

WATER

2003 WATER SYSTEM VULNERABILITY

ASSESSMENT

35.

Austin White Lime Company

P.O. Box 9556

Austin, Texas 78766



**CHEMICAL, BUILDING
AND
STABILIZATION LIME**

PHONE 512-255-3646

800-553-5463

FAX 512-388-1220

EPA - 214-665-6444

Water Supply Office

Call Greg Grover, EPA

214-665-2776

for Public Water Sept

ID. # TX 0570031

Jim Amick — LAN
did the VA for
Bedford —

9/23/03

Emergency Response Plan

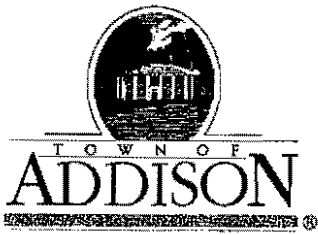
No need to go to infinite level of detail

Take care of the critical features of the system

Critical assets, threats, what can be done

10-15K range for the VA

10-15K range for Emergency Response Plan



PUBLIC WORKS DEPARTMENT

Post Office Box 9010 Addison, Texas 75001-9010

(972) 450-2871

16801 Westgrove

October 14, 2003

Sedi A. Toumani, P.E., President
DAL-TECH Engineering, Inc.
17311 Dallas Parkway, Suite 200
Dallas, TX 75248

Re: Water System Vulnerability Assessment

Dear Ms. Toumani:

This is to acknowledge receipt of your revised fee proposal dated October 10, 2003 regarding the above referenced project.

We appreciate all the time and effort that you have put into your fee proposals but as you know, our budget for this project is significantly less than your revised proposal.

Accordingly, we are closing the negotiation process with DAL-TECH Engineering, Inc. on this project and will begin negotiations with the second ranked firm.

We hope that you will continue to seek work with the Town of Addison.

Very truly yours,

Town of Addison

James C. Pierce, Jr., P.E.
Assistant Public Works Director

cc: Chris Terry, Assistant City Manager
Michael E. Murphy, P.E., Director of Public Works

DAL-TECH
ENGINEERING, INC.
CONSULTING CIVIL ENGINEERS / SURVEYORS
CONSTRUCTION MANAGERS

October 10, 2003

Mr. Jim Pierce, P.E.
Assistant Public Works Director
Town of Addison
16801 Westgrove
Addison, Texas 75024


**Re: Water System Vulnerability Assessment
Revised Fee Proposal
Addison, Texas
DTE Job 0304**

Dear Mr. Pierce:

DAL-TECH Engineering, Inc. (DTE) has revised the fee proposal for the above referenced project. DTE has reduced proposed hours, reduced the proposed meetings to three, and reduced the scope of the proposed subconsultant services. Attached is a copy of the fee proposal, revised contract scope, preliminary bar graph schedule and subconsultant fee proposal. DTE has tried really hard to reach the lowest possible fees for this project. DTE hopes that this is acceptable to you, and we hope that you would let us know if we could consider any other alternatives to meet the budget.

As always, if you have any questions, please do not hesitate to give us a call.

Sincerely,


Sedi A. Toumani, P.E.
President
SAT/dkj

Attachments

OVERVIEW

The **Town of Addison (Town)** and **DAL-Tech Engineering, Inc., (DTE)** agree to enter into a Special Services Contract for DTE to complete the Town's Vulnerability Assessment and Emergency Response Plan as required by the **Public Health Security and Bioterrorism Preparedness and Response Act of 2002** or (Bioterrorism Act) – (PL 107-188) which was signed into law on June 12, 2002. This law amends the Safe Drinking Water Act.

The Law applies to **Community Water System (CWS)** serving more than 3,300 persons

*	Complete by 6/30/04	3,300 persons > CWS > 49,999 persons
*	Complete by 12/31/03	50,000 persons > CWS > 99,999 persons
*	Complete by 3/31/03	100,000 persons > CWS
**	Complete by 12/31/04	3,300 persons > CWS > 49,999 persons
**	Complete by 6/30/04	50,000 persons > CWS > 99,999 persons
**	Complete by 9/30/03	100,000 persons > CWS

The Law requires:

- 1) Community Water System conduct a **Vulnerability Assessment**,
- 2) Community Water System certify and submit a copy of Vulnerability Assessment to the Administrator of the **Environmental Protection Agency (EPA)***,
- 3) Community Water System prepare or revise an **Emergency Response Plan** that incorporates the results of the Vulnerability Assessment and certify to the EPA Administrator that the Community Water System has completed Emergency Response Plan**.

The Purposes of the Vulnerability Assessment are:

- 1) Undertake risk-based vulnerability assessments of their assets;
- 2) Analyze potential adversarial threats; and
- 3) Consider potential modes of attack.

The Vulnerability Assessment includes six basic elements

- 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;

critical assets will include the following the Community Water System's infrastructure:

- a) pipes and constructed conveyances
 - b) physical barriers
 - c) water collection, pretreatment, treatment,
 - d) storage and distribution facilities
 - e) electronic, computer or other automated systems which are utilized by the public water system
 - f) the use, storage, or handling of various chemicals
 - g) the operation and maintenance of such system
- 4) Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries (e.g. terrorists, vandals, etc.);
 - 5) Evaluation of existing countermeasures; and
 - 6) Analysis of current risk and development of a prioritized plan for risk reduction.

The **Town of Addison (Town)** will:

- 1) provide **DAL-Tech Engineering, Inc., (DTE)** with the Baseline Threat Document received from the **Environmental Protection Agency (EPA)**;
- 2) provide DTE with the complete Town's water system inventory. The inventory will include, but may not be limited to the following components, including number, location and description of each item. The inventory document will be drafted in Microsoft Word.

Main (Water) Feed Points

Storage (Water) Tanks

Power

 Primary Power (Electric Feed)

 Secondary Power (Back up generators)

Distribution Pumps

Offices

 Buildings

 Computers

 Files

 Transportation and Work Vehicles

Communications

 Telephones

 Cell Phones

 Radio

 Computer Control System

SCADA

- 3) provide DTE with four paper copies of a 1"=200' scale map (9'x7.5') of Addison showing:
 - a) City Limit line, north arrow, bar scale;
 - b) Streets showing names;
 - c) water mains showing sizes, valves, fire hydrants, City of Dallas feed points;
 - d) pump stations, storage tanks showing existing fences with fence description;
 - e) emergency generators;
 - f) Town offices (i.e. fire station(s), police station(s), hospital(s), Mayor's office, Town Manager's office, Public Works office);
 - g) SCADA facilities (i.e. where they are located, what they monitor, what they control); and
 - h) chemical storage and feed facilities;

provide the Town with paper copy of the map on 11"x17" sheets to be included in the Vulnerability Assessment and Emergency Response Plan with all the above information.

- 4) provide on-site Town representative while DTE is performing investigation
- 5) provide DTE with the Town's policies and procedures in Microsoft Word concerning the water system. These policies and procedures will include, but not limited to the following components.

Water System Facility Security – i.e. Facilities are locked, fenced, gated, with limited access doors, vents on storage tanks are screened and securely fastened, the facilities have security lighting, signs, patrol, alarm system, and secure chemical storage, etc.

Water System Personnel – i.e. Personnel wear uniforms, ID cards, potential employees receive background checks prior to employment, terminated employees must return ID cards, etc.

Water System Computer Security – i.e. Access to computers is password protected, computers are regularly backed-up, the computers have internet firewall software, etc.

Water System Public Relations – i.e. System has a neighborhood watch, system has a procedure to respond to a customer's odor or taste complaint, system has procedure in place to immediately advise the community in case of danger, etc.

- 6) provide Town senior staff and meeting facility for no less than two meetings lasting approximately four hours each, and a two-hour conclusion meeting. The meetings are described in the Preliminary Schedule portion of the Scope. Senior staff would include a Town representative from the Police Department, Fire Department, Local Government, Public Works, and Health Department with decision-making authority;
- 7) provide Town representative (preferably from Public Works) with decision making authority and familiar with the contract to assist DTE;
- 8) review draft documents, maps, meeting notes, and any other information assembled by DTE;
- 9) certify to the EPA that the Vulnerability Assessment was conducted;
- 10) provide a copy of the Vulnerability Assessment to the EPA; and
- 11) certify to the EPA that the Emergency Response Plan was completed.

DAL-Tech Engineering, Inc., (DTE) will

- 1) provide the Town with the specific format that the written inventory should be prepared;
- 2) assist the Town in acquiring its inventory;
- 3) accumulate inventory of Town's water system in Microsoft Word document to be included in the Vulnerability Assessment;
- 4) conduct meeting(s), draft meeting notes, and draft meeting agendas;
- 5) make final corrections to maps, draft information, for the Vulnerability Assessment to comply with the Town's review comments
- 6) (from the results of the inventory and meetings) provide Addison with four original copies and one original electronic file of the Vulnerability Assessment;
- 7) make final corrections to maps, draft information, for the Emergency Response Plan to comply with the Town's review comments

- 8) (from the results of the inventory, meetings, and the Vulnerability Assessment) provide Addison with three original copies, and one original electronic file of the Emergency Response Plan;
- 9) provide security expert sub-consultant who visits water system facilities (including the pump stations, storage tanks, office facilities), assess facility weaknesses, make security recommendations, and prepare security assessment report that will be incorporated in the Vulnerability Assessment and Emergency Response Plan; and
- 10) provide security expert sub-consultant to participate in necessary meetings.

Cost Breakdown for Addison Vulnerability Assessment and Emergency Response Plan
 DAL-Tech Engineering, Inc.
 10/09/03

No.	Description	Project Manager		Assistant PM		Secretary		Printing, Sub Mark-up	Security Consultant	Total
		\$ 102.50	Hr	\$ 89.00	Hr	\$ 54.00	Hr			
1)	Prepare for and provide Town with VA format		15		6		8			\$ 2,503.50
2)	Visit Town facilities in acquiring inventory (with Town's assistance)		6		4					971.00
3a)	Accumulate, and organize Town's written inventory (with Town's assistance)		15		6		15			2,881.50
3b)	Accumulate and organize Town's maps, detail drawings, and schematic diagrams (with Town's assistance)		15		6		10			2,611.50
3c)	Accumulate and organize Town's Policies and Procedures (with Town's assistance)		15		6		10			2,611.50
4a)	Prepare for and conduct 1st Meeting, VA preparation and make copies		24		10		10	900.00		4,790.00
4b)	Prepare Meeting Notes, conduct 2nd Meeting, prepare ERP draft, revise VA		20		10		10	150.00		3,630.00
4c)	Complete ERP, Conduct Conclusion Meeting		24		10		10	150.00		4,040.00
5)	Final revisions to Vulnerability Assessment		16		10		10			3,070.00
6)	Provide Town With Four Original and One Electronic Copies of VA		10		4		8	600.00		2,413.00
7)	Final revisions to Emergency Response Plan		20		8		8			3,194.00
8)	Provide Town With Three Original and One Electronic Copies of ERP		10		4		8	450.00		2,263.00
9a)	Provide Security Consultant, Draft Report, Visit Town Facilities		4		2		2	1,610.00	16,100.00	18,406.00
9b)	Visit Jobsite with Security Consultant		8		4					1,176.00
9c)	Review Security Consultant's Report		4		4					766.00
10a)	Provide Security Consultant at 1st Meeting							112.60	1,126.00	1,238.60
10b)	Provide Security Consultant at 2nd Meeting							112.60	1,126.00	1,238.60
10c)	Provide Security Consultant at Conclusion Meeting							112.60	1,126.00	1,238.60

Total \$ 19,478.00 \$ 59,042.80

DAL-Tech Engineering, Inc. Total	\$ 39,564.80
Security Consultant (Kimmons Security Services, Inc.)	<u>\$ 19,478.00</u>
Total	\$ 59,042.80



Kimmons Security Services, Inc.
Investigations and Security Services

August 29, 2003

Mr. Matthew W. Stevens, P.E.
DAL-TECH ENGINEERING, INC.
17311 Dallas Parkway, Suite #200
Dallas, Texas 75248

**RE: VULNERABILITY (RISK) ASSESSMENTS
EMERGENCY RESPONSE PLANS**

Dear Mr. Stevens:

Thank you for your interest in our firms services in reference to **Vulnerability (Risk) Assessments and Emergency Response Plans for Municipalities and MUD Districts**. Below is some additional information concerning the Risk Assessment Services we provide. If you have any other specific questions, please do not hesitate to contact me.

The Vulnerability (Risk) Assessment is designed to evaluate threats to utility sites and identify key mitigation measures that can be implemented to address those possible threats. We believe our firm is uniquely qualified to provide these assessments, due to our vast experience in the security field. Our security experts have also attended the AWWA/EPA (RAM-W) seminar for Vulnerability Assessment training.

We work as a team when conducting a Risk Assessment. Our team consist of at least one security expert, a consultant from the water industry, and law enforcement representatives. We believe this team of security experts, separates us from other firms who offer similar services. We also install security systems for the protection of water and other utilities, which gives us unique insight regarding security concerns relating to these sites. Most of our employees are former law enforcement officers with many years of security experience.

A study for a site would include a review of the following: backgrounds on personnel, backgrounds on vendors and others who visit the site, security of records (system maps, accounting, customer list), emergency plan, source water storage, distribution system, electric power, transportation, transmission system checklist, treatment facility checklist, finished water storage, interdependent infrastructure, guideline information on emergency response, SCADA communications, emergency contacts, crisis communications planning and response. Also, if available, this report would include previous crime statistics in the area in order to provide valuable insight regarding the types of threats to be aware of and protect against. Please note that the below listed prices will also include an Emergency Response Plan for the sites.

2000 Dairy Ashford, Suite 300
Houston, Texas 77077

(281)679-0070
Fax (281)679-0080

www.kimmonssecurity.com

Page #2 Continued: VA's & ERP Pricing Dal-Tech Engineering, Inc.

The cost for conducting a Vulnerability (Risk) Assessment for a Municipality or Municipal Utility District, including a bound illustrated report and the Emergency Response Plan, would be \$5,000 for the first site plus travel and out of pocket expenses. If a district has more than one site or an administrative office, each additional site could be included for a discount of \$2,500 (plus out of pocket expenses). The out of pocket expenses would include photographs, copy cost, etc.

The following total will apply to the Town of Addison, Texas (6 sites):

*1 Elevated Storage Tank
\$5,000 plus travel and out of pocket expenses

*5 Additional Sites (2 Ground Storage Tanks and 3 City Buildings)
5 x \$2,500
\$12,500 plus out of pocket expenses.

Note: The out of pocket expenses would include approximately 512 miles travel (x) .50 cents per mile, food, lodging, and approximately 7 hours travel time (x) \$75 per hour. It is believed that all 6 sites could be surveyed in two (2) days.

TOTAL FOR VA's AND ERP's: \$17,500 plus out of pocket expenses.

The report would be a flat rate of \$750 plus photo cost.

(In lieu of retainer, full payment is due within 15 days upon delivery of completed reports.)

You can also review our firms web site at www.kimmonsandassociates.com for additional information. If you have any questions please feel free to contact me at 281-679-0070 or by e-mail at jim@kimmonsandassociates.com.

Sincerely,

KIMMONS SECURITY SERVICES, INC.


Rob L. Kimmons
President

APPROVED - DAL-TECH ENGINEERING, INC.

DATE

**2000 Dairy Ashford, Suite 300
Houston, Texas 77077**

www.kimmonssecurity.com

**(281)679-0070
Fax (281)679-0080**



Kimmons Security Services, Inc.
Investigations and Security Services

August 29, 2003

Mr. Matthew W. Stevens, P.E.
DAL-TECH ENGINEERING, INC.
 17311 Dallas Parkway, Suite #200
 Dallas, Texas 75248

RE: VULNERABILITY ASSESSMENT MEETINGS

Dear Mr. Stevens:

Per our conversation on this date, the following charges would be incurred for traveling from Houston to Dallas, Texas for Council Meetings, etc, in reference to the Vulnerability Assessments for Addison, Texas.

*Travel time from Houston to Dallas and return 3.5 hours each way 7 hours x \$75 per hour travel time	\$525.00
*Mileage from Houston to Dallas and return 256 miles each way 512 miles x .50 cents per mile	\$256.00
*Meeting with Dal-Tech Engineering and City Council 4 hours x \$75 per hour	\$300.00
*Meals	\$ 45.00
<u>TOTAL FOR EACH TRIP:</u>	<u>\$1,126.00</u>
Total For 5 Trips:	\$5,630.00

If you have any questions or need any additional information, please contact me at 281-679-0070.

Sincerely,

KIMMONS SECURITY SERVICES, INC.

James W. Dunbar
 James W. Dunbar
 Executive Vice President

2000 Dairy Ashford, Suite 300
 Houston, Texas 77077

www.kimmonsandassociates.com

(281)679-0070
 Fax (281)679-0080



Baseline Threat Information for Vulnerability Assessments of Community Water Systems

Notice: Limited Distribution. This document contains information that may not be appropriate for public dissemination. Do not copy or further distribute this document.

Larry Wright Region 6 1-800-887-6063



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
WATER

DRINKING WATER SECURITY INFORMATION

The U.S. EPA received your request and is providing you with the document, *Baseline Threat Information for Vulnerability Assessments of Community Water Systems*. Although it is not a blueprint for developing a vulnerability assessment, it does present an overview of threats, methodologies, and strategies for water utilities to consider as they develop vulnerability assessments. As you probably know, vulnerability assessments are required of all community water systems that serve a population greater than 3,300 persons under the Safe Drinking Water Act, amended by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

U.S. EPA requests that you take reasonable measures to:

- Hold all information contained in the document in confidence and take reasonable precautions to protect it;
- Limit access only to those with significant need for the information to assist with or perform water utility security planning; and
- Do not photocopy all or any portion of the document.

If you have further questions or need additional information, please visit the Web site at: <http://www.epa.gov/safewater/security> or contact the Safe Drinking Water Hotline by phone: 1-800-426-4791 or E-mail: hotline-sdwa@epa.gov.



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE ADMINISTRATOR

STATEMENT FROM THE ADMINISTRATOR

I am pleased to release to you this document, *Baseline Threat Information for Vulnerability Assessments of Community Water Systems*. The primary objective of this information document is to provide a framework for utility managers and their staffs to identify and evaluate vulnerabilities that could place the operation of the water utility, staff, and/or customers in harms way. I hope this document will be useful to drinking water utilities as they undertake the very important task of determining their vulnerabilities to attack and taking steps to improve the safety and security of their operations.

The U.S. Environmental Protection Agency (EPA) has developed this information document under Congressional mandate in the Public Health Security and Bioterrorism Response Act signed into law on June 12, 2002. The EPA received assistance in developing this document from other Federal Agencies such as the Federal Bureau of Investigation, water industry association representatives, and experts from a peer review panel sponsored by the National Academy of Sciences. I recognize the need to provide useful information and sound science, without unnecessary delay.

I wish you success in this important endeavor to protect our nation's critical water infrastructure on which millions of our citizens depend.


