout these Instructions, reference to “you” means the collective group of persons or those individuals involved in the work necessary to enable the community water system to comply with the Bioterrorism Act. This includes but is not limited to, the community water system’s owner(s), operator(s), authorized representative(s), and other employees.)

The following are the most frequently asked questions concerning compliance with the Bioterrorism Act. Following each answer are notes indicating the sections of the Instructions where you can find detailed information. (The complete Instructions that follow Instructions At-A-Glance explain the things you should do to comply, in detail.)

2.1 I represent a community water system. What must I do to comply?

Answer: If you represent a community water system serving more than 3,300 people, you must:

1. Conduct a vulnerability assessment (Section 7 and Appendix 2);
2. Send a written and signed certification to EPA that the system has conducted a vulnerability assessment (Sections 6.1.1 and 6.1.2; Appendix 1);
3. send a copy of the vulnerability assessment to EPA (Sections 6.1.2 and 6.2; Appendix 3);
4. send a written certification to EPA that your system has completed an emergency response plan (Section 6.3 and Appendix 4).

2.2 The information in my vulnerability assessment is very important and sensitive. How do I make sure my submission gets to EPA safely and securely?

Answer: Follow the mailing and packaging instructions in sections 6.1.2 and 6.2. In brief, you should USE A COURIER SERVICE, send the documents to the Recommended Delivery Address in section 6.1.2, and use double envelopes and the proper package labels as discussed in section 6.2. Appendix 3 contains a mailing label for your convenience.

2.3 My system serves more than 3,300 persons. When must these actions be completed?

Answer: Systems of different sizes must comply by different deadline dates, with the largest systems required to comply by the earliest date. For example, the largest water systems—those that serve populations of 100,000 or greater—must certify to EPA that they conducted a vulnerability assessment and submit a copy of the assessment to EPA prior to March 31, 2003. Systems must also certify to EPA that they completed an emergency

response plan not later than six months after certifying the vulnerability assessment or by the dates shown in Table 1, whichever is sooner.

Smaller systems (those serving fewer than 100,000 persons) should refer to Table 1 within Section 4 to determine their deadlines for conducting and certifying vulnerability assessments, sending vulnerability assessments to EPA, and certifying emergency response plans to EPA.

2.4 How will EPA determine the number of people that a community water system serves, which will in turn determine the deadline with which the system must comply?

Answer: As a general matter, EPA will use the Safe Drinking Water Information System (SDWIS) data that was submitted to EPA by the States on July 1, 2002, as the information that determines a system's population size. The information is publicly available, is maintained in EPA's Safe Drinking Water Information System, and is on file with state drinking water administrators (Section 5).

2.5 I am responsible for a water system owned or operated by the federal government. The system's vulnerability assessment will contain officially classified information. How should I submit the vulnerability assessment to EPA? Are there additional precautions to observe?

Answer: EPA most strongly recommends that all US Government-classified documents, of any security classification, be hand delivered to EPA either by a representative of the government water system or by courier service. Follow the instructions in Section 6.2.1 for details.

2.6 Who should I call if I need more information?

Answer: You should call the EPA Safe Drinking Water Hotline at 800-426-4791. The Hotline staff can provide additional information or refer you to the correct EPA contact person. Refer to the document number: EPA 810-B-02-001, dated January 2003.

3. What a CWS must do to comply with requirements of the Bioterrorism Act:

CWSs serving populations more than 3,300 persons must comply with the Bioterrorism Act. The Bioterrorism Act requires these community water systems to:

1. Conduct a VA;
2. Certify to EPA that the CWS conducted a VA;
3. Submit a copy of the VA to EPA; and
4. Certify to EPA that the CWS has completed an ERP.

With respect to the VA submission, EPA encourages you to provide an Executive Summary of the VA, which summarizes the major system vulnerabilities and planned improvements to reduce the vulnerabilities. EPA also encourages you to provide a Table of Contents describing the VA by section and page number, including a page count to allow EPA to determine if the package, as received, is complete. Both of these items are optional and are not required by the Bioterrorism Act.