Christine Todd Whitman

ACKNOWLEDGEMENTS

The Environmental Protection Agency (EPA) would like to thank the following individuals who took the time and energy to review and submit comments as a part of the *Baseline Threat Information* development process. They are to be commended for their perseverance and dedication. Paul Bennett, New York City Department of Environmental Protection; David Binning, Fairfax County Water Authority; Frank Blaha, American Water Works Association Research Foundation; Peter Cook, National Association of Water Companies; Tom Curtis, American Water Works Association; Gregg Grunenfelder, Washington State Department of Health; Gerald Iwan, Connecticut Department of Public Health; Craig Jackson, New York State Department of Health; Bruce Larson, American Water Works Service Company; Vanessa Leiby, National Association of State Drinking Water Administration; Victor L' Esperance, Massachusetts Water Resource Authority; Jeff Mosher, Association of Metropolitan Water Agencies; Bridget O'Grady, Association of State Drinking Water Administration; Brian Ramaley, City of Newport News; Stephen Schmitt, American Water Works Service Company; Mic Stewart, Metropolitan Water District of Southern California; Ed Thomas, National Rural Water Association; Diane VanDe Hei, Association of Metropolitan Water Agencies; and Steve Via, American Water Works Association.

This report was reviewed by a number of individuals chosen for their expertise relevant to this important topic. This peer review was conducted to help assure the highest possible quality report and to engage perspectives beyond those of the authors and the U.S. Environmental Protection Agency. We wish to thank the following for their contributions as reviewers of the report: Gregory B. Baecher, University of Maryland; Kenneth R. Bradbury, Wisconsin Geological and Natural History Survey; Gunther Craun, Gunther Craun & Associates; David Fries, University of South Florida; Jerome B. Gilbert, J. Gilbert Inc.; Richard G. Luthy, Stanford University; Dr. Christine L. Moe, Emory University; David Spath, California Department of Health Services; and Rhodes Trussell, MWH, Inc. We also wish to acknowledge the role of the National Research Council's Water Science and Technology Board, especially that of its Director Stephen D. Parker, for the role played in helping to engage these experts and helping to facilitate the review. The reviewers provided many constructive comments and suggestions that were incorporated in the final report, but were not asked to endorse the report individually or on behalf of the National Research Council. The U.S. Environmental Protection Agency is responsible for the final content of the report.

In addition, EPA would like to thank the following federal agencies and departments for their important contributions: Federal Bureau of Investigation, including the National Infrastructure Protection Center; Centers for Disease Control and Prevention; Central Intelligence Agency; Federal Food and Drug Administration; Lawrence Livermore National Laboratory; Sandia National Laboratory; Office of Homeland Security; US Army Corps of Engineers; US Bureau of Reclamation; US Departments of Defense; Health and Human Services; US Geological Survey; and USDA Rural Utilities Service.

Finally, EPA appreciates the reviews, comments and contributions made by the National Governors Association, the National League of Cities, Jane's Information Group, Malcolm Pirnie, Incorporated, and Michael Baker Jr., Incorporated.

PREFACE

The Environmental Protection Agency (EPA) has developed this *Baseline Threat Information for Vulnerability Assessments of Community Water Systems* to assist water utilities in conducting vulnerability assessments. While this report is not a vulnerability assessment tool, this document does present an overview of threats, methodologies, strategies, and responses for water utilities to consider when conducting these assessments. Additionally, as water utilities vary in their assets and system design, some elements of this document will not apply equally to all water systems.

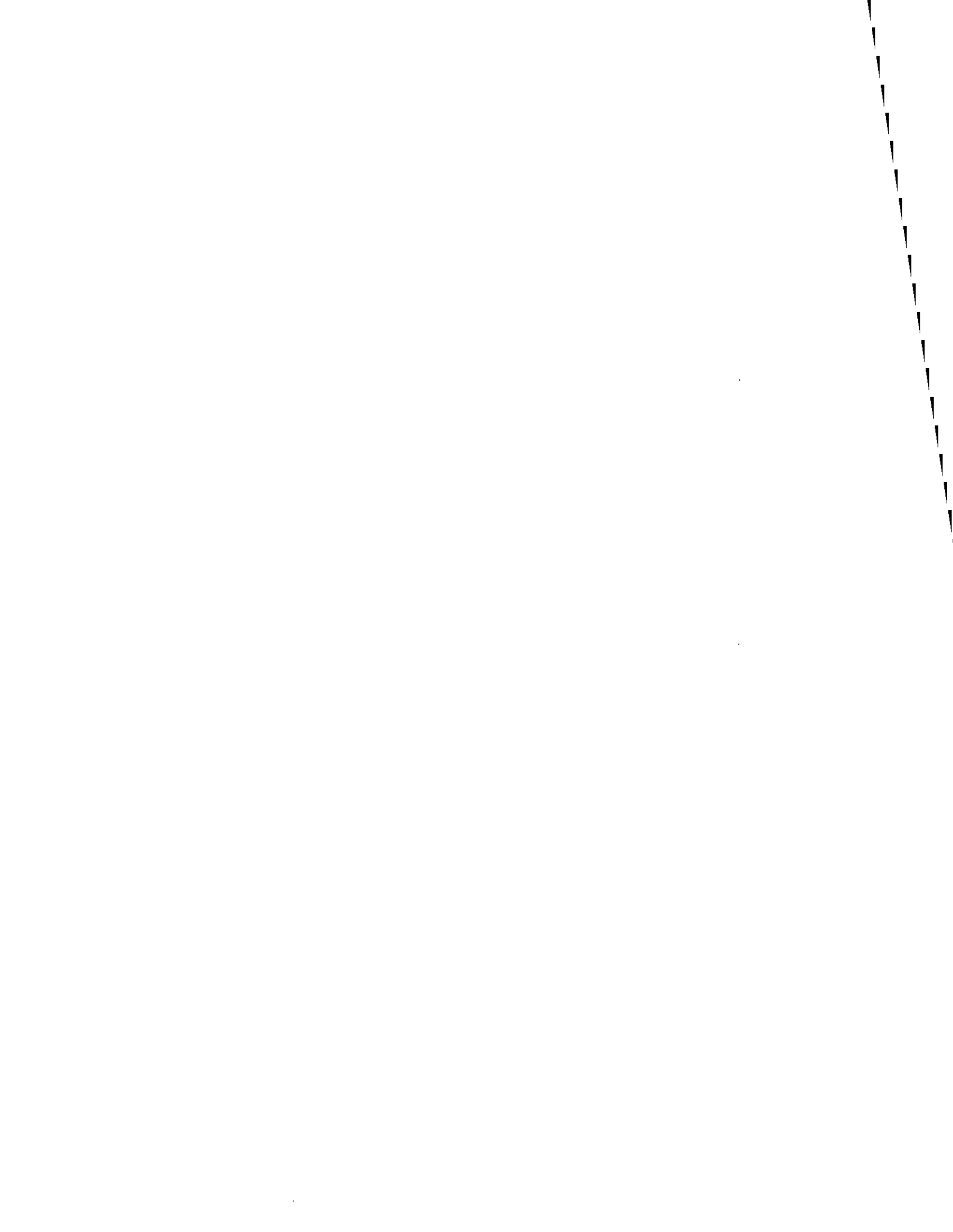
The primary objective of this document is to provide information for utility managers and their staffs to identify and evaluate vulnerabilities that could place the operation of the water utility, staff, and/or customers in harms way. The EPA recognizes that, because water systems vary in design and operations, the level of threat and types of risks also vary from system to system. In addition, technologies to protect systems continue to evolve and levels of threats and risks are dynamic. As these issues alter, utility managers should evaluate the need to periodically update their vulnerability assessments to properly manage these factors.

Vulnerability assessments contain sensitive information that should be protected from inadvertent disclosure. Procedures should be established at the early stages of a vulnerability assessment to control sensitive information developed throughout the assessment process.

It should be noted that this informational document does not cover the integration between a vulnerability assessment and an emergency response plan. However, EPA encourages utilities to incorporate the vulnerability assessment results into their emergency response plan. Also, EPA has developed emergency response notification guidelines for water and wastewater facilities. More information is available on EPA's Web site at <http://www.epa.gov.safewater/security>.

TABLE OF CONTENTS

	<u>PAGE</u>
INTRODUCTION	1
PURPOSE	2
1.0 ASSESSING VULNERABILITIES	
1.1 INTRODUCTION	2
1.2 WHAT ARE THE BASIC ELEMENTS OF VULNERABILITY ASSESSMENTS.....	2
1.3 EXAMPLES OF CURRENTLY AVAILABLE VULNERABILITY ASSESSMENT METHODOLOGIES AND TOOLS	8
2.0 DETERMINING THE LEVELS OF THREAT	
2.1 INTRODUCTION	10
2.2 WHAT KINDS OF POTENTIAL ADVERSARIES SHOULD WATER SYSTEMS CONSIDER WHEN UNDERTAKING VULNERABILITY ASSESSMENTS?	10
2.3 WHAT ARE SOME TYPICAL MOTIVATIONS AND OBJECTIVES OF POTENTIAL ADVERSARIES?	12
2.3.1 WHAT DO TERRORISTS KNOW ABOUT WATER SYSTEMS?	12
2.3.2 WHAT TACTICS ARE TERRORIST LIKELY TO USE TO ATTACK WATER UTILITIES?	14
2.4 HOW CAN UTILITIES OBTAIN MORE SPECIFIC, UP-TO-DATE INFORMATION ON THREATS?	15
2.4.1 OBTAINING LOCAL THREAT INFORMATION	15
2.4.2 NATIONAL RESOURCES FOR OBTAINING THREAT INFORMATION	16
2.4.3 OTHER THREAT-RELATED EFFORTS	18
3.0 MODES OF ATTACK FOR SYSTEMS TO CONSIDER WHEN ASSESSING VULNERABILITIES	
3.1 INTRODUCTION	20
3.2 WHAT KINDS OF ATTACKS MIGHT RESULT IN PHYSICAL DAMAGE?	20
3.2.1 SPECIAL CONSIDERATIONS FOR TOXIC CHEMICALS AND HAZARDOUS MATERIALS.....	21
3.3 ATTACKS THAT COULD RESULT IN CONTAMINATION OF WATER	24
3.4 CYBER ATTACK	30
3.5 ATTACK ON RELATED INFRASTRUCTURE ON WHICH THE WATER SYSTEM IS DEPENDENT	31
3.6 ADDITIONAL CONDSIDERATIONS	32
APPENDICES.....	33
REFERENCES	54



**BASELINE THREAT INFORMATION FOR VULNERABILITY ASSESSMENTS OF
COMMUNITY WATER SYSTEMS**

INTRODUCTION

On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Preparedness and Response Act) into law (PL 107-188). The Bioterrorism Preparedness and Response Act requires every community water system serving a population of greater than 3,300 persons to (1) conduct a vulnerability assessment (VA); (2) certify and submit a copy of the assessment to the Administrator of the US Environmental Protection Agency (EPA) (within a specified schedule); and (3) prepare or revise an emergency response plan (ERP) that incorporates the results of the vulnerability assessment and certify to the EPA Administrator that the system has completed such a plan within 6 months of completing the vulnerability assessment.

scope
←

The time frames for VAs and ERPs are:

Table 1

Systems serving population of:	Certify and submit VA by:	Certify ERP within 6 months of VA but no later than:
100,000 or greater	March 31, 2003	September 30, 2003
50,000 – 99,999	December 31, 2003	June 30, 2004
3,301 – 49,999	June 30, 2004	December 31, 2004

Sec. 1433 (a)(5) of the Safe Drinking Water Act, as amended by the Bioterrorism Preparedness and Response Act, instructs the EPA to develop protocols to protect the disclosure of submitted vulnerability assessments.

Additionally, Sec. 1433 (a)(1) of the Safe Drinking Water Act, as amended by the Bioterrorism Preparedness and Response Act, instructs the EPA to “provide baseline information to community water systems required to conduct vulnerability assessments regarding which kinds of terrorist attacks or other intentional acts are the probable threats to: (A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or (B) otherwise present significant public health concerns.”

Drinking water utilities today find themselves facing new responsibilities. While their mission has always been to deliver a dependable and safe supply of water to their customers, the challenges inherent in achieving that mission have expanded to new sectors of security and counter-terrorism. In PL 107-188, Congress recognizes the need for drinking water systems to undertake a more comprehensive view of water safety and security, and set specific requirements to meet that objective. Utility managers and operators may need assistance to understand how to approach issues traditionally regarded to be the domain of law enforcement, for example, protecting their facilities against vandalism or other ill-intended damage, or safeguarding

sensitive records and plans. It is in this new context that the information contained in this document is provided.

PURPOSE

This document provides the baseline threat information required by PL 107-188 and additional information to drinking water utilities to assist them in their efforts to:

- Undertake risk-based vulnerability assessments of their assets (Section 1);
- Analyze potential adversarial threats (Section 2);
- Consider potential modes of attack (Section 3);

The report also provides references to resources for additional information.

Information on security for water systems is evolving very quickly as the field receives increased attention and as new research and investment in technology yield useful results. EPA is committed to providing the latest information, as it becomes available. New information will be provided through the Water Information Sharing and Analysis Center (Water ISAC). See Section 2 for more information on the Water ISAC.

1.0 ASSESSING VULNERABILITIES

1.1 Introduction

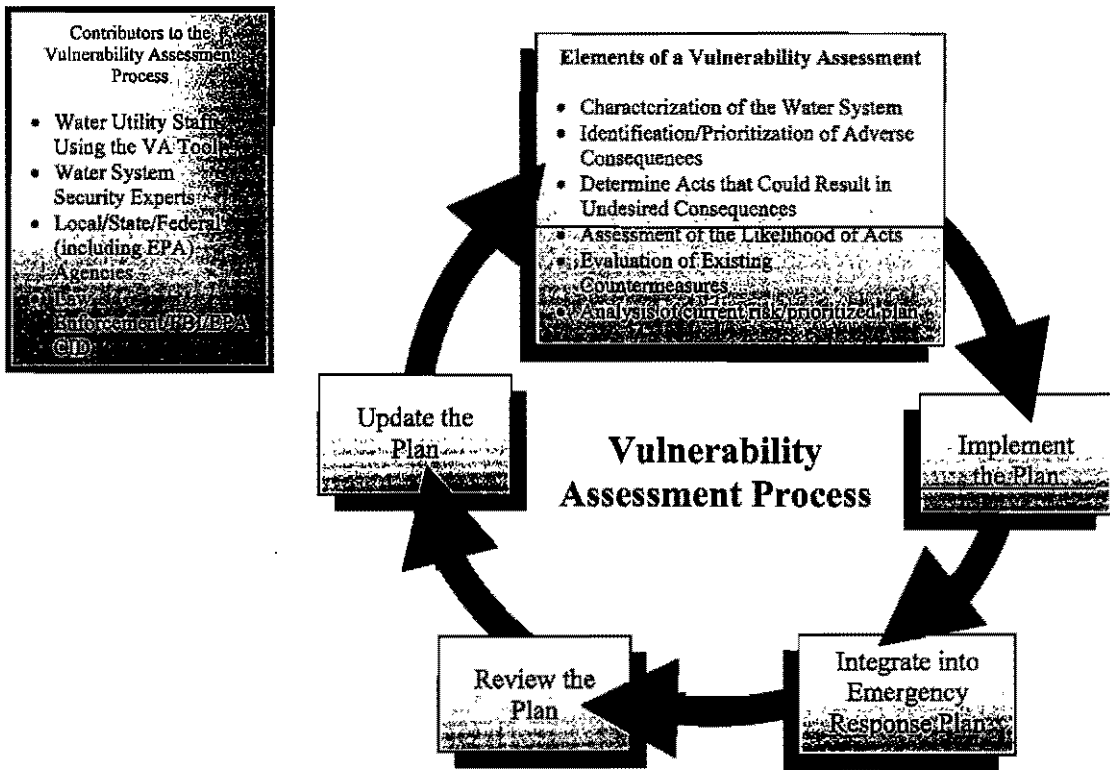
This section describes the basic assets of a vulnerability assessment and provides information on existing vulnerability assessment tools. The steps outlined below are appropriate to any size water system required to conduct a vulnerability assessment pursuant to PL 107-188. The vulnerability assessment process, however, will range in complexity based on the design and operation of the water system itself. These steps are conceptual in nature and not intended to serve as a detailed methodology.

1.2 What are the Basic Elements of Vulnerability Assessments?

Vulnerability assessments help an organization evaluate susceptibility to potential threats and identify corrective actions that can reduce or mitigate the risk of serious consequences from adversarial actions. Such an assessment for a water system takes into account the vulnerability of the water supply (ground and surface), treatment, and distribution systems. It also considers risks posed to the surrounding community related to attacks on the water system. An effective vulnerability assessment serves as a guide to the water utility by providing a prioritized plan for security upgrades, modifications of operational procedures, and/or policy changes to mitigate the risks and vulnerabilities to the utility's critical assets. The vulnerability assessment provides a framework for developing risk reduction options and associated costs. Water systems should review their vulnerability assessments periodically to account for changing threats or additions to the system to ensure that security objectives are being met. Preferably, a vulnerability assessment 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 adversarial actions.

The nature and extent of the vulnerability assessment will differ among systems based on a number of factors, including system size, potential population affected, source water, treatment complexity, system infrastructure and other factors. Security and safety evaluations also vary based on knowledge and types of threats, available security technologies, and applicable local, state and federal regulations. Regardless of these complexities and nuances, the following are common elements of vulnerability assessments:

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;
5. Evaluation of existing countermeasures; and
6. Analysis of current risk and development of a prioritized plan for risk reduction.



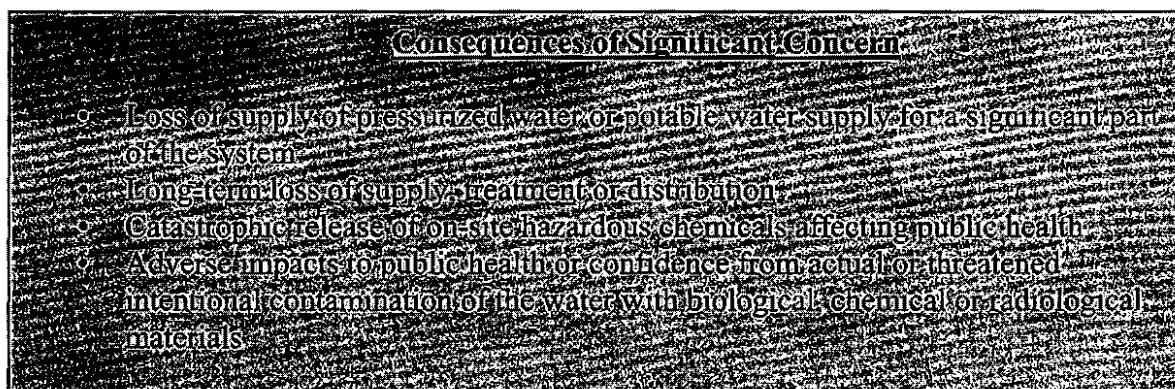
Points to consider related to these six basic elements are included below. The manner in which the vulnerability assessment is performed is determined by each individual water utility. It will be helpful to remember throughout the assessment process that the ultimate goal is twofold: to safeguard public 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 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*, PL 107-188 specifies that the utility should review the potential for physical damage to the water system's infrastructure, including:
 - Pipes and constructed conveyances
 - Physical barriers
 - Water collection, pretreatment and treatment
 - Storage and distribution facilities
 - Electronic, computer or other automated systems that are utilized by the public water system (e.g., Supervisory Control and Data Acquisition (SCADA))
 - The use, storage, or handling of various chemicals
 - The operation and maintenance of such systems

Section 3 provides more information on the methods by which terrorists may attack systems.

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. Section 2 provides more information on threats (potential adversaries and modes of attacks) that water systems should consider during the vulnerability assessment process and mutual assistance arrangements that some utilities have initiated. 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 SCADA and business-related computer information systems such as firewalls, 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.

**Have You Already Improved Security?
Consider Whether These Strategies Apply To You.**

Sound Business Practices

- Adopt *security* as an integral part of overall operations;
- Develop policies and procedures, train and test employees on them;
- Put someone in charge of implementing an effective security program;
- Review and revise emergency response plans—drill, drill, drill;
- Cooperate with adjacent utilities or regional utility networks;

System Upgrades

- Eliminate single-points-of-failure;
- Store back-up equipment off-site in a secure location;
- Develop back-up systems;
- Reduce risks from hazardous chemicals; or
- Optimize treatment;

Security Upgrades

- Employ *detection* devices that characterize the intrusion-- who has entered, how many people, with what equipment?
- Use physical barriers to *delay* intruders (e.g., doors, vaults, walls, locks, and distance or separation between assets).
- Establish contacts and agreements with local law enforcement and emergency response officials to ensure minimal *response* times.

1.3 Examples of Currently Available Vulnerability Assessment Methodologies and Tools

A number of methodologies and tools have been developed or are being refined to aid water utilities in performing vulnerability assessments and understanding risk and risk reduction. Several of these are nationally available and are identified below. Water systems are also encouraged to consult with their state drinking water primacy agency to obtain additional information and to determine whether any specific state requirements apply.

- Sandia National Laboratory, under an Interagency Agreement between EPA and the Department of Energy, has tested and provided training on a methodology known as *Risk Assessment Methodology for Water Utilities* (RAM-W). RAM-W was developed in

cooperation with the American Water Works Association Research Foundation (AwwaRF), EPA, and municipal water utilities. This security risk assessment methodology is very comprehensive and covers most aspects of water utility operations. It was designed for large drinking water utilities. Extensive fault-trees are used throughout the analysis to assist the water utility in systematically assessing the vulnerabilities to malevolent attack. The results provide the water utility with a prioritized list of relative risks to be considered for system and/or security upgrades. Version 2, expected to be available in late September 2002, will include both physical and cyber security assessment tools.

A list of firms selected as trainers on RAM-W and more information is provided at: http://www.epa.gov/safewater/security/sandia_training.pdf.

- VSAT, the *Vulnerability Self-Assessment Tool* was completed July 2002 for wastewater systems, and is under development for drinking water utilities. The current version provides a comprehensive, easy-to-use CD-ROM package for wastewater utility professionals seeking to: 1) assess their utilities' vulnerabilities; 2) determine potential solutions for the prioritized vulnerabilities; and 3) develop priorities for security improvements based on cost and feasibility. The software tool, created with support from EPA, makes this process possible for the full suite of potential utility assets subject to a crisis event, including the physical plant, employees, information technology, communications, and utility customers. The drinking water system version will be available and distributed free of charge to drinking water utilities. Expert assistance will be provided through an on-line help desk. The tool will support vulnerability assessments at all size facilities. More information is available at <http://www.VSATusers.net/>
- *Water System Security: A Field Guide* was developed by the American Water Works Association (AWWA). Managers and operations personnel of small- to medium-sized water utilities will find this guidebook helpful as they assess and upgrade the physical and operational security of their systems. It covers emergency preparedness plans; vulnerability assessments; mitigation measures for critical assets; emergency response and recovery; and crisis communications. More information is available at <http://www.awwa.org/>.
- The *Security Vulnerability Self-Assessment Guide*, a result of collaboration among the Association of State Drinking Water Administrators (ASDWA), the National Rural Water Association (NRWA) with consultation from EPA, is designed for drinking water systems serving fewer than 3,300 people. The guide helps these systems assess critical assets and identify security measures. More information is available at <http://www.asdwa.org/>.
- *The National Drinking Water Clearinghouse* (NDWC) at West Virginia University is a public service organization that collects, develops, and distributes timely drinking water related information. Sponsored through the U.S. Department of Agriculture's Rural Utilities Service (RUS), the EPA, NDWC provides technical assistance to America's small and rural drinking water treatment plants. NDWC intent is to educate governing boards and system personnel, help them prepare emergency plans, and find sources of more information. More information is available at <http://www.nesc.wvu.edu/>.

2.0 DETERMINING THE LEVEL OF THREAT

2.1 Introduction

Due to recent events, potential terrorist actions are of serious concern to water utilities. People with many different motivations, both external (outsiders) and those internal (insiders) to the water utility, might intend to harm a water system or neighboring communities. Even those who are not considered to be highly skilled (e.g., vandals) may create a situation that terrorizes the community. While many kinds of threats are possible, depending on local circumstances and the nature of a specific water system, some may be more likely than others.

Attacks on water systems might be undertaken by a variety of people with different motivations and objectives. Determining who poses a threat is the first step in determining the level of threat. In general, domestic terrorist groups tend to act locally and therefore, it is critical that water utility managers become aware of such groups. Likewise, when undertaking a vulnerability assessment, water systems should consider a full range of potential adversaries and, with assistance from law enforcement agencies and FBI officials, attempt to identify those that might be of particular concern for their facility.

This section provides information on the kinds of adversaries that might attack a water system and what their motivations and objectives might be, as well as actions underway to help water systems learn more about the threat they face and how to improve coordination with law enforcement.

2.2 What Kinds of Potential Adversaries Should Water Systems Consider when Undertaking Vulnerability Assessments?

There are two categories of potential adversaries (outsiders and insiders) that water systems should consider when attempting to determine the threat level for their particular facility.

Outsiders could include:

- Vandals;
- Criminals;
- Disgruntled researchers;
- Computer hackers of various skill levels;
- Domestic terrorists; or
- International terrorists.

Insiders could come from the ranks of:

- Disgruntled employees;
- Contractors with access privileges; or
- Vendors.

Collusion can occur between any of the insider and outsider categories. Insiders and outsiders may employ the same or similar tactics. They might attempt to physically attack assets

(including employees), hack into the cyber systems, or contaminate the water by affecting the treatment processes or injecting a contaminant. The goal may not be to have a long-term effect on the water utility, but to disrupt water supply so they can attempt some other malicious act. The insider, often a disgruntled employee or former employee, may be of special concern because they could have detailed knowledge of a system.

Resources available to the attacker might include personnel, equipment, access to agents, and knowledge of the system, all of which determine the level of sophistication of an attack. The level of support available to the attacker will have a significant impact on the available resources. For example, a disgruntled employee may have intimate knowledge of the system, but would presumably not have access to biological warfare agents. On the other hand, a well funded/supplied terrorist may have the resources and access necessary to develop, purchase, or steal biological warfare agents. Table 2.1 provides examples of the resources that might be available to various adversary categories.

Table 2.1 Examples of Resources Available to Selected Adversarial Categories

Adversary 1	Personnel	Equipment	Access to Contaminants 2	Knowledge
Vandal	1 to 3 untrained individuals	Basic hand tools, firearms	Commercially available chemicals	Minimal
Disgruntled employee or contractor	1 untrained individual (unless working with outsider)	Work crew equipment, pumps, on-site hazardous chemicals	Commercially available chemicals and treatment chemicals	Detailed knowledge of system
Domestic terrorist organization	Team of 1 to 6 individuals	Tools, pumps, firearms, explosives	Bulk quantities of restricted toxic chemicals	Possible insider collusion, public information previously available
Disgruntled researcher	1 skilled individual	Lab equipment, tools and pumps	Biotoxins, toxic chemicals and purified or crude pathogens	Some system-specific information
International terrorist organization	Team of 1 to 6 skilled individuals	Tools, pumps, firearms, explosives	Chemical and biological warfare agents	Possible insider collusion, public information previously available

Note:

1. Any of these groups might pose a cyber threat.

2. The listed contaminants represent the most harmful and/or restricted substance that the adversary would have access to. Any adversary is also presumed to have access to less harmful contaminants.

2.3 What are Some Typical Motivations and Objectives of Potential Adversaries?

Depending on the kind of aggressor, motivations may vary widely. A vandal, for example, might not really intend to harm the drinking water facility. Rather, he or she might have another more general goal in mind (e.g., malicious mischief, minor damage or disruption). Some typical examples of vandalism are destruction of locks and windows to gain unauthorized access and spray painting of graffiti.

Vandalism becomes a serious problem when the operators of a water utility determine that unauthorized entry has occurred, but the objective of the perpetrators is unknown or uncertain. Then, the utility should investigate to determine whether the incident has created a dangerous situation. In some cases, utilities may have to shut down portions of their systems or notify the public not to drink the water until final determinations can be made. In such situations, the vandals have raised significant concerns in the community, not unlike the concerns raised by a terrorist action.

Terrorists, on the other hand, are likely to try to use the water system to achieve broader objectives in response to American political or social policy and/or practices. These might include causing widespread fear and panic by:

- Creating an adverse impact on public health within a population;
- Disrupting system operations and interrupting the supply of safe water;
- Causing physical damage to system infrastructure;
- Reducing public confidence in the water supply; or
- Long term denial of water and economic hardship due to remediation efforts resulting from a successful contamination attack.

Terrorists may be dedicated to studying the utility, gathering background information, using the utility's assets as weapons, and working in multiple groups to attack multiple locations. Some may be willing to kill and be killed, as such; they are our most dangerous adversaries.

Those people with detailed knowledge of a specific facility and its operations may pose some of the most serious threats to a water system. Motivations of such people may include revenge or the venting of anger manifested because of a real or imagined problem; financial gain (bribery or other criminal activity); or sympathy for the motivation or objectives of outsiders. In addition, it is not inconceivable that an insider could be "planted" by a terrorist organization for the specific purpose of becoming an insider to collude with outsiders.

2.3.1 What do Terrorists Know about Water Systems?

It is safe to assume that terrorist groups know information about a water utility that was readily available through the Internet, periodicals, utility flyers, design drawings, plans distributed during a bidding process, and calls to facilities, whether or not the information has been secured since September 11, 2001. This information might include: plant capacity, methods of treatment (including disinfection), source water intake, conveyance and distribution system location, and

chemical analytical capabilities. Terrorists might also have detailed knowledge through collusion with disgruntled insiders.

Table 2.2 summarizes a terrorist's approach to target selection, what terrorists like and do not like to see during reconnaissance activities and questions that they may be asking themselves as they review potential targets.

Table 2.2 The Terrorist Approach

The Terrorist Approach
Examine maps and facility diagrams
Drive around the general area keeping away from the target to get a feel for the locale
Drive past the target with the passenger giving a running commentary
Drive past the target once again – this time take a more detailed look to answer questions such as:
<ul style="list-style-type: none"> ▪ How close can we get without arousing suspicion? ▪ Can we get in here at night? ▪ Can we drive straight in/up to the target during the mission? ▪ Is this target easy to exploit? ▪ An exit/escape plan may be necessary – how possible is this?
Be careful about making incriminating notes
Have a credible cover story prepared in case you are checked by law enforcement
Put a US flag (decal) on the fender
Think out of the box – remember that a successful attack is almost an “art form”

What Terrorist Reconnaissance Units Do Not Like
Activity in the area, such as inquisitive people, barking dogs in backyards
Well trained /equipped security guards
Closed circuit TV cameras
Perimeter lights; buildings with lights on at night
Random, local police patrols
Interior perimeter patrols; cleared area around the perimeter fence
Inquisitive librarians who take a great interest in the fact that you are researching water supplies

What Terrorist Reconnaissance Units Like to See
Open, unguarded gates
Broken or damaged fencing
No sign of security guard or local law enforcement patrols
No perimeter lights
Keypads where the gate entry number can be seen at a distance through binoculars
A good view of the potential target during a drive past
Lots of good background target information on the internet
Detailed notice boards that tells exactly what is in a facility
Trees, bushes, and foliage tight up against the perimeter fence

2.3.2 What Tactics are Terrorists Likely to Use to Attack Water Utilities?

Statistics indicate that the vast majority of terrorist attacks worldwide continue to be perpetrated with conventional weapons such as explosives. From existing data, it appears that the likelihood of a water utility being bombed is greatest, followed in likelihood by chemical, biological, cyber, and nuclear/radiological attacks.

There is, however, a disturbing trend towards heightened interest in chemical and biological warfare agents. These high profile, high-impact warfare agents are often referred to as Weapons of Mass Destruction (WMD). WMD cases primarily dealing with the threatened use or procurement of chemical, biological, or radiological materials with intent to harm, have shown a steady increase since 1995. Most of these cases have involved hoaxes rather than actual use of a WMD.

Work is ongoing to create a centralized and informative list of security events that have already taken place at drinking water utilities under an AwwaRF-sponsored project. It is expected that this information will be available to the Water Information Sharing and Analysis Center (discussed in Section 2.4.2) for threat analysis purposes.

Currently over 150 security events have been identified, but experts believe that this represents only a fraction of the total of all security events that have taken place at water utilities in the recent past. In any case, this list of events is very informative. The majority of these events are trivial, trespass or common vandalism cases, or may not even have been a "security" event at all. However, there are also a number of security events that have been identified of a very serious nature, and these events cover the full range of possible attacks on a water utility. There are already examples of threatened intentional contamination of drinking water, including examples where the perpetrators were accumulating the means to follow through on this threat and even succeeded in contaminating the water, physical disruption of the drinking water supply, the use of explosives against utility structures, cyber attacks on a utility including remote operation of SCADA-controlled facilities, and threats/attacks on drinking water utility personnel. A number of the more serious events involved or are suspected to have involved disgruntled utility personnel, a number of the events involved criminals, and some of the events involved people and groups that can clearly be defined as "terrorists."

The kind of adversaries and tactics to consider during a vulnerability assessment is a decision to be made by the utility. Given that utilities will want to avoid the *consequences of significant concern* (described in Section 1.2) and the fact that the majority of terrorist attacks to date have employed conventional weapons, systems may want to focus on protecting single points of failure and improving security for toxic chemical and hazardous materials storage facilities. To address contamination threats, utilities should also consider enhancing water quality monitoring to aid in assessing the presence of possible contaminants in source and/or treated water and the potential benefit(s) of adding real-time analytical capabilities for chemical, biological and/or radiological contaminants. (See Section 3 for more information on the contamination threat).

2.4 How Can Utilities Obtain More Specific, Up-to-date Information on Threats?

Obtaining information on threats is critical for a utility performing a vulnerability assessment. Utilities should communicate with local, state, and federal agencies who may advise them on local and general threat considerations. Obtaining general information on threats may also be useful to systems in assessing threats to be considered as a part of the vulnerability assessment. The following information is provided to assist systems in the threat determination process.

2.4.1 Obtaining Local Threat Information

Local Law Enforcement

Local law enforcement agencies are a valuable resource for obtaining local threat information. Local agencies, such as municipal, county and/or state police, can provide information relevant to local criminal activity trends and arrest data; such as the number of crimes reported to police, crime rates and arrests by age group, number, and types of offenses (violent, property, etc.).

Federal Bureau of Investigation (FBI)

The FBI is the lead federal agency for investigating terrorist acts that include the intentional release of a weapon of mass destruction (WMD), defined as high-impact warfare agents (chemical, biological, radiological, nuclear or high explosive devices). The FBI aggressively investigates any threat or incident believed to be an act of terrorism. Consequently, the FBI ~~and~~ can be an important source of information on threats. The FBI has designated a WMD Coordinator in each of the 56 field offices. The primary responsibilities of the coordinators are to establish liaison with the federal, state and local response communities, and other incident-specific responders, such as water utilities. In the case of an incident, WMD Coordinators also serve as the FBI representative for operational support, ensuring that a criminal investigation is properly performed and prosecuted. Most FBI offices also have a Critical Infrastructure Protection (CIP) Coordinator that is responsible for communicating with municipalities and private industry on infrastructure protection matters.

Utilities should establish close relationships with their local FBI WMD and CIP coordinators. These people are important resources for up-to-date and system-specific information on threats to be considered during a vulnerability assessment. Your local FBI office can be located by visiting <http://www.fbi.gov/contact/fo/info.htm>.

EPA Criminal Investigation Division (EPA CID)

As the subject matter expert in the investigation of criminal acts involving or impacting drinking water, wastewater treatment, hazardous materials, toxic substances, or other environmental media, EPA CID works closely in support of the FBI Weapons of Mass Destruction Operations Unit and other response elements within the federal law enforcement community. During a response to a suspected act of terrorism, particularly those involving drinking water and

wastewater critical infrastructure, EPA CID would respond accordingly in support of the FBI. EPA CID can also provide support for assessments of the potential threats for drinking water facilities.

EPA CID currently has approximately 200 Special Agents located across the country in 15 area offices and 29 resident offices. One of the responsibilities of the Special Agents is to establish liaison with the federal, state and local response communities, as well as the quasi-governmental communities that provide critical services, which EPA regulates. Certain designated Special Agents also serve as a liaison to the FBI sponsored Joint Terrorism Task Forces, U.S. Attorney's Offices Anti-Terrorism Task Forces, and EPA sponsored Environmental Crimes Task Forces. Through these organizations and others where EPA CID plays a key participatory role, EPA CID can provide assistance to drinking water utilities during vulnerability assessment process. For more information regarding the Criminal Enforcement Program's support to homeland security, visit <http://www.epa.gov/compliance/criminal/homelandsecurity/index.html>

Local Emergency Planning Committee (LEPC)

Another source of local threat information, as well as information on emergency response planning, may be your Local Emergency Planning Committee (LEPC). The Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) called for the establishment of local emergency planning committees (LEPCs). LEPCs have broad-based membership with responsibility to develop comprehensive emergency plans for their communities. There are now more than 3,500 LEPCs, and they reflect the diversity of our country. Most LEPCs are organized to serve a county; some are for a single large city; others cover the better part of an entire state. You can find the LEPC for your location at <http://www.epa.gov/ceppo/lepclist.htm>.

2.4.2 National Resources for Obtaining Threat Information

The Water Information Sharing and Analysis Center (ISAC)

The Water Information Sharing and Analysis Center, or Water ISAC, will play a critical role in communicating security information to water and wastewater utilities. The Association of Metropolitan Water Agencies (AMWA) is developing the Water ISAC with funding assistance from EPA. The mission of the Water ISAC is to provide water and wastewater utilities a secure forum for gathering, analyzing, and sharing security-related information. The ISAC will provide utilities timely, useable information that will support their efforts to protect our nation's critical water infrastructure.

The Water ISAC will provide the following:

- Alerts of potential and actual physical or cyber attacks;
- Access to information from the FBI, EPA, CDC, intelligence agencies and other federal agencies;
- Information on chemical, biological and radiological agents;
- Information on physical vulnerabilities and security solutions;
- Notification of cyber vulnerabilities and technical fixes;

- Research, reports and other information;
- A secure mechanism to report security incidents;
- Access to vulnerability assessment tools and resources;
- Emergency preparedness and response resources;
- An electronic bulletin board and other forums on security topics;
- Summary of open-source security information; and
- Information on security products and services.

Although this document was made available through the Water ISAC, it is expected that regular operation will begin in December 2002.