VA submissions need not include supporting documentation such as working papers, background or raw data, or other preparation or analytical materials. You may omit these items; however, if you omit these items, the VA itself should be complete and clear when reviewed on its own merits.

4. Key dates for compliance with the requirements of the Bioterrorism Act:

Table 1 provides the dates by which CWSs must comply with the above requirements. A discussion of how EPA will determine the size of the CWS follows Table 1.

TABLE 1

Column A Systems serving population* of:	Column B Submit VA and VA Certification** prior to:	Column C Certify ERP within 6 months of VA but no later than***:
100,000 persons or greater	March 31, 2003	September 30, 2003
50,000 to 99,999 persons	December 31, 2003	June 30, 2004
3,301 to 49,999 persons	June 30, 2004	December 31, 2004
* See also Section 6, below, for discussion of determination of system population size.	** Compliance with these deadlines is determined by the date of the postmark or the date the courier places on the mailing label of the submission.	*** VA certifications submitted to EPA earlier than the dates shown in Column B means that the CWS must submit an ERP certification <i>earlier</i> than the dates shown in Column C.

5. Determination of the size of the population the CWS serves:

In order to determine whether the system is subject to the above requirements and the deadline that applies to the system, you must determine your CWS's size.

The Agency will use data from the Safe Drinking Water Information System (SDWIS) to determine system size. This data was filed by States, as of July 1, 2002, and made available to the public on October 1, 2002. EPA will presume that the size of the CWS indicated by SDWIS on that date is the size of the system that must comply with the due dates shown in Table 1 for certification and submission of VAs, and for certification of ERPs.

CWSs that operate as wholesalers, who sell water to other systems, should count the populations of those systems in determining the size of their total populations served. For example, if a wholesale CWS has no retail customers, but serves four water systems each having 30,000 retail customers, EPA will presume, for compliance purposes, that

the wholesale CWS serves 120,000 persons and must comply with the deadlines shown in Table 1 for systems serving 100,000 persons or greater.

General SDWIS data are available from:

<http://www.epa.gov/safewater/data/getdata.html>

Useful information on populations served by CWSs can also be obtained from State Drinking Water Administrators.

If you are unclear about whether the system is subject to the Act's requirements or which deadlines apply to the system, or if you have additional information relevant to determining the size of the system, we strongly recommend that you contact your State for a system-specific assessment. Systems that are operated on tribal lands, in the state of Wyoming, and in the District of Columbia should consult directly with EPA for final determinations of system sizes.

6. How to Submit VA Certifications, VAs, and ERP Certifications to EPA

6.1 Submission of VA Certifications

6.1.1. Content of a VA Certification:

If the CWS serves a population greater than 3,300, then the CWS is required to certify to EPA that it has conducted a VA. EPA recommends that you submit the certification to EPA along with the required copy of the VA itself. The certification may be sent prior to sending a copy of the VA, but EPA recommends sending both at the same time.

EPA suggests that you use the standardized certification form in Appendix 1 of these Instructions to certify to EPA that you have conducted a VA. The form is provided as a guide and is not required for this purpose. If you decide to use your own format for certifying that a VA was conducted, we recommend that the certification include the following language, printed on the CWS letterhead, above the signature of the authorized CWS representative:

“I certify to the Administrator of the U.S. Environmental Protection Agency that this community water system has conducted a vulnerability assessment that complies with Section 1433(a)(1) 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 and all attachments were 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 VA addresses the following components of the CWS: ‘pipes and constructed conveyances, physical barriers, water collection, pretreatment, treatment, storage and distribution facilities, electronic, computer or other automated systems which are utilized by the public water system, the use, storage, or handling of various chemicals, the operation and maintenance of such system.’”