National Infrastructure Protection Center

The National Infrastructure Protection Center (NIPC), located in the FBI's headquarters building in Washington, DC, brings together representatives from the FBI, other US government agencies, state and local governments, and the private sector into a partnership to protect US critical infrastructures. Established in February 1998, the NIPC's mission is to serve as the US government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures include telecommunications, energy, banking and finance, water systems, government operations, and emergency services. More information about the NIPC is available at <http://www.nipc.gov/about/about.htm>

InfraGard

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of the United States' critical infrastructures. All InfraGard participants are committed to the proposition that a robust exchange of information about threats to, and actual attacks on, these critical infrastructures is an important element for successful infrastructure protection efforts. The goal of InfraGard is to enable that information flow so that the owners and operators of infrastructure assets can better protect themselves, and so that the U.S. government can better discharge its law enforcement and national security responsibilities. InfraGard is organized into 56 sections each associated with a field office of the FBI. More information is available at <http://www.fbi.gov/contact/fo/info.htm>

The Water Critical Infrastructure Protection Advisory Group

Under Presidential Decision Directive 63 issued in 1998, federal agencies are required to work with private sector counterparts to protect the nation's critical infrastructure from terrorist attacks. EPA was given the lead for the water sector and EPA appointed Association of Metropolitan Water Agencies as the private sector lead. In January 2000, AMWA formed the Critical Infrastructure Protection Advisory Group (CIPAG), comprised of representatives from water utilities and related organizations, to advise them in this role. The CIPAG provides an

important forum for discussing all aspects of water sector critical infrastructure protection. More information is available at <http://www.amwa.net/isac/watercipag.html>

U.S. Environmental Protection Agency (USEPA)

The USEPA's Office of Water hosts a Water Security Web site located at <http://www.epa.gov/safewater/security/>. It contains information on:

- Financial assistance, including Federal Grants for Large Drinking Water Utilities;
- Training opportunities including workshops and Web-cast seminars;
- Tools to aid in development of vulnerability assessments and emergency operation plans;
- Information sharing through the Information Sharing and Analysis Center under development;
- Research and technology initiatives; and
- Links to other sources of information.

For more information about other EPA efforts on terrorism preparedness and response, go to www.epa.gov/swercepp/cntr-ter.html.

Centers for Disease Control and Prevention (CDC)

The Centers for Disease Control and Prevention hosts a Web site on Public Health Emergency Preparedness and Response, located at <http://www.bt.cdc.gov>. The site provides information on biological and chemical agents, radiological emergencies, whom to contact in the event of bioterrorism emergency. It includes fact sheets, CDC health alerts, advisories, and updates. Site topics include preparation and planning, emergency response, and training.

2.4.3 Other Threat-Related Efforts

Interagency Efforts to Better Understand the Contamination Threat

In the fall of 2001, several federal agencies with expertise in drinking water protection and weapons of mass destruction undertook an assessment of the state of knowledge on contaminants that could be used to threaten drinking water supplies. The analysis focused on the characteristics of agents, detection technologies, analytical methods, laboratory capacity, and treatment effectiveness.

Besides forming the basis for the information concerning the contamination threat contained within this document, this analysis supports several ongoing initiatives to improve information on drinking water protection from intentional contamination. Products under development include:

- A database on contaminant characteristics to be accessible to emergency responders on a 24-hours per day/7 days a week basis;
- Monitoring guidance;

- Compendium of analytical methods and laboratory capabilities; and
- Research to fill information gaps;

As these products are completed, additional information will be provided to drinking water utilities through the Water ISAC and other appropriate means.

Office of Homeland Security (OHS) Advisory System

As part of a series of initiatives to improve coordination and communication among all levels of government and the American public in the fight against terrorism, President Bush signed directive creating the Homeland Security Advisory System (HSAS). The advisory system provides the foundation for building a comprehensive and effective communications structure for the dissemination of information regarding the threat and risk of terrorist attacks to all levels of government and the American people. For more information on how a consortium of utilities have adapted this system for water utilities, see Appendix A of this document.

State Support

Both State drinking water agencies and emergency response officials may have significant expertise and resources to assist utilities in vulnerability assessment, security improvements and emergency preparedness. Utilities are encourage to consult with appropriate State officials.

Utility Partnership – Mutual Aid

Some utilities have formed partnerships to assist each other with emergency response and other security issues. These may be especially beneficial for information sharing, working with the intelligence community and providing support during emergencies. As an example, information on an existing partnership can be found at <http://www.calwarn.org>.

3.0 MODES OF ATTACK TO CONSIDER WHEN ASSESSING VULNERABILITIES

3.1 Introduction

Just as drinking water systems vary in design, the kinds of attacks that could result in significant loss or consequences also vary. Water systems should consider the entirety of the system when assessing vulnerabilities. In general, there are four categories or modes of attack to consider when undertaking a vulnerability assessment of a drinking water system. These are:

- Physical damage or destruction of critical assets, including intentional release of toxic Chemicals;
- Actual or threatened contamination of the water supply;
- Cyber attack on information management systems (e.g., SCADA) or other electronic systems; and
- Interruption of services from another infrastructure.

When determining the types of attacks that are most problematic to the particular facility it is important to keep in mind both the *Consequences of Significant Concern* (discussed in Section 1) and the particular characteristics of the system being assessed. It may be that some of the consequences are not possible, or are highly unlikely, due to the design of the system. For example, there may not be significant quantities of toxic chemicals on-site. Also, it may be determined that the countermeasures already in place at the utility will reduce risks sufficiently to eliminate a consequence of significant concern.

The remainder of this section provides general information on the four primary types of attack to consider.

Potential Consequences of Significant Concern That Could Result from an Attack on Critical Physical Assets

- Loss of supply of pressurized water or potable water supply for a significant part of the system
- Long-term loss of production
- Catastrophic release of on-site toxic chemicals affecting public health

3.2 What Kinds of Attacks Might Result in Physical Damage?

Physical attacks on source water(s), water treatment plants and distribution systems could take various forms. Damage to critical impoundments and conveyances, treatment plant processes, or pumping facilities could interfere with the utility's capability to produce safe, pressurized water for consumption firefighting and other uses. A physical attack targeting toxic chemicals or hazardous materials stored on-site could cause a release of toxic fumes into the environment, a fire, or an explosion.

Any water system asset could conceivably be a target for physical damage or destruction, however, not all parts of a system's infrastructure are equally vulnerable or crucial to the mission of the system. During a vulnerability assessment, each *critical asset* should be identified and described, and potential points of vulnerability identified.

In particular, water systems may want to examine the vulnerabilities associated with physical damage to intakes, pumps, storage tanks, impoundments (including associated valves and gates), non-redundant transmission lines, electrical supply, and treatment facilities (especially the storage of toxic chemicals and other hazardous materials used in treatment processes). Some key points to consider are:

- The design of the system's physical assets, especially considering whether there is sufficient redundancy or if there are any single points of failure;
- The accessibility of critical assets, the loss of which could cause system failure; and
- The availability of areas where explosives or other destructive means could be used in order to successfully disrupt the water system operations or create unsafe conditions (e.g., cause a release of toxic chemicals).

The mode of attack will likely vary depending on the utility and the location within the system an adversary would attempt to attack. If the adversary's objective is to affect the largest population possible, then they are likely to attack the system in a manner that will take the entire utility off-line. *For this reason, understanding single points of failure in the system is crucial to creating safe water and a more secure utility.*

Have You Already Improved Security?

Consider Whether These Strategies Apply To You.

- Redundancy for raw water intakes, transmission lines, and storage (consider the benefits of agreements and interconnections with a nearby water system e.g., mutual aid, purchase agreements, etc.);
- Back up power, spare parts for pumps and other equipment, and shared equipment;
- Limited access to critical assets (e.g., burying transmission lines, rerouting traffic, detection and delay systems).

3.2.1 Special Considerations for Toxic Chemicals and Hazardous Materials

Water utilities use a wide range of toxic chemicals and hazardous materials that may be stored on-site in large quantities. Reviewing the use, transfer, and storage of all toxic chemicals and hazardous materials is a necessary part of the vulnerability assessment. Serious consequences could result from an attack. Of particular concern is how an adversary might use the chemicals to release toxic fumes, contaminate the water or damage or destroy critical assets.

From a public health perspective, disinfectants are some of the most important chemicals used by drinking water utilities. They serve as one of the key barriers in the multi-barrier approach for

No
chemicals
stored
on
sites

drinking water treatment. On a day-to-day basis, chemical disinfectants inactivate disease-causing microorganisms. They may also provide some protection from intentional contamination. While a number of disinfectants such as chlorine (gaseous and hypochlorite), chloramines (chlorine and ammonia), chlorine dioxide, ozone and ultra violet light can be used in the treatment plant, generally either chlorine (gaseous or hypochlorite) or chloramines (chlorine and ammonia) disinfection is used to provide a residual for the distribution system.

From a security perspective, a disadvantage of using some toxic Chemicals is the danger associated with intentional release of toxic fumes. For example, the potential impacts to public health from toxic releases of gaseous chlorine or anhydrous ammonia are of concern. *If the utility stores chemicals such as gaseous chlorine and anhydrous ammonia on-site, then these chemicals are critical assets and should be evaluated as such.* A catastrophic release of chlorine gas can result in a significant risk to facility personnel and the surrounding population, and may result in the disruption of water treatment. Therefore, it is in the best interest of the drinking water utility to reduce hazards associated with the use, transfer and storage of toxic Chemicals, especially gaseous chlorine and anhydrous ammonia. A summary of characteristics, advantages, and limitations of these disinfectants is presented in Appendix D to help utilities evaluate the risk associated with the disinfection process during the vulnerability assessments.

Gaseous chlorine and anhydrous ammonia are not the only chemicals of concern. Hazards associated with other on-site chemicals should also be evaluated during the vulnerability assessment and protective measures should be identified. The following is a list of some additional chemicals that are generally used in a treatment plant. These chemicals are considered hazardous substances and should be treated as such. This list is not inclusive, but is provided to alert utilities to the need for risk reduction pertaining to the use of chemicals.

- Oxygen (used as a liquid (LOX) in the production of ozone);
- Silicofluoric acid (Hydrofluosilicic acid, Hexafluosilicic acid);
- Sulfuric acid;
- Sodium hydroxide;
- Ferric chloride; and
- Hydrogen peroxide.

X

Suggestions for Reviewing Vulnerabilities Related to the Use, Transfer and Storage of Toxic Chemicals or Hazardous Materials

- Define highly toxic and/or reactive chemicals as critical assets. For example, define gaseous chlorine and anhydrous ammonia as critical assets.
- Evaluate the severity of the consequences of an intentional release of chemicals considering the public health and safety, environmental, and economic impacts if this critical asset is attacked.
- If you are a facility that is required to develop a Risk Management Plan (RMP) under Clean Air Act Section 112r, then you are already doing calculations to determine the risk of releases. (For example, you are required to do a RMP if you store more than 2500 pounds of gaseous chlorine or 10,000 pounds of anhydrous ammonia). Review the plan to more fully understand the consequences of an intentional chemical release. If you are not required to do a RMP, consider going through a similar analysis for yourself. (See Appendix C for more information on RMP and refer to the Web Site at: www.epa.gov/ceppo)
- Consider performing a calculation using appropriate models such as ALOHA to determine the extent of the contamination if a catastrophic failure in chemical storage were to occur (e.g., evaluate the consequence of release of the average total amount of gaseous chlorine and/or anhydrous ammonia stored on-site). Available at: <http://www.epa.gov/ceppo/cameo/aloha.html> or <http://response.restoration.noaa.gov/cameo/aloha.html>
- If your analysis shows risks to public health, evaluate countermeasures that could reduce these risks. For example, evaluate the use of alternative chemicals and technologies (see Appendix D for a summary pertaining to the use of alternative disinfectants to support the vulnerability assessment). Work towards a goal of minimizing the use of hazardous chemicals when possible, *without compromising public health protection*.
- When evaluating options consider the following: the health risks associated with each option, the security concerns with storage and transport, operational constraints (including on-site storage space), and the cost associated with each option. Also evaluate the multiple benefits of improving day-to-day water quality associated with the use of several of the alternatives (e.g., ozone and ultra violet radiation).
- Determine whether and where security measures should be increased. Consider increasing physical protection of chemical use, transfer, and storage areas to improve the utility's ability to detect, delay and respond in a timely fashion should an attack on these assets take place.

3.3 Attacks That Could Result In Contamination of Water

In the context of the contamination threat to drinking water systems, a “harmful contaminant” is defined as any substance that can achieve terrorist objectives when introduced into water.

***Potential Consequences
Associated with Intentional
Contamination of a Drinking
Water System***

- Creating an adverse impact on public health within a population
- Disrupting system operations and interrupting the supply of safe water
- Causing physical damage to system infrastructure
- Reducing public confidence in the water supply
- Long term denial of water and economic hardship due to remediation efforts resulting from a successful contamination attack (e.g., long-term contamination of water supply)

Concerns regarding attacks using biological, chemical, or radiological contaminants typically focus on death and disease in a population; however, it is important to consider that other potential consequences of significant concern could be achieved through intentional contamination of drinking water (See side bar). The consequences of an attack on public health could be severe, however, as described in section 1.2, the likelihood and potential for success of such an attack should be weighed in assessing the overall risk.

In order to evaluate the contamination threat to any section of a drinking water system, it is necessary to identify those characteristics of a substance that would allow it to be used in an attack on a water system and produce an adverse consequence. These attributes will vary depending on the objective of the attack. For example, it is not necessary to use a contaminant that is highly toxic or infectious if the objective of the attack is to interrupt the supply of drinking water of acceptable quality or reduce public confidence in the water supply.

For example, it is not necessary to use a contaminant that is highly toxic or infectious if the objective of the attack is to reduce public confidence in the water supply. However, the following general characteristics are applicable to all harmful contaminants regardless of the objective of the attack:

- Ability of the contaminant to produce an adverse consequence;
- Availability and accessibility of the contaminant to the adversary;
- Environmental stability of the contaminant;
- Susceptibility of the contaminant to common treatment and disinfection practices;
- Physical characteristics of the agent (e.g., solubility) that impact the ease with which the substance can be introduced and dispersed into water; and
- Difficulty in detecting the contaminant once introduced into water.

These criteria were used to develop a large list of contaminants that could potentially achieve one or more of the adverse consequences described above. Focusing on the subset of

contaminants that could potentially cause death and/or disease in a population, approximately 100 contaminants were identified that could be of concern from a public health perspective. Of these 100 substances, intelligence information indicates that terrorist organizations have shown interest in roughly a dozen, which they have the potential means to acquire.

A general discussion of the biological, chemical, and radiological contaminants posing a plausible risk to public health is presented in the following subsections to provide some insight to the contamination threat. Given the uncertainties associated with toxicity and infectivity data as well as the other characteristics listed above, it is impossible to come up with a definitive, comprehensive list of contaminants that pose a threat to public health via drinking water. Furthermore, the potential for various agents to cause harm in a particular system will depend on a number of site-specific factors and assumptions about the location and method of contamination. Thus, it is recommended that utilities consider the contamination threat in the context of their own facility characteristics and site-specific vulnerabilities. An approach for incorporating the contamination threat into a utility's site-specific vulnerability assessment is presented in Appendix E. This approach uses model contaminants that are intended to represent a typical contaminant in each major class. In addition to supporting a utility's vulnerability assessment, the approach in Appendix E can be used as a planning and response tool to help characterize the impact of a particular contamination scenario.

Biological Contaminants

Thirty-five biological contaminants were identified as potential threats to water, including bacteria, parasites, viruses, and biotoxins. Biological contaminants considered include those that are known or suspected to have been weaponized as well as pathogens that have been previously implicated in waterborne disease outbreaks. The biological warfare agents are highly infective or toxic, and while most have been weaponized for an aerosol attack, some do pose a plausible threat to public health through ingestion of contaminated drinking water. The virulence and health effects associated with many naturally occurring waterborne pathogens are typically less severe than those associated with biological warfare agents, but these organisms have a demonstrated ability to cause illness, and in some cases death, if present in finished water.

There is a wide range in susceptibility of biological contaminants to disinfection, and in general, viruses and vegetative bacteria are much more susceptible to inactivation by chlorine than spore forming bacteria and parasites. Of the thirty-five biological contaminants considered to be possible threats to drinking water, one-third are known to be susceptible to typical chlorine levels used in distribution systems, one-third are known to be resistant to typical chlorine levels, and disinfection information is unavailable for the final third. Much less information is available regarding the susceptibility of many of these biological contaminants to disinfectants other than chlorine. For those contaminants that have been evaluated during inactivation studies using disinfectants other than chlorine, stronger disinfectants, such as ozone, chlorine dioxide, and UV, have typically been shown to be more effective than chlorine, while chloramines have generally been found to be less effective.

Many of the biological contaminants identified as posing a potential threat to water are highly infectious or toxic in purified form, but purification and concentration of these materials can be

complex. While access to purified pathogens and biotoxins might be limited to terrorists with extensive resources and capabilities, some pathogens and biotoxins can be produced using simple equipment or can be harvested from natural sources. The high potency of these biological contaminants makes them a possible threat to water even in crude form.

Chemical Contaminants

An assessment of chemical contaminants posing a threat to water is a significant challenge simply due to the vast number of manufactured chemicals. The problem is further complicated by the wide availability of some of these chemicals, and their accepted use in bulk quantity. If one considers chemicals capable of achieving any terror objective, including undermining consumer confidence, there are hundreds if not thousands of chemicals of concern. Many would impart an objectionable taste or odor to the water making it undrinkable, several may be capable of causing damage to infrastructure, and some could produce death and disease in a population. Focusing on the latter category, and using toxicity as a primary selection criterion, 65 chemical contaminants were identified as posing a plausible threat to public health. The LD₅₀ (Lethal Dose to 50 percent of the population exposed) is used as a quantitative indicator of toxicity and is defined as the chemical dose resulting in death of half the exposed population expressed in milligrams of chemical per kilogram of body weight. While all 65 chemicals were considered to be toxic enough to pose a threat, LD₅₀ values of these chemicals span four orders of magnitude, from 0.01 to 125 mg/kg. In addition to toxicity, other characteristics, such as solubility in water, availability, taste and odor thresholds, and stability in the presence of a disinfectant residual should be considered.

Much attention has been focused on classical chemical warfare agents since they are highly toxic substances; however, they may not pose a significant threat to water for a number of reasons. First, almost all chemical warfare agents were developed for aerosol deployment and exhibit the most severe and widespread health effects through inhalation, dermal, and ocular exposure. While some of these materials may also be capable of causing death or other severe health impacts via ingestion, the lethal dose is typically much higher via this route compared to inhalation exposure. Another consideration is the low stability of many chemical warfare agents in water, and several are completely destroyed upon contact with water. Furthermore, synthesis of many of these chemicals is technically complex, and the agents themselves, as well as their precursor materials, are tightly controlled. Given all these considerations, it seems unlikely that a terrorist would use a chemical warfare agent in such an inefficient manner as dumping it into water.

It is more likely that toxic industrial chemicals would be used in the intentional contamination of a drinking water system. These might include substances such as pesticides, herbicides, cyanide compounds, and pharmaceuticals. While most of these toxic industrial chemicals have LD₅₀ values greater than 1 mg/kg, they are much more widely available than the chemical warfare agents, and thus are considered to pose a greater threat.

Radiological Contaminants

A few radiological contaminants do pose a potential acute health risk to the public via contaminated water. The amount of radioactive material present in some large devices, such as food irradiators and medical treatment equipment, is enough to contaminate a significant volume of water at lethal levels. While there is a potential acute risk associated with radiological contamination of water, the threat of such contamination is deemed to be relatively low. This is due to a variety of factors including the high amount of radioactivity required to produce a fatal response, the relatively small quantities of material available in most applications, the controlled nature of the material, and logistical difficulties in handling and dispersing the material in water. Furthermore, the radiological devices that contain enough material to be of concern are very large pieces of equipment in which the radioactive material has been encased to prevent any leakage. It would be difficult to obtain and move the equipment, remove the radioactive source from the equipment, and covertly transport it without immediately killing the perpetrators.

While the threat of radiological contamination is assumed to be relatively low, chronic health effects associated with sublethal levels of contamination, such as cancer and birth defects, cannot be ignored. Any event involving the introduction of radionuclides into water will likely raise serious initial reactions and concerns in the public, which may not necessarily be commensurate with the actual risk. In any case, it would likely be necessary to remediate water and infrastructure contaminated with radioactive material. Such a decontamination effort would likely be an expensive and lengthy process, and may leave a community without a convenient source of water for some time. In some cases, the contaminated portion of the system may need to be abandoned or replaced.

Summary of Contamination Threat

The discussion on contamination threat is intended to characterize the threat, especially those contaminants posing a potential risk to public health. A general assessment of this threat indicates that it is *possible* to achieve one or more terror objectives through intentional contamination of drinking water systems.

- Only a few contaminants have the potential to produce widespread death or illness in a population, such as purified biological warfare agents (including some biotoxins) and a few highly toxic chemicals that may remain stable in water long enough to produce the desired effect.
- A larger group of contaminants could produce localized death or illness in a segment of a population, including several dozen toxic chemicals and a few radionuclides.
- There are hundreds to thousands of contaminants that could potentially disrupt service or undermine consumer confidence, but which would not result in death or illness in a population.

While it is important to consider the possibilities associated with an intentional contamination event, a threat assessment is typically based on the *probability* of such an attack. There are historical accounts of intentional contamination of drinking water supplies with biological or chemical contaminants, but most have been associated with wartime activities. The few

documented accounts of intentional contamination of public water systems in the U.S. have not resulted in any reported fatalities. Based on these accounts, it would appear that the probability of a successful contamination attack on a drinking water system is relatively low. However, there has been a reported increase in the interest of various terrorist groups in weapons of mass destruction, including biological and chemical contaminants. Furthermore, some intelligence information indicates that terrorist organizations have considered water infrastructure as a possible target, thus the potential for such an attack does exist.

While the probability of an actual contamination event is considered low relative to other modes of attack, the probability of the *threat* of contamination is relatively high compared to other forms of attack. Many of the apparent security breaches at drinking water utilities that have occurred since 9/11 have involved the threat of contamination. Although a few threats have been verbal, most have been circumstantial, such as a low-flying airplane over a reservoir or a lock cut from the hatch of a distribution system storage tank. Given the possibility of the contamination threat, many utilities chose to treat these security breaches as credible threats, and in some cases isolated the suspected area from the rest of the system until water quality analyses confirmed the safety of the water.

Have You Already Improved Security?

Consider Whether These Strategies Apply To You.

- Treatment systems with both physical and chemical barriers have been shown to be highly effective for removal and inactivation of many microorganisms.

Optimization of treatment and disinfection barriers, through steps such as reducing filtered water turbidity and improving hydraulic efficiencies in disinfectant contact chambers, can increase the level of protection against source water contamination. Additional information on treatment process can be found in Appendix D.

- Maintaining a disinfectant residual at all times and locations throughout a distribution system maximizes protection. At least one third of the biological contaminants identified as plausible threats are susceptible to typical chlorine levels used in distribution systems.

Residual monitoring is an effective tool for verifying disinfectant levels at critical locations within a distribution system. Monitoring can be improved by increasing the number of sampling points and taking samples more frequently, or through the use of continuous residual monitors.

- Easy access to remote assets throughout the system could be problematic. Additional protection may be needed.

Since the probability of incidental security breaches that could be considered potential contamination threats is relatively high, utilities should consider approaches to manage this threat. One strategy is to harden system assets that could be targeted by adversaries who intend to contaminate the water or by vandals whose activities while trespassing could be interpreted as a threat of contamination. Controlling access to assets that may be attractive targets to terrorists as well as vandals, such as distribution system storage tanks and pump stations may reduce the occurrence of false contamination threats resulting from incidental security breaches. However, security improvements that may be sufficient to keep vandals away from these assets may not be sufficient to deter a motivated terrorist. It is also recommended that utilities document procedures for dealing with contamination threats in their emergency response plan. Procedures for responding to contamination threats might include a protocol for establishing the credibility of a threat, sampling procedures, criteria for triggering public health response measure (such as issuing a boil water order), and a risk communication plan.

Early Warning Systems for Intentional Contamination Events

As concerns regarding the contamination threat to water have risen, there has been increasing interest in early warning systems (EWS) to detect intentional contamination events in water systems. An EWS is a monitoring strategy that is capable of detecting an event with sufficient time for an appropriate response (i.e., steps to protect public health). Issues to consider in the design and implementation of an EWS are discussed in more detail in Appendix F. Some factors to consider before implementing an EWS include:

- Currently, an ideal EWS that can monitor for all potentially harmful contaminants does not exist; however, some monitoring technologies may be able to serve as an EWS for some contaminants.
- An EWS should allow for secure remote operations so that the sensors can be deployed at key locations, but managed from a central location.
- Two key features of an EWS are the ability to screen for a range of contaminants and the ability to positively identify a specific contaminant. These two features are often in competition with one another, and it will likely be necessary to strike a balance between screening and specificity.
- It is important to characterize the performance of the monitoring technology to ensure that it is capable of meeting the objectives of the EWS. Specific performance variables include: specificity, sensitivity, accuracy, precision, recovery, rate of false positives, and rate of false negatives.
- Before initiating an EWS, the objectives of the monitoring program should be clearly defined, and a plan should be developed for the interpretation, use, and reporting of monitoring results. This could be done in the context of a utility's emergency response plan.

3.4 Cyber Attack

Recent trends to automate asset management programs, linkages between asset management and maintenance scheduling databases, automated business operations such as billings, and increased use of modern Supervisory Control and Data Acquisition (SCADA) systems can increase the operational efficiency of water systems. It is also important to understand that the increased use of information management systems bring potential vulnerabilities to the water system through a cyber attack.

Potential Consequences of Significant Concern That Could Result from a Cyber Attack

- Loss of supply of pressurized water or potable water supply for a significant part of the system
- Adverse impacts due to public health or confidence from actual or threatened intentional contamination of the water with biological, chemical or radiological materials

Some of the key trends related to information management systems include:

- Utilities are transitioning from proprietary hardware and software platforms towards commercial off-the-shelf products (e.g., Windows, Unix, Cisco network devices etc.).
- For business purposes, SCADA systems are being connected to other information technology (IT) networks such as corporate Local Area Network (LAN) and the Internet.
- Many water utilities have “piggy-backed” their security systems on the SCADA system.

There may be unique vulnerabilities inherent to SCADA applications because those applications were not designed with security as a primary requirement, as may be the case for other networked IT systems. For example, a denial-of-service attack against a SCADA system that also supports the security alarm

system could put the entire utility at risk.

Conceivably, a wide range of IT adversaries could be using electronic means to attack the utility and they do not need to be physically present to attack. The adversaries range from the novice hacker up to a cyber terrorist. Obviously, the goals are different for different adversaries. While a novice may attempt to hack into the system just as a challenge, the cyber terrorist will typically be more focused and may try to intentionally disrupt the utility’s ability to provide treated water. Major differences in the nature of cyber attacks versus physical attacks have to do with the dynamics of the adversary capabilities. As software and/or hardware vulnerabilities are uncovered, they are often posted on the Internet and available to anyone willing to attempt an attack. Adversarial tools used in cyber attacks mature at an alarming rate, making it difficult to stay ahead of the threat.

For cyber attacks, insiders may be one of the major threats and are often overlooked. The assessment should include a review of all the administrative functions of information management and SCADA systems. Who has access and what level of access do they have? How

are passwords controlled? What type of remote access exists and who has privileges to use remote systems? What systems are inter-connected and who has access to them? What are the policies on installing new software? These questions as well as many others need to be answered to understand the vulnerabilities of the information and SCADA systems.

Water systems should also assess Internet and Intranet access on their computer networks and whether there are linkages from these to the automated operational control and management programs. Where links are found, security patches, firewalls and other network protection programs should be considered to reduce cyber intrusion risks.

**Have You Already Improved Security?
Consider Whether These Strategies Apply To You.**

- Policies for information management system and SCADA administration, including protecting sensitive data;
- Employee training and security monitoring of IT systems;
- Restricted access to the SCADA control room and equipment;
- Separate communication system for security alarm systems;
- Non-shared boot-up and screen saver passwords; and
- Virus-checking software, security patches on the SCADA and information management networks.

3.5 Attack on Related Infrastructure on which the Water System is Dependent

***Consequences of
Significant Concern That
Could Result from an
Attack on Related
Infrastructure***

- Loss of supply of pressurized water or potable water supply for a significant part of the system

The water infrastructure is highly interdependent with several other critical infrastructures, for example electric and gas utilities, transportation systems, telecommunications, and chemical manufacturers and distribution. Destruction of these interdependent infrastructures could significantly hinder or halt water utility operations for an indefinite period. Of considerable concern is the reliance on electrical power to operate the majority of water utilities.

During the assessment the water utility should review significant electrical interfaces owned by the water utility and work with the local power utility to track assets of the system back to at least the nearest substation. The review should help the utility

understand how the power is delivered, from where, the condition of the electrical equipment, and what plans the utility has in case of a power outage.

Since the water utility does not own or operate anything beyond the incoming feeders, it is important to develop a close relationship with the local power utility and develop contingency plans in the event of a loss of the substation providing incoming power. Local power utilities or other third party providers may have emergency back-up systems that could be used in the event of a power outage. Utilities should undertake periodic exercises to ensure back-up system readiness. The electrical power system can also impact the information management and SCADA and communication systems as well, so it is important to understand what works and what does not during an outage, and how long the back-up systems will operate.

Similar analyses should be undertaken concerning the utility's dependence on other infrastructures as mentioned in the first paragraph of this section. For example, utilities may want to analyze for disruption of delivery of needed chemicals or diesel fuel for back-up generators due to interruption of the transportation system. Another concern may be the loss of communications capability during an emergency due to an overload of the telecommunications networks.

**Have You Already Improved Security?
Consider Whether These Strategies Apply To You.**

- Formal agreements or joint contingency plans with related critical infrastructure;
- Joint emergency response exercises;
- Up-to-date emergency contacts; and
- Back-up power.

3.6 Additional Considerations

In addition to credible threats and suspicious incidents, water utilities, like other forms of critical infrastructure, are susceptible to the damaging consequences of psychological attacks in the form of hoaxes. For this reason, water utilities need to be prepared to manage the emotional responses that these attacks can invoke from the public, utility employees, and responders. Detection devices and monitoring protocols will be useful for responding to and recovering from hoaxes as well as actual contamination events.

APPENDICES

APPENDIX A:

Homeland Security Advisory System for Water Utilities developed by the Bay Area Security Information Collaborative (BASIC)

The *Homeland Security Advisory System for Water Utilities* was developed in California as a joint collaboration of the Bay Area Security Information Collaborative (BASIC) in an effort to establish a consistent response among the bay area water utilities. Table A.1 is based on the Federal Office of Homeland Security Advisory System (HSAS), which is intended to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist attacks to Federal, State, and local authorities.

The *Homeland Security Advisory System* characterizes levels of vigilance, preparedness, and readiness in a series of graduated threat conditions. The protective measures that correspond to each threat condition are examples for response, designed to be adaptable to changing threat conditions. As the threat condition changes so will the protective measures.

Table A.1

Condition	Consequence (Real or Imminent)	Protective Measure
LOW (GREEN)	Low risk of terrorist attack.	Conduct on-going facility assessments; develop, test, and implement emergency plans.
GUARDED (BLUE)	General risk of terrorist attack.	Activate employee and public information plan as needed; exercise communication channels with response teams and local agencies; review and exercise emergency plans.
ELEVATED (YELLOW)	Significant risk of terrorist attack; water utilities are a potential target.	Increase surveillance of critical facilities; coordinate response plans with allied utilities and response agencies; and implement emergency plans, as appropriate.
HIGH (ORANGE)	High risk of terrorist attack; water utilities are potential targets.	Limit facility access to essential staff only. Coordinate security efforts with armed forces or local law enforcement.
SEVERE (RED)	Severe risk of attack; a specific utility has been identified.	Decision to close specific facilities. Redirect staff resources to critical operations only.



APPENDIX B:

CHEMICAL SAFETY AND EMERGENCY PLANNING REGULATIONS

This appendix briefly describes the safety and emergency planning regulations that apply to the use of gaseous chlorine and other toxic Chemicals at water utilities. It is not intended as a substitute for the regulations themselves. Readers who desire more information on these or other applicable regulations should read the appropriate regulations and consult agency guidance materials and other available resources.

B.1 OSHA Process Safety Management Standard

Some water utilities that store or use more than 1500 pounds of gaseous chlorine (or other listed toxic Chemicals) in a process are required to comply with the OSHA Process Safety Management (PSM) rule (29 CFR Part 1910.119). This rule is designed to prevent or minimize the consequences of catastrophic releases of highly toxic Chemicals by requiring subject facilities to design and operate safe processes, and plan for emergencies. Briefly, the requirements of the PSM rule include:

- Employee participation - employers must consult with employees in developing and implementing the various safety measures required under the rule.
- Process safety information - compile complete documentation regarding hazardous chemical processes, including chemical hazard information, process technology information, and equipment information.
- Process hazard analysis - perform a systematic analysis of process hazards, and implement appropriate mechanisms to control hazards that are identified.
- Operating procedures - develop and implement written operating procedures that provide clear instructions for conducting activities involved in the process, accounting for each operating phase (e.g., normal operations, startup, shutdown, emergency operations, etc.).
- Training - employees involved in operating the process must be trained in operating procedures, safe work practices, emergency operations, etc.
- Contractors - employers must inform contract employees of hazards, explain emergency plan, evaluate the safety performance of contract employees. Contract employers must ensure that contract employees are instructed in process hazards, are trained to safely perform his or her job, and follow applicable safety procedures.
- A pre-startup safety review for new facilities or significantly modified facilities.
- Mechanical integrity - establish and implement written procedures to maintain the integrity of process equipment, conduct training for employees involved in equipment maintenance, conduct inspections and tests, and correct equipment deficiencies.
- Hot work permits - issue permits for hot work conducted on or near a covered process to ensure that appropriate fire prevention and protection measures are taken.
- Management of change - establishes and implement written procedures to manage changes to process chemicals, technology, equipment, and procedures.
- Incident investigation - investigate each incident that resulted in or could have resulted in a catastrophic chemical release.

- Emergency planning and response - establish and implement an emergency action plan for handling chemical releases.
- Compliance audits - conduct a compliance audit to certify compliance with rule requirements at least every three years.
- Trade secrets - make necessary information known to those responsible for compiling process safety information, conducting process hazard analyses, developing procedures, performing incident investigations or compliance audits.

The OSHA PSM rule does not apply to publicly owned facilities in states that have not been delegated authority by federal OSHA to implement the PSM rule. About half of the states have not received such delegation; publicly owned utilities in these states are not required to comply with the OSHA PSM rule. Other chemicals besides chlorine that may be present at water utilities may also trigger PSM requirements.

B.2 EPA Risk Management Plan (RMP) Regulation

Utility processes containing more than 2500 pounds of chlorine gas are regulated by the EPA. This regulation requires operators of these processes to take the following actions:

- Implement an accident prevention program (applicable to most RMP facilities). RMP facilities fall into one of three accident prevention program levels - Programs 1, 2, and 3. Program 3 is the most rigorous level, and applies to RMP-covered water utilities that present a risk to offsite public receptors and who are also covered by the OSHA PSM standard. For these utilities, the accident prevention requirements under the RMP rule are virtually identical to those of the OSHA PSM standard. RMP Program 1 applies to utilities that meet RMP applicability criteria but do not present a serious risk to offsite public receptors. These facilities are not required to implement an RMP accident prevention program in order to comply with the RMP rule. However, other RMP requirements still apply to these facilities, and they may still be required to implement accident prevention measures under OSHA PSM if they are covered by that standard. Utilities that meet the RMP chemical threshold, but fall into neither of the previous program levels are in RMP Program 2. These utilities are required to implement a streamlined set of accident prevention program measures derived from the OSHA PSM set.
- Conduct a hazard assessment. All RMP facilities must perform a hypothetical estimate of the consequences of a worst-case chemical release (a worst-case scenario), and prepare a five-year accident history including information about any accidents that meet certain threshold triggers (e.g., fatalities, serious injuries, etc.). Facilities in RMP Program 2 or 3 must also perform one or more alternative release scenarios. Alternative release scenarios are hypothetical estimates of the consequences of accident scenarios that are considered more likely than the worst-case scenario.
- Prepare and implement an emergency response plan. Program 2 and 3 facilities that use their own employees to respond to accidental releases must develop and implement an emergency response program and plan that include procedures for informing the public and local emergency responders about accidental releases, documentation of proper

treatment for chemical exposures, procedures for responding to releases, and employee training in emergency procedures and the proper use of emergency equipment. Program 2 and 3 facilities that do not use their own employees to respond to accidental releases must ensure that the facility is included in the community emergency response plan and implement appropriate mechanisms to notify emergency responders when there is a need for a response. Program 1 RMP facilities must coordinate emergency response with local emergency planning and response agencies.

- Send a summary report, called the Risk Management Plan, to EPA. The Risk Management Plan provides government officials information about the facility's toxic chemicals, accident prevention measures, and emergency response plans. Risk Management Plans are also available to the public (the worst-case and alternative release scenario portions of the plan are available to the public only on a restricted basis).

These requirements, like the OSHA PSM requirements, are designed to prevent catastrophic chemical accidents and minimize the consequences of those that do occur. Although not specifically intended to enhance security of utility chemical processes, some of the actions taken under the Risk Management Program will effectively increase site security. For example, a well-maintained vessel or piping system will be more difficult for a criminal or terrorist to breach than a poorly maintained one. Similarly, emergency process operations and shutdown procedures will allow a facility to safely respond to process upset conditions that may arise due to criminal activity. The Process Hazards Analysis (PHA) conducted by many RMP facilities is well suited for consideration of hazard reduction options - a critical step in reducing a facility's security vulnerability. Many facilities already use a PHA approach to evaluate hazard reduction options. A good emergency response program should help mitigate the effects of any chemical release that does occur, whether it occurs accidentally or not.

Other chemicals that may be present at water utilities, including ammonia, sulfur dioxide, and chlorine dioxide, also trigger RMP regulatory requirements if they exceed certain threshold quantities in a process. The RMP threshold quantity is 10,000 pounds for anhydrous ammonia, 5000 pounds for anhydrous sulfur dioxide, and 1000 pounds for chlorine dioxide.

B.3 Emergency Planning and Community Right-to-Know Act (EPCRA) and Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)

The Emergency Planning and Community Right-to-Know Act of 1986 (also known as SARA Title III or EPCRA) establishes requirements for Federal, State and local governments and industry regarding emergency planning and "Community Right-to-Know" reporting on hazardous and toxic chemicals. EPCRA has sections covering emergency planning, emergency release notification, and community right-to-know reporting requirements that are relevant to water utilities.

- Emergency planning. Water utilities holding more than a threshold planning quantity of an extremely hazardous substance (100 or more pounds for chlorine) must meet specific requirements that include having an emergency response plan and providing the local emergency planning committee and/or fire service with information that indicates the

location and maximum quantities of chemicals on-site. Presently, information must also be made available to the public upon request.