[For those parts of the system that are applicable to the CWS, indicate whether the VA addressed each part. For those parts that are not applicable, indicate so.]

The Certification should also include the following information:

- A. name, address, telephone number, email address if available, and Federal Public Water System Identification Number (PWSID#) of the CWS;
- B. Name(s), title(s), address(es), telephone number(s), and email address(es) of two persons designated by the Community Water System that EPA may contact with questions about the assessment (main contact person and alternate);

You should keep and securely file a copy of this form.

The owner, manager, Certified Operator, or other Authorized Representative of the water utility **must sign** the certification form. That person should have responsibility over the management and daily operation of the CWS, as well as knowledge of the development of the VA.

6.1.2 Mailing a VA Certification to EPA:

You must send a signed original certification form (Appendix 1 or another version of the Certification) to EPA on or before the dates shown in Column B of Table 1. You may also submit a copy of the VA in this package, along with the VA Certification. **If you choose to submit the Certification and VA together in one package (EPA recommends this), please be sure to read Section 6.2, entitled “Instructions specific to submitting the Vulnerability Assessment.”**

Recommended Delivery Address:

We recommend that you submit the VA Certification using an express or courier service such as Federal Express, United Parcel Service, Airborne, etc., which provides tracking and certification of delivery. Using 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 EPA. 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. (For convenience, a mailing label with this address appears in Appendix 3, which the CWS can also use.)

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

Address to Use for US Postal Service Delivery (NOT RECOMMENDED):

If the CWS chooses to use US Postal Service delivery (any of their modes of delivery including certified mail, registered mail, express mail, and first class, etc.), use the following address. **EPA does not recommend using US Postal Service delivery because the shipment cannot always be tracked during transit. Also, there can be significant delays in the postal system's deliveries to EPA due to decontamination irradiation of the mail, which may also damage or destroy the submission.**

Use a double envelope and put this address on the **OUTER** envelope:

Attention: Janet Pawlukiewicz
Mail Code: 4601M
U.S. Environmental Protection Agency
1200 Pennsylvania Ave., NW
Washington DC 20460

6.2 Instructions specific to submitting the Vulnerability Assessment:

The CWS should use these instructions when submitting a copy of the VA to EPA or if submitting the Certification of Conduct of a VA **AND** a copy of the VA together in one package.

You should use the “Recommended Delivery Address” shown in the above Section 6.1.2. **EPA strongly recommends that the CWS send the VAs to EPA sealed in two envelopes, one inside the other. No reference should be made on the outer envelope to its contents.** Avoid the use of markings on the outer envelope that may lead someone to know what it contains. Do NOT use words such as “vulnerability assessment,” “confidential,” “Water Protection Task Force,” “Bioterrorism Act,” etc.

The inside envelope should be sealed, and marked “**TO BE OPENED BY ADDRESSEE ONLY–Janet Pawlukiewicz.**” The outside envelope should be

addressed to the Recommended Delivery Address shown above.

6.2.1 Special Instructions for Water Systems Owned or Operated by the Federal Government:

If the CWS classifies the VA under one of the federal government's denoted security classifications (Confidential, Secret, Top Secret, etc.), it is very important that you make advance arrangements with EPA to properly receive your submission.

Call the following numbers to request that you be placed in contact with the Water Security Information Security Manager. The Information Security Manager or her designee will help you arrange a time for hand delivery of your submission directly to an EPA employee who possesses the appropriate security clearance:

202-564-9932 or
202-564-6186

6.3 Submission of Certification of Completion of an Emergency Response Plan (ERP) to the Administrator of EPA

6.3.1 Content of an ERP Certification:

If the CWS is required to conduct a VA, then you must also certify to EPA that you have completed an ERP. **(Do not submit a copy of the ERP to EPA.)** EPA suggests that you use the standardized certification form in Appendix 4 of these Instructions to certify to EPA that the CWS has completed an ERP. The form is provided as a guide and is not required for this purpose. If you use your own format for certifying that you have completed an ERP, the certification should include the following language above the signature of the authorized CWS representative:

"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 and all attachments were 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.”