- Emergency release notification. Water utilities that experience an accidental release of an EPCRA extremely hazardous substance or CERCLA hazardous substance in a quantity greater than its designated reportable quantity (10 pounds for chlorine, 100 pounds for hypochlorite) must notify local and state authorities and the National Response Center.
- Community right-to-know reporting. Water utilities located in states that administer the OSHA program under a delegation from the federal government must comply with the community right-to-know provisions of EPCRA requiring facilities to submit copies of their Material Safety Data Sheets (MSDSs) or a list of MSDS chemicals to the local emergency planning committee, state emergency response commission, and the local fire department with jurisdiction over the facility.

B.4 Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA)

Chlorine and hypochlorite are both registered under the Federal Insecticide, Fungicide, Rodenticide Act (FIFRA) as pesticides and are required to be labeled following EPA instructions when used as a disinfectant. In 1999, EPA issued a Registration Eligibility Decision (RED) on chlorine gas (1999, FR 65, 56305). The registration will classify chlorine as a restricted use chemical in water and wastewater treatment plants. The restricted use classification will require all applicators to obtain certification, which would require training in the safe handling and application of chlorine gas. This decision, if finalized, will also impose new labeling requirements on containers of chlorine gas, as well as safety requirements for operators of chlorine gas systems.

B.5 Other OSHA Safety Regulations

There are several other important OSHA safety regulations applicable to worksites containing toxic Chemicals such as chlorine gas. These include, but are not limited to:

- The OSHA Hazard Communication Standard (29 CFR 1910.1200);
- Standard for Control of Hazardous Energy (Lockout/Tag out) (29 CFR 1910.147);
- Respiratory Protection Standard (29 CFR 1910.134);
- Personal Protective Equipment Standard (29 CFR 1910.132); and
- HAZWOPER Standard (29 CFR 1910.120).

These are some of the OSHA safety regulations that may apply to water utilities, whether or not chlorine gas or other listed toxic Chemicals are present. Consult with applicable OSHA guidance, your trade association, or other available resources to determine whether particular OSHA regulations apply to your utility.

APPENDIX C:

Summary of Characteristics, Advantages, and Limitations of Drinking Water Disinfectants and Other Hazardous Chemicals

This Appendix C primarily presents a summary of characteristics, advantages, and limitations of disinfectants typically used in drinking water treatment. The appendix also includes information on additional hazardous chemicals used in the treatment plant. This appendix does not include every disinfectant or chemical that may be used in a treatment plant, but focuses on the most prevalent. This information is provided to support the utilities' efforts to minimize the risk associated with the use, storage and transport of hazardous chemicals as they perform their vulnerability assessments.

Disinfectants are primarily added to inactivate disease-causing microorganisms. Because of their strong oxidizing nature, which accounts for their microbial inactivation efficiency, they can also be used to meet other treatment objectives in water such as the control of algae, oxidation of taste and odor causing compounds, oxidation of iron and manganese and destruction of organic pollutants.

For more details regarding inactivation efficiency, disinfection chemistry, analytical methods, and mode of application, refer to *Alternative Disinfectants and Oxidants Guidance Manual*, USEPA 1999 available at www.epa.gov/safewater/mdbp/alternative_disinfectants_guidance.pdf

C.1 Individual Disinfectants

Chlorine gas

Characteristics: Chlorine gas is the most widely used disinfection alternative for water utilities. Its effectiveness, relatively low cost, high reliability, and ease of operation contribute to its popularity. Chlorine is produced, collected, purified, compressed, cooled, packaged, and shipped as a liquefied gas under pressure. In water disinfection, chlorine gas is injected into the water stream, where the hydrolysis and ionization reactions take place.

Chlorine gas is about 2.5 times denser than air, is pungent, and has a noxious odor and a greenish-yellow color. It is highly irritating to the eyes, the nasal passages, and the respiratory tract. It can be lethal if a few breaths are taken at concentrations as low as 0.1 percent (1000 ppm). While chlorine gas itself cannot burn, it does support combustion, similar to oxygen. It is not explosive but will react violently with gasoline, greases, turpentine and other hydrocarbons, ammonia, metal filings, and other flammable materials.

If exposed to the atmosphere, for example via a container breach, elemental chlorine will rapidly volatilize and typically disperse in the downwind or downgrade direction, posing a real risk to site workers as well as any nearby populations. Because of its hazardous nature, chlorine gas requires special handling and storage. It is shipped and used in 150 lb cylinders, 1-ton containers, or 90-ton railroad cars. In the extreme event of a release of the total contents of a 1-ton container of chlorine gas, people located within as much as a mile of the point of release could

potentially be injured or die under the most unfavorable possible weather and topographic conditions according to the predictions of some analytical models. A larger release, such as the contents of a 90-ton chlorine railcar, could be catastrophic over a much greater area.

Chlorine should be stored in a cool, dry, well-ventilated area that is labeled in accordance with OSHA's Hazard Communication Standard [29 CFR 1910.1200]. More detailed information on regulations related to chlorine gas (such as Risk Management Plan requirements under the Clean Air Act 112r) are described in Appendix B. Standard chlorine containers are robust, high-strength vessels, designed to DOT specifications to withstand large physical stresses without failure. Containers of chlorine should be protected from exposure to weather, extreme temperature changes, and physical damage, and they should be stored separately from flammable and combustible substances. Full and empty containers must be clearly identified, separated, and properly labeled. Workers handling and operating chlorine containers, cylinders, and tank wagons should receive special training in standard safety procedures for handling compressed corrosive gases. Each site with at least 100-lbs. of chlorine is required to have emergency response plans under SARA Title 3 which typically includes but is not limited to chlorine leak detectors, self-contained breathing apparatuses, and emergency repair kits. All pipes and containment used for chlorine service should be regularly inspected and tested. Empty chlorine containers should have secured protective covers on their valves and require appropriate handling.

Advantages: Chlorine gas can be used both for primary and secondary disinfection. From a public health perspective, chlorine gas is an effective disinfectant and can inactivate many microbial contaminants. It is also a strong oxidant, which makes it effective at controlling algae, taste and odor compounds, and oxidizing iron and manganese. The use of chlorine gas as a disinfectant is not a complicated process. Once operators are trained on how to safely handle chlorine gas, few accidental problems should occur.

Chlorine gas can provide a residual for the distribution system and can be used for booster disinfection. At least one third of the biological contaminants identified as plausible threats are susceptible to typical chlorine levels used in distribution systems. Maintaining a residual in the distribution system and monitoring for changes in the demand may be a protection against the risk of contamination by unknown agents in the distribution system. Additional research is necessary to confirm the efficacy of chlorine against many specific agents.

Disadvantages: One of the main disadvantages of using chlorine gas is the danger associated with the release of the gas. The gas is poisonous and the release results in volatilized elemental chlorine, which will disperse downwind and pose a threat to site workers as well as to neighboring populations. If the release is large, this may be catastrophic resulting in injury and death. Therefore, using chlorine gas requires special handling and storage and requires special equipment to ensure safe handling and feeding of the gas. Transportation also presents a risk for accidental releases

As a disinfectant, it is not effective against some microorganisms and spores. For example, chlorine is ineffective against *Cryptosporidium* at concentrations typically applied in drinking water treatment.

Another disadvantage of using chlorine gas is the formation of halogenated disinfection byproducts (DBPs) that are of health concern and should be controlled to minimize population exposure. Standards are set under the Stage 1 Disinfectants/Disinfection Byproducts (D/DBP) Rule (1998, 63 FR 69390) to ensure that DBP concentrations are less than the maximum contaminant levels (MCLs). However, utilities need to balance the risk from DBPs against the risk from pathogens. Also, smaller molecular weight oxidation byproducts are formed and if not removed by biological processes, may cause microbial regrowth in the distribution system.

Sodium hypochlorite (NaOCl)

Characteristics: The solution is a clear, light-yellow liquid. It is produced by reacting chlorine with sodium hydroxide and is sometimes referred to as liquid bleach. Commercial or industrial grade solutions have hypochlorite strengths of 10 to 20 percent. The sodium hypochlorite solution is alkaline with a pH of 9 to 12, depending on the amount of excess sodium hydroxide. The solution can be purchased in 1- or 5-gal carboys, 55-gal lined, steel drums or polyethylene barrels, and even tanker trucks. The stability of sodium hypochlorite depends on the hypochlorite concentration, storage temperature, time storage, impurities, pH, and exposure to light. At room temperature, sodium hypochlorite solutions can lose up to 2 to 4 percent of their available chlorine content per month adding to the cost of the operation due to the need to compensate for the diluted strength with increased chemical use.

Advantages: Hypochlorite can be used both for primary and secondary disinfection. From a public health perspective, similar to chlorine gas, it is an effective disinfectant and can provide inactivate many microbial contaminants. It is also a strong oxidant which makes it effective at controlling algae, taste and odor compounds, oxidizing iron and manganese. Sodium hypochlorite (10 to 20 percent available chlorine) can also provide a residual for the distribution system.

The use of sodium hypochlorite as a water disinfectant is increasing because it decreases the risk a of chlorine gas release. It is generally used in smaller systems because on a small scale, it is simpler to operate. It can also be used by large systems but many require more frequent intervention by operators and maintenance personnel than gaseous chlorine. It can be generated on-site, or transported as a liquid. At least one third of the biological contaminants identified as plausible threats are susceptible to typical chlorine levels used in distribution systems.

Disadvantages: One of the concerns associated with the use of sodium hypochlorite is the fact that the liquid is highly alkaline with a pH of 9 to 12, and therefore requires operators to wear appropriate personal protective equipment. Although there is no fire hazard associated with sodium hypochlorite, it is very reactive with metals. If sodium hypochlorite is inadvertently mixed with an acid or other incompatible chemical, significant amounts of chlorine gas can be released, potentially resulting in serious harm to people in the vicinity. Utilities that use sodium hypochlorite should supervise the delivery process and ensure that the liquid is delivered to the correct storage tank.

As a disinfectant, it is not effective against some microorganisms and spores. For example, hypochlorite is ineffective against *Cryptosporidium* at concentrations typically applied in drinking water treatment.

Another health concern is the formation of unintended DBPs including halogenated organic compounds (similar to formation reactions with chlorine gas) and chlorite and chlorate (the latter two DBPs are formed from the decomposition of sodium hypochlorite - chlorite is an intermediate in the formation of chlorate). Another DBP of concern is bromate, which may be formed from contaminants in the salts used for the generation of sodium hypochlorite. Bromate is regulated under the Stage 1 D/DBP Rule at an MCL of 0.010 mg/L (1998, 63 FR 69390). These DBPs are of health concern and most are regulated under the Stage 1 DBP Rule. Smaller molecular weight oxidation byproducts are formed and if not removed by biological processes may cause microbial regrowth in the distribution system.

From an operational perspective, a disadvantage of using sodium hypochlorite is the fact that it loses its strength over time and needs to be frequently replaced. Some utilities use a diluted solution (from the stock) that allows for longer storage times. In all scenarios, determining the actual concentration of the dosing solution is critical to meeting the demand and ensuring the presence of a residual. Given that the solutions contain about 80 to 85 percent water, large storage volume is needed for larger facilities. The use of hypochlorite may create a storage concern for large disinfection processes.

Other operational difficulties are:

- Given the alkaline pH of the solution, some final pH adjustment problems may be engendered.
- Scale formation and possible plugging of injectors in hard waters
- Increased maintenance requirements associated with the feed process, primarily because of vapor locking in the feed pumps given the incompatibility of sodium hypochlorite with some facility materials. Gas binding in feed pumps can interrupt the disinfectant flow, therefore, degassing the feed is recommended.
- On-site generation generally requires significant operator attention.
- There are currently no quality control requirements for the salts used in the production of hypochlorite.

Calcium hypochlorite (Ca (OCl)₂)

Characteristics: Calcium hypochlorite is a dry white or yellow-white granular solid and is also available as compressed tablets. It contains about 65 percent available chlorine by weight. It can be produced by combining equivalent amounts of sodium hypochlorite and calcium chloride. A slurry of lime and caustic soda is chlorinated and cooled to form the crystals. When used in a treatment plant, it is mixed with water to form a dilute hypochlorite solution and fed in the same manner as sodium hypochlorite. For spot disinfection in pipes or small basins, tablets are deposited, water added, and a hypochlorite solution is formed.

Most of the advantages and concerns associated with the use of sodium hypochlorite apply to the use of calcium hypochlorite. Calcium hypochlorite also requires special storage to avoid contact with organic material. The reaction that results from such contact generates enough heat and oxygen to start and support a fire. Calcium hypochlorite has the added advantage of requiring no electrical power.

Chloramines

Characteristics: Chloramines are formed by the reaction of chlorine (gaseous or hypochlorite) and ammonia (anhydrous ammonia or aqueous salt solutions). Chloramines can be generated on-site (either by adding ammonia first followed by chlorine, or by adding chlorine first (for more effective inactivation) and then ammonia (to “quench” the chlorine and control DBP formation) or can be preformed and then added in the treatment plant. Typical application points are at open channels and basin facilities. Anhydrous ammonia is usually applied by direct feed or solution feed. Ammonia feed systems are located on-site and can either be gaseous (anhydrous ammonia) or liquid (aqueous salt solutions). The anhydrous form is a gas at ambient temperature and pressure but is generally transported as a liquid in a pressurized vessel. These cylinders are similar to chlorine cylinders and are typically 100, 150 and 800-lb. sizes. Some facilities use stationary tanks that are typically 1,000-gallon vessels that can be used on-site and are refilled by tanker trailers. When stored outdoors, cylinders should be protected from extreme temperatures, from direct sunlight, and from extreme heat to avoid pressure increases in the tank. If stored indoors, ventilation and vapor detection devices should be located at high points in the room. From a safety and security perspective, chlorine gas and ammonia gas should never be stored in the same room and the ammonia application points should be at least 5 feet away from the chlorine feed solution lines.

Advantages: Chloramines can be used for both primary and secondary disinfection and require significantly higher CTs (Concentration x Time) than chlorine for the equivalent inactivation. Chloramines are stable and very effective for controlling biofilms (limiting microbial regrowth) in distribution systems.

Another advantage of using chloramines is that fewer DBPs are formed compared with chlorine.

Disadvantages: Chloramines are weaker disinfectants than chlorine and are not effective against protozoa and viruses. Chloramines are ineffective for the inactivation of *Cryptosporidium* under the typical doses used in drinking water treatment. Chloramines cannot oxidize iron, manganese, or sulfides. Given that chloramines are weak oxidants, other oxidants (primary disinfectants) may need to be added in the treatment plant to meet operational needs. Excess ammonia from the generation of monochloramine may cause nitrification problems in the distribution system, particularly in dead ends and other low disinfectant residual locations. Distribution systems that use chloramine disinfection typically require a chlorine burnout period to prevent nitrification problems.

From a security perspective, chloramines require the use of both chlorine (gas or hypochlorite) and ammonia and thus have the same security concerns that exist with the use of chlorine as well as release and corrosivity concerns associated with ammonia.

From a health perspective, while halogenated DBP formation is lower than when chlorine is used, the formation of nitrogenous DBPs, such as N-nitrosodimethylamine (NDMA), may be a health concern. Also, chloramines need to be removed from water that is used for kidney dialysis as they can pass through the dialysis membranes and pose a health hazard to patients. Chloramines can also be harmful to fish in aquariums.

Chlorine Dioxide

Characteristics: Chlorine dioxide is formed by the reaction of a sodium chlorite (NaClO_2) solution with an oxidizing agent. The oxidizing agent can be any of the following: 1) gaseous chlorine or hypochlorite solutions; 2) a mineral acid with or without chlorine; and 3) an acid in combination with a hypochlorite solution. The generation process occurs on-site in mechanical generators. For details on the generation of chlorine dioxide, refer to Gates (1998).

The aqueous solution is generally dark to light yellow or greenish. A dark brown color is generally an indication of generator malfunction and the production of pure chlorine dioxide, which is extremely unstable and explosive as a gas. The explosive nature of highly concentrated solutions (greater than 10 g/L) depends on the partial pressure of the gas itself, the solution temperature, and the water vapor pressure in the space above the solution.

Advantages: It is an effective oxidant and disinfectant, is stronger than chlorine for the inactivation of *Cryptosporidium*, *Giardia*, and viruses, and provides better inactivation at a wider pH range, particularly at higher pH. However, inactivation levels are restricted by the MCL for chlorite. Chlorine dioxide is a powerful disinfectant for primary disinfection, however it is not commonly used for secondary disinfection.

From an operational perspective, chlorine dioxide is generally used for taste and odor control and for the oxidation of iron, manganese, phenolic compounds and sulfides. The disinfectant will not form trihalomethanes except if free chlorine is present, but can form some other organic halogenated DBPs (disadvantage). Therefore, the generation process should be optimized to prevent the presence of excess chlorine, which leads to the formation of these DBPs.

Disadvantages: Using chlorine dioxide requires the transportation and storage of chemicals including chlorine (gaseous or hypochlorite). So, from a security perspective, chlorine dioxide has all the same security concerns associated with gaseous chlorine or hypochlorite. Additionally, the disinfectant, once formed is highly toxic and may be explosive. Because it has to be generated on-site, the production process is expensive and requires careful operation.

Chlorine dioxide cannot be used as a secondary disinfectant because at concentrations needed to maintain a residual for the distribution system, a taste and odor problem occurs. It can sometimes be used for residual disinfection in low-oxidant demand waters.

One of the main disadvantages of using chlorine dioxide is the production of chlorite and chlorate, as byproducts of reaction with organic matter in water. Once formed, chlorate is stable and will remain in the distributed water. Chlorite is not very stable and ultimately converts to

chlorate. Chlorite is regulated under the Stage 1 DBP Rule because of health concerns associated with the ingestion of this byproduct.

Ozone

Characteristics: Ozone exists as a gas at room temperature. The gas is colorless with a pungent odor readily detectable at concentrations as low as 0.02 to 0.05 ppm (by volume), which is below concentrations of health concern. Ozone gas is highly corrosive and toxic.

Because of its instability, ozone is generated at the point of use. Ozone can be generated from oxygen present in air or high purity oxygen [liquid oxygen (LOX)] and requires considerable energy. Ozone is used for primary disinfection and chemical oxidation and cannot be used for secondary disinfection because it is highly reactive and does not maintain residual levels in the distribution system.

Advantages: Ozone is one of the most potent and effective germicides used in water treatment. It is effective against bacteria, viruses, and protozoan cysts. Inactivation efficiency for bacteria and viruses is not affected by pH (at pH levels between 6 and 9). However, as pH increases, ozone decomposition increases (providing less CT). As water temperature increases, ozone disinfection efficiency increases. Ozone is a powerful oxidant and can oxidize many organic and inorganic compounds in water. Therefore, it is used for oxidation of iron, manganese, sulfides, color, taste and odor.

It does not form halogenated organic DBPs except for some bromine-substituted DBPs if the precursor bromide is present in the water. Ozone's oxidation of the organic matter also decreases the potential for DBP formation upon subsequent residual disinfection (using chlorine or chloramines).

The use of pre-ozonation as a coagulant-aid results in better organic matter removal in the coagulation/flocculation and sedimentation process, thus improving the removal of DBP precursors.

Disadvantages: Ozone is unstable, particularly at higher pH, and will not provide a residual for secondary disinfection. Chlorine or chloramines have to be added to provide a residual for the distribution system.

Ozone is a highly corrosive and toxic gas. It can be a hazard to operators if any leaks occur. On-site monitors are used to detect leaks that may occur during operation. From an operational perspective, the process is relatively sophisticated and requires trained operators. The process is expensive, relative to chlorine, and requires power for operation.

From a security perspective, ozone formed from LOX requires the storage of oxygen on-site. Oxygen can support combustion, thus the storage facility should be well protected to prevent any misuse of the gas.

Ozone can oxidize bromide to form bromate, a carcinogen, and some bromine-substituted DBPs that are of health concern. Other by-products are the low molecular weight aldehydes, ketones, ketoacids, and carboxylic acids. These compounds, if not removed by biological filtration, may serve as a substrate for microorganisms and promote microbial regrowth in the distribution system.

Ultraviolet Radiation (UV)

Characteristics: when used as a disinfection technology, microorganisms absorb UV radiation. UV radiation penetrates the cell wall and reacts with the nucleic acids and other cell parts resulting in injury and loss of infectivity.

The UV radiation waves are electromagnetic waves 100 to 400 nm long (between the X-ray and visible light spectrums). The optimum disinfection range is between 245 and 285 nm. The process utilizes low-pressure lamps with a maximum output at 253.7 nm or medium pressure lamps that emit energy at wavelengths of 180 to 1370 nm. Lamps that emit pulsed light at high intensity have also been used. Typical disinfection lamps are made of quartz tubes filled with an inert gas (such as argon) and small quantities of mercury.

Advantages: UV radiation is applied directly to the water and is only used for primary disinfection. The disinfectant is very effective for the inactivation of many microorganisms, particularly *Cryptosporidium* and *Giardia*. Moreover, UV inactivation is not pH dependent. UV light does not involve any chemical addition and therefore has no chemical storage, handling, or transportation concerns. No feed equipment is necessary either. It is not as sensitive as other disinfectants to water quality except to turbidity. To date, no identified byproducts of health concern have been reported.

Disadvantages: UV radiation can only be used as primary disinfectant because it does not provide residual disinfection and chlorine or chloramine need to be added to provide a residual for the distribution system.

While used and tested for wastewater treatment, the technology has not been extensively used in drinking water treatment. The disinfection process requires power, which is expensive, and turbulent flow conditions are needed to ensure mixing. UV radiation is very sensitive to turbidity; particulates in turbid water prevent the UV radiation from being absorbed by the organisms.

The following factors are known to negatively impact the effectiveness of UV radiation:

- Chemical or biological films that form on the surface of the lamps;
- Clumping of microorganisms;
- Turbidity and color; and
- Short-circuiting leading to ineffective mixing.

C.2 Disinfectant Combinations

The above advantages and limitations apply to the individual disinfectants and do not address advantages obtained from combining these disinfectants. In drinking water treatment, combinations of these disinfectants are usually used. The disinfectant choices depend on the purpose for the application and the water quality. No general rules can be provided because the disinfectant choices are very site specific and water quality dependent. For example, a water source that is high in bromide has to choose a disinfectant and apply it in such a way to ensure that formed bromate levels are below the MCL for the Stage 1 D/DBP Rule MCL.

As systems examine the disinfectant choices that work best for their treatment plant, it is recommended that they select disinfectants that can accomplish multiple goals and improve public health protection. The application of sequential disinfection has been shown to provide better disinfection than individual disinfectants. Details of the benefits of using combinations of disinfectants are presented in *Alternative Disinfectants and Oxidants Guidance Manual*, USEPA 1999.

While EPA does not recommend that systems use one disinfectant over another, EPA recommends that primary and secondary disinfectants be selected to minimize hazards from the disinfectant choice and to ensure public health protection. Disinfectant combinations should take into account the synergistic effects that can be gained. Disinfectants should be carefully chosen with the goal of minimizing contact times and high doses in order to control the formation of DBPs. EPA also recommends that systems consult the States if a change in disinfectant is decided upon. This is done to evaluate the profiling and benchmarking requirements as described in 40 CFR, 141.172. Disinfection benchmarking is a procedure requiring certain public water systems to evaluate the impact on microbial risk from changes in disinfection practices. This is done by compiling daily measurements of disinfectant residual concentrations, contact times, temperature and pH over a period of one year to develop a disinfection profile for *Giardia* and virus inactivation.

C.3 Other Hazardous Chemicals Used in Drinking Water Systems

The following chemicals that are generally used in drinking water treatment plants are considered hazardous substances and fall under the OSHA Hazard Communication Standard 1910.1200, which requires employers to follow safe handling procedures. This listing is not all-inclusive but highlights the chemicals most commonly used by drinking water systems:

Ammonia

Ammonia is a corrosive chemical (a colorless gas with a strong odor) that can irritate and burn the skin and eyes. Ammonia reacts with chlorine to form chloramine, a disinfectant used to provide residual disinfection for the distribution system. Generally, either ammonia gas or an ammonium compound is used in the treatment plant to form chloramines, with a higher percentage of plants using ammonia gas over liquid ammonia. Exposure can irritate the nose, mouth and throat causing coughing and wheezing. Breathing ammonia can irritate the lungs with higher exposure causing build-up of fluid in the lungs (pulmonary edema). Exposure can also cause headache, loss of the sense of smell, nausea, and vomiting.

Ammonia reacts violently or produces explosive products when in direct contact with halogens such as chlorine and bromine. It is not compatible with strong acids (such as sulfuric or hydrochloric acids), permanganates, perchlorates, peroxides, and galvanized iron. It may also react with zinc, copper, tin, and their alloys.

It should be stored in tightly closed containers in a cool, well-ventilated area away from moisture, heat, and direct sunlight. Local exhaust ventilation in an enclosed operation area should be available in case of chemical release.

Oxygen (liquid oxygen (LOX) used to produce ozone)

Oxygen, a colorless, odorless gas, is naturally present at a concentration of 21 percent in the air. Liquid oxygen is odorless and has a slight blue color. If exposure to a concentration greater than 40 percent occurs, then there are some health risks. Liquid oxygen forms explosive mixtures with organic and other readily oxidizable materials and therefore, should be stored outdoors and in a location to avoid contact with oil, grease, or other combustible material. Oxygen can support combustion and should therefore be kept away from any sources of ignition such as smoking and open flames.

Silicofluoric acid (Hydrofluosilicic acid, Hexafluosilicic acid)

Silicofluoric acid is a straw colored, transparent, fuming liquid with a sharp unpleasant odor. It is available as a 20 to 35 percent aqueous solution and is used in drinking water treatment for fluoride application. It is a highly corrosive chemical (aqueous solution has a pH of 1.2) and contact can irritate and burn the skin and eyes with possible eye damage. High exposures can cause nausea, loss of appetite and nosebleeds. Very high exposures can cause poisoning with stomach pain, weakness, convulsions and sometimes death. Repeated exposures can cause fluoridosis of the bones and teeth.

The acid should be stored away from combustibles since violent reactions can occur. Silicofluoric acid is not compatible with acids such as hydrochloric and sulfuric acids, oxidizing agents (such as peroxides, perchlorates, permanganates, chlorates, nitrates, chlorine, bromide, and fluorine) and organic compounds. The acid should not be stored in metal containers as it will readily corrode the metal and release flammable hydrogen gas. The acid should be stored in tightly closed containers in a cool, well-ventilated area. It should not be stored or dispensed in the same area as other chemicals.

Sulfuric acid

Sulfuric acid is a corrosive chemical that can severely irritate and burn the eyes and skin and may even cause blindness. Breathing vapors can irritate the nose and throat as well as the lungs, leading to coughing and shortness of breath. Higher exposures can lead to pulmonary edema (fluid build-up in the lungs). It is used in the treatment plant for pH adjustments.

The oily liquid is a reactive chemical and an explosion hazard. It should be stored to avoid contact with water, oxidizing agents (such as peroxides, perchlorates, permanganates, chlorates, nitrates, chlorine, bromide, and fluorine), strong bases (such as sodium hydroxide, and potassium hydroxide) and many other organic compounds. The acid should be stored in a tightly closed container in a cool dry well-ventilated area away from sunlight and combustibles. The area should have an acid resistant cement floor. Explosion-proof electrical equipment and fittings should be used when handling the acid. Contact of sulfuric acid with metal drums may cause the release of flammable and explosive hydrogen gas. Storage containers should be coated with acid resistant material. Sulfuric acid does not burn, but may ignite combustibles such as wood, paper, and oil.

Sodium hydroxide

Sodium hydroxide is a white, odorless pellet or solid often dissolved in water. It is a corrosive chemical and contact can severely irritate and burn the skin and eyes. Breathing vapors can result in irritation of the mouth, nose, and throat, with higher exposures leading to fluid build-up in the lungs. It is used in the treatment plant for pH adjustments.

As a solid, it can react with water to release heat and contact with aluminum, tin, lead, and zinc will release flammable and explosive hydrogen gas. Sodium hydroxide is not compatible with strong acids (such as hydrochloric acid, and sulfuric acids), organic peroxides, organic halogens and flammable liquids.

Ferric chloride

Ferric chloride is a black-brown solid that is usually dissolved in water. The solution is acidic and corrosive to most metals. In drinking water treatment, ferric chloride is used for coagulation and stored on-site. The compound is a strong irritant to skin and tissue. Symptoms of exposure to a concentrated solution include mouth and stomach irritation. Prolonged contact can cause irritation and burns.

Hydrogen peroxide

Hydrogen peroxide is a colorless liquid used as a common oxidizing agent. It is a corrosive chemical and contact can irritate the eyes and skin causing damage to the eyes. Breathing fumes can irritate the nose and throat as well as irritating the lungs. It is a highly reactive chemical and a dangerous explosion hazard. Hydrogen peroxide is also a mutagen and should be handled cautiously as a possible carcinogen. The chemical should be stored in tightly closed containers in a cool well-ventilated area, stored away from oxidizing agents, organic compounds, and strong acids. If in contact with combustibles, hydrogen peroxide may result in spontaneous combustion.

Other disinfection alternatives and chemicals

Several other chemicals such as sulfur dioxide and alum that may be used at water utilities also present potential safety risks. Sulfur dioxide is a volatile, toxic gas that, like chlorine, can cause

injury or death if inhaled. Sulfur dioxide is potentially a significant transportation risk, since it must be transported to the utility site and is highly volatile and toxic. However, it is not widely used at drinking water utilities.

APPENDIX D:

Treatment Barriers to Intentional Contamination

Synopsis: Many of the treatment processes used in drinking water treatment plants may be effective for removing, inactivating, or neutralizing contaminants that could be used in a terrorist or criminal act. Appendix D provides an overview of treatment efficacy for conventional treatment (coagulation, sedimentation, filtration, and disinfection) and select advanced treatment processes with respect to various contaminant classes. The appendix also highlights the importance of the residual disinfectant as a means of maintaining distribution system protection.

Notice:

If you are interested in obtaining the additional information contained in this appendix, fax or mail your request on your organization's letterhead stationery *signed by the community water system manager or designated security official*. Provide the name of the individual designated to receive the document, mailing address, phone number, and E-mail address.

Fax or mail your request to U.S. EPA. The fax number is 202-564-8513. The express mail delivery address is: Environmental Protection Agency, Attn: Documents Room 2104, EPA East, 1201 Constitution Ave. NW, Washington DC, 20004. *If you send the letter by U.S. Postal Service there will be a significant delay.* You will receive the document by registered U.S. mail.

As with the entire document, please hold all information contained in the appendices in confidence, and take reasonable precautions to protect it.

APPENDIX E:

Considering Contamination Threats during a Vulnerability Assessment

Synopsis: Along with physical and cyber attacks, the threat of intentional contamination should be evaluated during a vulnerability assessment; however, the complexity of the contamination threat can make this difficult. Appendix E presents a framework for evaluating the threat of intentional contamination during a vulnerability assessment. The framework is consistent with many vulnerability assessment methodologies in that vulnerabilities to attacks using contaminants are evaluated against a design basis threat. The framework establishes a systematic approach for developing contamination scenarios that can serve as design basis threats. To fully utilize this methodology, a utility will need a calibrated hydraulic model of its distribution system network. However, even if a utility does not have such a model, the methodology can still be applied in a less rigorous manner.

Notice:

If you are interested in obtaining the additional information contained in this appendix, fax or mail your request on your organization's letterhead stationery *signed by the community water system manager or designated security official*. Provide the name of the individual designated to receive the document, mailing address, phone number, and E-mail address.

Fax or mail your request to U.S. EPA. The fax number is 202-564-8513. The express mail delivery address is: Environmental Protection Agency, Attn: Documents Room 2104, EPA East, 1201 Constitution Ave. NW, Washington DC, 20004. *If you send the letter by U.S. Postal Service there will be a significant delay.* You will receive the document by registered U.S. mail.

As with the entire document, please hold all information contained in the appendices in confidence, and take reasonable precautions to protect it.

APPENDIX F:

Early Warning Systems for Detecting Contamination Events

Synopsis: One approach for avoiding or mitigating the impacts from an intentional contamination event is to perform monitoring in the context of an early warning system (EWS). The core of an EWS is the monitoring technology, and a typical EWS for water would utilize a technology that could detect or screen for toxic substances or infectious microorganisms. However, an EWS is much more than a monitoring technology – it is an integrated system for deploying the monitoring technology, analyzing and interpreting the results, and using the results in making decisions that are protective of public health while minimizing unnecessary concern and inconvenience within a community. Appendix F provides guidance on the design of EWSs and an overview of potential EWS monitoring technologies.

Notice:

If you are interested in obtaining the additional information contained in this appendix, fax or mail your request on your organization's letterhead stationery *signed by the community water system manager or designated security official*. Provide the name of the individual designated to receive the document, mailing address, phone number, and E-mail address.

Fax or mail your request to U.S. EPA. The fax number is 202-564-8513. The express mail delivery address is: Environmental Protection Agency, Attn: Documents Room 2104, EPA East, 1201 Constitution Ave. NW, Washington DC, 20004. *If you send the letter by U.S. Postal Service there will be a significant delay.* You will receive the document by registered U.S. mail.

As with the entire document, please hold all information contained in the appendices in confidence, and take reasonable precautions to protect it.

REFERENCES:

Disinfectants and Other Hazardous Chemicals

Abraham, R.G. et al., Design and Operational Issues for Converting Disinfection Facilities from Gas Chlorine to Sodium Hypochlorite, Proceedings AWWA Annual Conference, New Orleans, LO, June 16 – 20, 2002.

AWWA, Water Quality and Treatment, 4th Edition, McGraw Hill, Inc. 1990. [Chapters 12, 14 and 15].

AWWA, Introduction to Water Treatment Principles and Practices of Water Supply Operation Vol 2, 1984. [Module 10, Disinfection].

Gates, D. The Chlorine Dioxide Handbook. AWWA, Denver, CO.1998.

Gordon, G., Adam, L., Bubnis, B. Hoyt, B., Gillette, S., Wilczak, A. (1995) *Minimizing the Chlorate Ion Formation in Drinking Water When Hypochlorite Ion is the Chlorinating Agent*. American Water Works Association Research Foundation, Denver, CO.

U.S. Environmental Protection Agency. 1996. Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act, Section 112(r)(7); Final Rule. 61 FR 31668.

U.S. Environmental Protection Agency. 1998. National Primary Drinking Water Regulations: Disinfectants and Disinfection Byproducts; Final Rule. EPA-815-Z-98-008.

U.S. Environmental Protection Agency. 1999. *Alternative Disinfectants and Oxidants Guidance Manual*, EPA 815-R-99-014.

Contamination

Daughton, C.G. 2001. One Proposal for a Nation-Wide Approach to Identifying Emerging, Nascent Risks: Pollutant Fingerprint Anomalies.
<http://www.epa.gov/nerlesd1/chemistry/pharma/science-issues.htm>

International Life Sciences Institute Risk Science Institute. 1999. Early Warning Monitoring to Detect Hazardous Events in Water Supplies. ILSI PRESS, Washington, DC.

Kessler, A., Ostfeld, A., and Sinia, G. 1998. Detecting accidental contaminations in municipal water networks. *M.W. Resources Planning and Management*, pp. 192-198.

Lee, J.Y. and Deininger, R.A. 1992. Optimal location of monitoring stations in water distribution systems. *Jour. Environ. Eng.* 118(1): 4-16.

Speth, T.F. and R. J. Miltner. 1990. "Adsorption Capacity of GAC for Synthetic Organics", *J. Am. Water Works Assoc.*, 82(2): 72-75.

Speth, T.F., et.al., *Treatment Studies of CCL Contaminants*, Presented at the Water Quality Technology Conference and Exhibition Conference. Nashville, Tennessee, November 11-15, 2001

Speth, T.F. and J.Q. Adams. "GAC and Air Stripping Design Support for the Safe Drinking Water Act." *Strategies and Technologies for Meeting SDWA Requirements*. (Ann Arbor, MI: Lewis Publishers, Inc), 47-89.

U.S. EPA 1988. Methods for Aquatic Toxicity Identification Evaluations. Phase I Characterization Procedures. Duluth, MN. EPA/600/3-88/034.

U.S. EPA 1989a. Methods for Aquatic Toxicity Identification Evaluations. Phase II Toxicity Identification Procedures. Duluth, MN. EPA/600/3-88/035.

U.S. EPA 1989b. Methods for Aquatic Toxicity Identification Evaluations. Phase III Confirmation Procedures. Duluth, MN. EPA/600/3-88/036.

Office of Water (4606M)
EPA 810-R-02-002
www.epa.gov/safewater
September 2002

Printed on Recycled Paper

For Limited Distribution

56

To: Mr. Michael E. Murphy Town of Addison (972) 450-2837

From: AWWA (303) 795-1989 06/23/03 07:35PM

cc: JP
JD



**American Water Works
Association**

6666 West Quincy Avenue
Denver, CO 80235-3098
T (303) 794-7711
F (303) 795-1440
www.awwa.org

The Authoritative Resource for Safe Drinking WaterSM

TO: Utility Managers

FROM: Jack Hoffbuhr, Executive Director, AWWA

DATE: June 23, 2003

CONFIDENTIAL:
**SECURITY ADVISORY FROM THE OFFICE OF THE
U.S. DEPARTMENT OF HOMELAND SECURITY**

The attached confidential security advisory was released today by the U.S. Department of Homeland Security. This contains sensitive information and is intended only for general managers/directors of community water systems.

DO NOT DISTRIBUTE THIS CONFIDENTIAL ADVISORY

To: Mr. Michael E. Murphy Town of Addison (972) 450-2837

From: AWWA (303) 795-1989 06/23/03 07:35PM



Advisory
Potential Al Qaeda Threats to US Water Supply
June 23, 2003

The following advisory contains sensitive potential threat information. Distribution should be limited to utilities serving community water systems, State Drinking Water Administrators, Federally operated water systems, State and Federal public health agencies and their laboratories, and the Environmental Protection Agency.

Although the Department of Homeland Security (DHS) has no specific information indicating that an Al Qaeda attack against the US water supply is imminent, or that any specific target systems or locations have been identified, recent intelligence indicates that members of Al Qaeda had discussed plans to attack the US drinking water supply. Two potential attack scenarios were discussed: 1) disruption of water delivery through a physical attack on the water supply infrastructure, and 2) introduction of chemical or biological agents into water distribution systems and post-treatment facilities. DHS assesses both types of attacks to be difficult but feasible. Moreover, Al Qaeda has considered denial of water availability and creating mass casualties through contamination as equally important modes of attack. Both contamination agents and a physical attack could cause a denial of water availability. The former can cause denial of water availability by contaminating water mains and distribution systems severely enough to require officials to prohibit use of the water in order to protect public health. A denial of water availability attack could have cascading effects on other water-dependent sectors depending on the duration of the attack.