The Certification should also include the following information:

- A. name, address, telephone number, email address if available, and Federal Public Water System Identification Number (PWSID#) of the CWS;
- B. name(s), title(s), address(es), telephone number(s), and email address(es) of two persons designated by the CWS that EPA may contact with questions about the plan (main contact person and alternate);

The Bioterrorism Act requires that CWSs maintain a copy of the emergency response plan for five years after such plan is certified to EPA.

6.3.2 **Mailing an ERP Certification to EPA**

Follow the mailing instructions above under Section 6.1.2, “Recommended Delivery Address,” discussing mailing VA certifications to EPA.

7. **Additional Information on Vulnerability Assessments (VAs)–components of a CWS the Bioterrorism Act requires a VA to cover; guidance on a VA’s elements**

7.1 **Vulnerability Assessment– components of a CWS that a VA must address:**

Each CWS that serves a population greater than 3,300 persons must perform an assessment of the vulnerability of its system to a terrorist attack or other intentional acts that are intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. This is a “vulnerability assessment” and is discussed further in the Bioterrorism Act as follows. **These components must be addressed in the VA, to the extent they are applicable to the CWS, in order to comply with the Bioterrorism Act:**

“The vulnerability assessment shall include, but not be limited to a review of:
[1.] pipes and constructed conveyances,
[2.] physical barriers,
[3.] water collection, pretreatment, treatment, storage and distribution facilities,
[4.] electronic, computer or other automated systems which are utilized by the public water system,
[5.] the use, storage, or handling of various chemicals, and
[6.] the operation and maintenance of such system.”

7.2 Additional Information on the elements of a VA:

EPA has provided additional information about VAs and related security topics to CWSs in the document entitled *Baseline Threat Information for Vulnerability Assessments of Community Water Systems* (Baseline Threat Document). The Baseline Threat Document is not a blueprint for developing a VA, however, it does present an overview of threats, methodologies, and strategies for the CWS to consider as it develops a VA required under the Bioterrorism Act.

A VA generally should address six basic elements, as they were outlined in the Baseline Threat Document¹. A VA is performance based, meaning that it evaluates the risk to the water system based on the effectiveness (performance) of existing and planned measures to counteract potential adversarial actions. The VA elements are:

1. Characterization of the water system, including its mission and objectives;
2. Identification and prioritization of adverse consequences to avoid;
3. Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences;
4. Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries (e.g., terrorists, vandals);
5. Evaluation of existing countermeasures; and
6. Analysis of current risk and development of a prioritized plan for risk reduction.

¹See also, Appendix 2 to these Instructions entitled “Points to Consider in Vulnerability Assessments.” This Appendix provides additional discussion of these six elements.

8. List of Acronyms

CWS	Community Water System
EPA	US Environmental Protection Agency
ERP	Emergency Response Plan
SDWA	Safe Drinking Water Act, as amended
SDWIS	Safe Drinking Water Information System
VA	Vulnerability Assessment

Appendix 1

VULNERABILITY ASSESSMENT CERTIFICATION

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 conducted a vulnerability assessment that complies with Section 1433(a)(1) 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 and all attachments were 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 vulnerability assessment this community water system conducted addresses the following components of my system (Check YES if the CWS has the element in its system; check N/A if the element is not applicable to the system.):

YES N/A

- | | | |
|--------------------------|--------------------------|-----------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | pipes and constructed conveyances |
| <input type="checkbox"/> | <input type="checkbox"/> | physical barriers |

- water collection
- pretreatment
- treatment
- storage
- distribution facilities
- electronic, computer or other automated systems which are utilized by the public water system
- the use, storage, or handling of various chemicals
- the operation and maintenance of such system

Other components in the CWS that were evaluated under this VA (list those applicable):

Signed: _____ **Date:** _____

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

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: _____

Appendix 2

Points to Consider in Vulnerability Assessments

Points to consider related to the six basic elements of a vulnerability assessment are included below. The manner in which the vulnerability assessment is performed is determined by each individual water utility. It will be helpful to remember throughout the assessment process that the ultimate goal is twofold: to safeguard public health and safety, and to reduce the potential for disruption of a reliable supply of pressurized water.

1. **Characterization of the water system, including its mission and objectives.**

Answers to the following system-specific questions may be helpful in characterizing the water system.

What are the important missions of the system to be assessed? Define the highest priority services provided by the utility. Identify the utility's critical customers (e.g., public, government, military, industrial, critical care, retail operations, firefighters).

What are the most important facilities, processes, and assets of the system for achieving the mission objectives and avoiding undesired consequences? Describe the utility facilities, operating procedures, and management practices that are necessary to achieve the mission objectives. Describe how the utility operates (e.g., water source, including ground and surface water, treatment process, storage methods and capacity, chemical use and storage, and distribution system). In assessing those assets that are critical, consider critical customers, dependence on other infrastructures (e.g., electricity, transportation, other water utilities), contractual obligations, single points of failure (e.g., critical aqueducts, transmission systems, aquifers, etc.), chemical hazards and other aspects of the utility's operations, or availability of other utility capabilities that may increase or decrease the criticality of specific facilities, processes, and assets.

2. **Identification and prioritization of adverse consequences to avoid.**

When considering adverse consequences, the water system should take into account the impacts that could substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water or otherwise present significant public health concerns to the surrounding community. In general, water systems should use the vulnerability assessment process to determine how to reduce risks associated with the consequences of significant concern.

Ranges of consequences or impacts for each of these events should be identified and defined. Factors to be considered in assessing the consequences may include: magnitude

of service disruption; economic impact (such as replacement and installation costs for damaged critical assets or loss of revenue due to service outage); number of illnesses or deaths resulting from an event; impact on public confidence in the water supply; chronic problems arising from specific events; or other indicators of the impact of each event as determined by the water utility. Risk reduction recommendations at the conclusion of the vulnerability assessment should strive to prevent or reduce each of these consequences.

3. Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences.

What are the malevolent acts that could reasonably cause undesired consequences?

Consider the operation of critical facilities, assets, and/or processes, and assess what an adversary could do to disrupt these operations. Such acts may include physical damage to or destruction of critical assets, contamination of water, intentional release of stored chemicals, interruption of electricity or other infrastructure interdependencies.

Regarding water system vulnerabilities and determination of *critical assets*, the utility should review the potential for physical damage to the water system's infrastructure, including:

1. Pipes and constructed conveyances
2. Physical barriers
3. Water collection, pretreatment and treatment
4. Storage and distribution facilities
5. Electronic, computer or other automated systems that are utilized by the public water system (e.g., Supervisory Control and Data Acquisition (SCADA))
6. The use, storage, or handling of various chemicals
7. The operation and maintenance of such systems

The water system's vulnerabilities should also be reviewed for threats with the potential to significantly affect public health, such as chemical, biological, radiological, and other types of contamination.

4. Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries (e.g., terrorists, vandals).

Based on the critical *assets* of the water system, one can determine the possible modes of attack that might result in *consequences of significant concern*. However, the objective of this step of the assessment is to move beyond what is merely possible and determine the likelihood of a particular attack scenario. This is a very difficult task as there is often insufficient information to determine the likelihood of a particular event with any degree of certainty.

The threats (the kind of adversary and the mode of attack) selected for consideration during a vulnerability assessment will dictate, to a great extent, the risk reduction measures that should be designed to counter the threat(s). Some vulnerability assessment methodologies refer to this as a Design Basis Threat (DBT) where the threat serves as the basis for the design of countermeasures, as well as the benchmark against which vulnerabilities are assessed. It should be noted that there is no single DBT or threat profile for all water systems in the United States. Differences in geographic location, size of the utility, previous attacks in the local area, and many other factors will influence the threat(s) that water systems should consider in their assessments. From this perspective, water systems should consult with the local FBI and/or other law enforcement agencies, public officials, and others to determine the threats upon which their risk reduction measures should be based. Utilities may also want to review their incident reports to better understand past breaches of security.

5. Evaluation of existing countermeasures.

Having determined how various *critical assets, processes, and operations* are related to the system's mission and the potential for malevolent actions to cause adverse consequences, the effectiveness of existing security measures and operational practices should be considered. Depending on countermeasures already in place, some critical assets may already be sufficiently protected. This step will aid in identification of the areas of greatest concern, and help to focus priorities for risk reduction.

What capabilities does the system currently employ for detection, delay, and response? Identify and evaluate current detection capabilities such as intrusion detection systems, water quality monitoring, operational alarms, guard post orders, and employee security awareness programs. Identify current delay mechanisms such as locks and key control, fencing, structure integrity of critical assets and vehicle access checkpoints. Identify existing policies and procedures for evaluation and response to intrusion and system malfunction alarms, adverse water quality indicators, and cyber system intrusions. It is important to determine the performance characteristics. Poorly operated and maintained security technologies provide little or no protection.

What cyber protection system features does the utility have in place? Assess what protective measures are in-place for the Supervisory Control and Data Acquisition (SCADA) and business-related computer information systems such as fire walls, modem access, Internet, and other external connections, including wireless data and voice communications, and security policies and protocols. Identify whether vendors have access rights and/or "backdoors" to conduct system diagnostics remotely.

What security policies and procedures exist, and what is the compliance record for them? Identify existing policies and procedures concerning personnel security, physical security, key and access badge control, control of system configuration and operational data, chemical and other vendor deliveries, and security training and exercise records.

6. Analysis of current risk and development of a prioritized plan for risk reduction.

The information gathered on threat, critical assets, water utility operations, consequences, and existing countermeasures should be analyzed to determine the current level of risk. The utility should then determine whether current risks are acceptable or risk reduction measures should be pursued.

Recommended actions should measurably reduce risks by reducing vulnerabilities and/or consequences through improved deterrence, delay, detection, and or response capabilities or by improving operational policies or procedures. Selection of specific risk reduction actions should be completed prior to considering the cost of the recommended action(s). Utilities should carefully consider both short- and long-term solutions. An analysis of the cost of short- and long-term risk reduction actions may impact which actions the utility chooses to achieve its security goals. Utilities may also want to consider security improvements in light of other planned or needed improvements. Security and general infrastructure may provide significant multiple benefits. For example, improved treatment processes or system redundancies can both reduce vulnerabilities and enhance day-to-day operation.

Generally, strategies for reducing vulnerabilities fall into three broad categories: 1) sound business practices, 2) system upgrades, and 3) security upgrades. Sound business practices affect policies, procedures, and training to improve the overall security-related culture at the drinking water facility. For example, it is important to ensure rapid communication capabilities exist between public health authorities and local law enforcement and emergency responders. System upgrades include changes in operations, equipment, processes, or infrastructure itself that make the system fundamentally safer. Security upgrades improve capabilities for detection, delay, or response.

Appendix 3

Mailing Label to use for courier deliveries of items submitted to EPA; Recommended Delivery Address

Use this label ONLY if you are using an express direct-delivery courier such as Federal Express, UPS, Airborne, and so forth.

DO NOT USE THIS ADDRESS FOR ANY FORM OF US POSTAL SERVICE DELIVERY. See Instructions Section 6.1.2 for the address to use for postal delivery.

Be sure to give the courier service this phone number, so they can be authorized entrance to the building, if so requested by building guards: 202-566-1729.

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

Appendix 4

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: _____