With respect to bio-chemical contamination of the drinking water supply, Al Qaeda has shown interest in cyanide, Botulinum toxin, *Salmonella typhi* (the causative agent of typhoid fever), and *Bacillus anthracis* (the causative agent of Anthrax). The documents in which these agents were identified indicated that Al Qaeda was developing plans to produce or acquire these agents. [reference: DHS Sector Notification 3-J076, 17 March 2003]. In addition, Al Qaeda discussed plans to hyperchlorinate treated water as another means of disrupting the drinking water supply.

With respect to physical attacks, Al Qaeda discussed attacks against critical components of the water infrastructure such as the primary and backup high service pumps. Even if such pumps are replaced within a week, a water system could be out of service during the replacement period. Cascading effects on other water-dependent sectors could also occur as mentioned above.

To: Mr. Michael E. Murphy Town of Addison (972) 450-2837

From: AWWA (303) 795-1989 06/23/03 07:35PM

Protective/Response Measures for Bio-Chemical Attacks

The normal US water treatment process has a number of built-in safeguards that would present challenges to any terrorist group aiming to create a mass contamination event. These safeguards include treatment with chlorine and other disinfectants, purification, dilution, and stringent quality control [reference: DHS Sector Notification 3-J076, 17 March 2003]. With respect to the four contaminants identified above, it is noted that all of these agents are threats to drinking water. Contamination of all or a portion of the distribution system or specifically targeting the water supply for high value targets such as a military base, government offices, schools, or hospitals is of particular concern. The following protective/response measures are recommended if such contaminants are found or suspected in the post-treatment water supply:

1. Unusual drops in residual disinfectant should always be investigated.

2. If a water contamination event is suspected, the credibility of the event must first be evaluated in order to determine appropriate response actions. This credibility assessment must be performed quickly and should be based on any information available about the event that is readily available or which can be quickly collected during a site investigation and rapid field testing of the water. Law enforcement can also provide assistance in making credibility determinations and may investigate the incident as a potential criminal or terrorist activity.

3. If a water contamination threat is determined to be credible, then response actions to protect public health will be necessary. Response actions might include isolation of affected areas of the system or more aggressive measures such as issuance of public notices to *not drink* or *not use* the water. Such public health decisions should be made in conjunction with appropriate government agencies, such as the state or local health departments. Furthermore, contingency plans must be in place to provide water to the public for consumption and to ensure that fire protection is maintained. In the case of a highly credible contamination threat, it is recommended that the local FBI field office and the National Response Center (NRC) be contacted in addition to the notifications made at the local and state levels. The NRC can quickly mobilize federal resources to provide assistance in the case of an emergency and can be reached on a 24 x 7 basis at 800-424-8802.

While it is important to take all contamination threats seriously and to conduct a thorough investigation to evaluate the credibility of the threat, it is equally important not to overreact to a potential threat because any response actions carry consequences of their own. EPA, in conjunction with experts from the drinking water treatment industry, is developing a more specific protocol to respond to contamination incidents that will expand upon the suggestions above and which should be available soon.

With regards to the particular contaminants mentioned above, the following information may be useful.

To: Mr. Michael E. Murphy Town of Addison (972) 450-2837

From: AWWA (303) 795-1989 06/23/03 07:35PM

- **Cyanide**—Cyanide is neutralized at low concentrations by chlorine residuals particularly at pH levels greater than 8.5. However, for high levels of cyanide, levels of chlorine much greater than those used in drinking water treatment are required to neutralize the cyanide. Cyanogen chloride, another toxic compound, is formed at low pH (< 8.5). EPA has approved standard methods and rapid detection kits for cyanide (see <http://www.epa.gov/ctv/verifications/vcenter1-23.htm>). If significant variations above the normal for cyanide are detected, immediately consult with public health officials to determine the actions that need to be taken, including the possible issuance of *no drink* or *no use* notices.
- **Botulinum Toxin, *Salmonella typhi***—These biological agents can be inactivated at levels greater than 90 percent by typical chlorine residual levels. *Salmonella typhi* can be cultured, and rapid test kits are available for this organism but have not been verified for drinking water applications. If there is an elevated threat of botulinum toxin or *Salmonella typhi* in the water system, residual chlorine levels may be increased. If chloramines are presently used as the disinfectant, consideration should be given to reverting to chlorine residual. If the presence of either of these agents is suspected, immediately consult with public health officials to determine the actions that need to be taken including the possible issuance of *no drink* notices.
- ***Bacillus anthracis***—*Bacillus anthracis* spores are not affected by normal chlorine residual levels. *Bacillus anthracis* can be cultured, and rapid test kits are available for this organism but have not been verified for drinking water applications. If *Bacillus anthracis* is suspected, immediately consult with public health officials to determine the actions that need to be taken, including the possible issuance of *no drink* or *no use* notices.

More information on test kits is available at the Association of Analytical Communities (AOAC) website --<http://www.aoac.org/testkits/TKDATA2.HTM>.

- **Hyperchlorination**—Normal water treatment quality control should detect hyperchlorination quickly. Because excess chlorine would be readily identifiable at levels that would lead to adverse health effects, most consumers would refuse to consume or use over-chlorinated water due to the pungent odor. Upon detection, a temporary 'no drink' order may need to be issued until the hyperchlorinated water has been flushed or purged from the system.

Further information may be found at these public web sites:

Centers for Disease Control Biological Agents:
<http://www.bt.cdc.gov/agent/agentlist.asp>

Centers for Disease Control Chemical Agents:
<http://www.bt.cdc.gov/agent/agentlistchem.asp>

To: Mr. Michael E. Murphy Town of Addison (972) 450-2837

From: AWWA (303) 795-1989 06/23/03 07:35PM

Protective Measures for Physical Attacks

Protective measures span the spectrum from prevention, detection of, response to, and recovery from physical attack. These measures are well known to the industry but warrant review in light of the potential threats cited here. A comprehensive listing of measures can be found in the EPA's document *Guarding Against Terrorist and Security Threats: Suggested Measures for Drinking Water and Wastewater Utilities* attached as a separate document to this advisory. Examples of such measures - to be adapted based on local conditions, needs, and available security resources - might include, but are not limited to, the following:

- Maintain and monitor disinfection residual throughout the distribution system
- Close monitoring, patrols, and video surveillance of critical water supply nodes and links from source through distribution
- Rapid communication of suspicious activity, including automated alarms, to local law enforcement authorities
- Well-tested and maintained emergency response plans that include responses by local, State, and the Federal government
- Tested and maintained protocols for quickly gaining approval and communicating 'boil water', 'no drink', or 'no use' orders to the public
- Well-tested and maintained recovery plans that include responses by neighboring water supply organizations, local, State, and the Federal agencies and private sector suppliers
- Review of security procedures with facility staff
- Requirements that employees change passwords periodically on critical management systems and that system administrators implement best security practices for information technology systems and networks

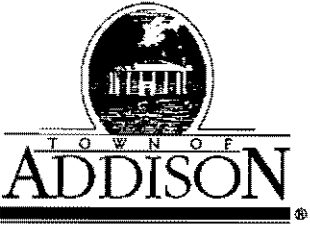
DHS encourages individuals to report information concerning suspicious or criminal activity to law enforcement or a Homeland Security watch office. Individuals may report incidents online at <http://www.nipc.gov/incident/cirr.html>, and Federal agencies/departments may report incidents online at <https://incidentreport.fedcirc.gov>.

Specific contact numbers for the LAIP watch centers are:

For private companies and citizens, 202-323-3205, 1-888-585-9078, or
nipc.watch@fbi.gov

For Federal agencies/departments, call 888-282-0870 or email fedcirc@fedcirc.gov

DHS intends to update this bulletin should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory Level (HSAS) is anticipated; the current HSAS level is **YELLOW**.



LETTER OF TRANSMITTAL

Public Works / Engineering
 16801 Westgrove • P.O. Box 9010
 Addison, Texas 75001
 Telephone: (972) 450-2871 • Fax: (972) 450-2837

DATE	5/20/03	JOB NO.
ATTENTION		
RE:	Vulnerability Assessment	

TO Matt Stevens
 Dal Tech

- GENTLEMAN:**
WE ARE SENDING YOU
- Attached
 - Under separate cover via _____ the following items:
 - Shop Drawings
 - Prints
 - Plans
 - Samples
 - Specifications
 - Copy of letter
 - Change order
 - _____

COPIES	DATE	NO.	DESCRIPTION
1			Baseline Threat Information for Vulnerability Assessments of Community Water Systems
			Document returned to Jeffrey 6-3-03
			<i>[Signature]</i>

- THESE ARE TRANSMITTED as checked below:**
- For approval
 - For your use
 - As requested
 - For review and comment
 - FOR BIDS DUE _____ 19____
 - Approved as submitted
 - Approved as noted
 - Returned for corrections
 - _____
 - Resubmit _____ copies for approval
 - Submit _____ copies for distribution
 - Return _____ corrected prints
 - _____
 - PRINTS RETURNED AFTER LOAN TO US

REMARKS Please do not make copies of this document. Return to Town of Addison when finished with the document. Please acknowledge receipt with signature below!

 Signature *[Signature]* 5/20/03

COPY TO Jerry Davis

SIGNED: *[Signature]*

If enclosures are not as noted, please notify us at once.

cc Mike
Jerry
Jef.



Threat Advisory

**U.S. Environmental Protection Agency
Office of Water
Water Protection Task Force
February 7, 2003**

EPA's Water Protection Task Force is providing the following information to water utilities to assist in their preparations for the newly announced Threat Level Orange:

- Suggested measures under Threat Level Orange
 - Joint EPA/CDC Advisory
-

SUGGESTED MEASURES UNDER THREAT LEVEL ORANGE

EPA's Water Protection Task Force has compiled a list of suggestions from a number of water utilities to assist in preparations at the various Homeland Security Threat Levels. The suggestions described below pertain to the Threat Level Orange and are organized in the areas of detection, preparedness, prevention, and protection. Water utilities should consider whether the following measures are appropriate for their facilities:

Suggested Measures

I. Detection:

- Confirm that county and state health officials will inform water utilities of any potential waterborne illnesses.

II. Preparedness:

- Post *daily* reminders for staff and contractors of the THREAT LEVEL ORANGE, along with a reminder of what events constitute security violations.
- Ensure employees are fully aware of the emergency response communication protocols so that appropriate notifications can be made quickly in the event of an incident. Consider the following list of organizations to be notified:
 - local law enforcement
 - local FBI Field Office
 - National Response Center (800-424-8802)
 - State and local emergency management organizations
 - Governor's office
 - EPA CID Special Agent in Charge (SAC)
 - other associated system authorities (wastewater, water)
 - local government officials
 - state/local health, water, and/or environmental departments
 - critical care facilities
 - employees
 - EMS and fire department as deemed necessary
 - Consider when to notify customers and what notification to issue

(Additional information is available in the *Model Emergency Response Guidelines* at www.epa.gov/safewater/security/)

- Evaluate the need for organizing an emergency operations center.

III. 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.

IV. Protection:

- Ensure water treatment/production facility is staffed at all times.
 - Consider the need for additional security measures needed for surface water reservoirs.
 - Limit mission critical facility access to essential employees and contractors.
 - Increase security patrol activity to the maximum level sustainable and ensure tight security in the vicinity of mission critical facilities. Consider varying the schedule of security patrols.
 - Prosecute intruders, trespassers, and those detained for tampering to the fullest extent possible under applicable laws.
-

Joint EPA/CDC Advisory

ADVISORY

FOR RELEASE February 7, 2003

Today, the Department of Homeland Security upgraded the Homeland Security Advisory System from yellow level (elevated risk of terrorist attack) to orange level (high risk of terrorist attack).

While there are no data to indicate that water has been specifically targeted, our nation's water infrastructure remains at risk to terrorist attacks, or acts intended to substantially disrupt the ability of a water system to provide a reliable supply of water. Therefore, public health agencies and water utilities are encouraged to continue to work together, keep each other informed of any unusual activities, and confirm the proper operation of notification channels in emergency response plans.

Public health agencies should immediately notify local water utilities and the state's drinking water administrator in the event of an unusual number of cases of gastrointestinal illnesses or other indications of illness that may suggest water contamination by a biological, chemical or radiological agent.

Water utilities should immediately notify public health agencies 24/7 emergency operations number, and the state's drinking water administrator in the event of specific threats received at a water facility, customer complaints in water quality, or if circumstances lead the utility to believe that the water has been or will be contaminated with a biological, chemical or radiological agent.

The Centers for Disease Control and Prevention (CDC) and the U.S. Environmental Protection Agency (EPA) issue this advisory jointly.

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 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. **Please do not post this document on publicly available web sites.**

CONDITION	CONSIDER ADOPTING THESE MEASURES	
<p style="text-align: center;">LOW (GREEN) Low Risk of Terrorist Attack</p> <p>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.)</p>	Detection	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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)	
<p>GUARDED (BLUE) General Risk of Terrorist Attacks</p> <p>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.</p>	Detection	<ul style="list-style-type: none"> ▪ Test security alarms and systems for reliability.
	Preparedness	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Control access to mission critical facilities.

CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
<p>ELEVATED (YELLOW) Significant Risk of Terrorist Attack</p> <p>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.</p>	<p>Detection</p>	<ul style="list-style-type: none"> ▪ 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.
	<p>Preparedness</p>	<ul style="list-style-type: none"> ▪ 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.
	<p>Prevention</p>	<ul style="list-style-type: none"> ▪ 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.
	<p>Protection</p>	<ul style="list-style-type: none"> ▪ 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)	
<p>HIGH (ORANGE) High Risk of Terrorist Attack</p> <p>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.</p>	Detection	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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.

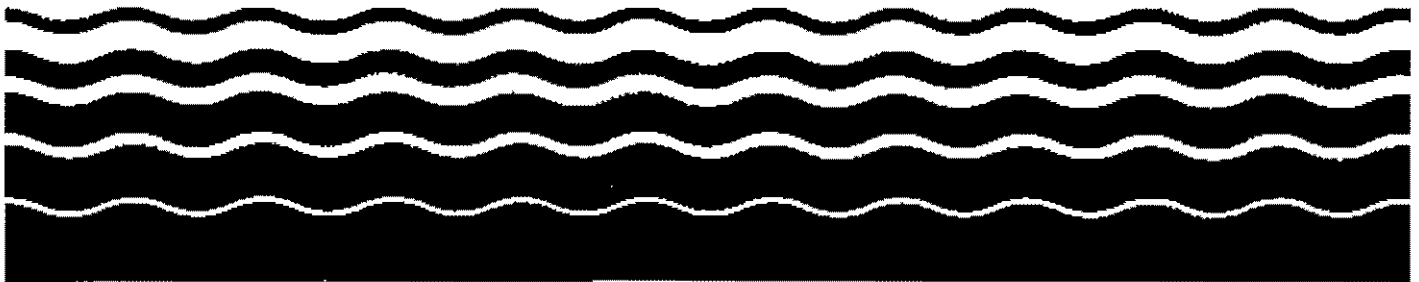
CONDITION	CONSIDER ADOPTING THESE MEASURES (and those at lower threat levels)	
<p>SEVERE (RED) Severe Risk of Terrorist Attack</p> <p>signifies a severe risk of terrorist attacks. Protective measures should focus on the decision to close specific facilities and the redirection of staff resources to critical operations.</p>	Detection	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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.

United States
Environmental Protection
Agency

Office of Water
Water Protection Task Force



Guidance for Water Utility Response, Recovery & Remediation Actions for Man-made and/or Technological Emergencies



DISCLAIMER

The statements in this document are intended solely as guidance. This document is not intended, nor can it be relied on, to create any rights enforceable by any party in litigation with the United States. EPA and state officials may decide to follow the guidance provided in this document, or to act in variance with the guidance, based upon an analysis of site-specific circumstances. This guidance may be revised without public notice to reflect subsequent changes in EPA's policy.

This document was prepared by Michael Baker Jr., Inc. for the EPA's Water Protection Task Force under contract EMW-2000-CO-0002.

Table of Contents

Introduction:	1
Background:	1
I. Incident types	1
II. Development of the Guidance	2
III. Structure	2
Response Planning:	2
Notification Considerations:	2
Sampling:	4
Annexes:	4
1. Sample Collection, Identification and Chain-of-Custody Form	Annex I-1
2. Incident-specific Guidance	
I. Contamination Event: (Articulated Threat with Unspecified Material)	Annex II- 1
II. Contamination Threat at a Major Event	Annex II- 3
III. Notification from Health Officials of Potential Water Contamination	Annex II- 5
IV. Intrusion through Supervisory Control and Data Acquisition (SCADA)	Annex II- 7
V. Significant Structural Damage Resulting from an Intentional Act	Annex II- 9

Introduction:

This document provides uniform response, recovery and remediation guidance for water utility actions in response to man-made and/or technological emergencies. The guidance was developed as an initiative of EPA's Water Protection Task Force and has been reviewed with water utilities and associations, EPA Regions, EPA Office of Water and other federal agencies. The intent of this guidance is to provide the minimum actions that EPA recommends be carried out by a water utility for the events described.

Emergency response planning is primarily a local responsibility. Good business practices suggest that every water utility have an Emergency Operations/Response Plan that is coordinated with state and local emergency response organizations, regulatory authorities and local government officials. Water utilities ought to consider whether the actions contained within this guidance have been thoroughly coordinated with these entities.

The Federal Response Plan (section VI) identifies Federal responsibilities and capabilities that can support the local response effort dependent upon the type and severity of the incident. Throughout this guidance "water system" includes the "system" elements of source water (ground and surface), drinking water treatment, drinking water distribution and storage, wastewater collection and wastewater treatment.

Background:

The Environmental Protection Agency (EPA) has been given the responsibility under Presidential Decision Directive (PDD) 63 for working with the Water Sector (including water and wastewater utilities) to provide for the protection of the nation's critical water infrastructure including the systems used to collect, treat and distribute potable water. The EPA has a similar responsibility for wastewater operations. These critical infrastructures are fundamental to the public health and welfare and are subject to both natural disasters such as floods and earthquakes, and man-made hazards such as terrorist attacks. Such disasters could place surrounding areas and populations at significant risk. In October, 2001 the EPA established an internal Water Protection Task Force to ensure that activities to protect and secure water supply infrastructure are comprehensive and carried out expeditiously. This guidance supports the Task Force's mission of providing information in an expeditious manner to public and private water utilities that can be used to protect public health and critical water infrastructure.

I. Incident types

This guidance was developed for five (5) different incident types:

- **Threat of or Actual Intentional Contamination of the Water System**
- **Threat of Contamination at a Major Event**
- **Notification from Health Officials of Potential Water Contamination**
- **Intrusion through the Supervisory Control and Data Acquisition (SCADA); and**
- **Significant Structural Damage Resulting from an Intentional Act**

While this guidance is oriented toward these 5 incident types, it should also serve as a guide for response, recovery and remediation actions for other threatened or actual intentional acts that would affect the safety or security of the water system..

II. Development of the Guidance

Each incident type was assessed for potential impact on water system operations and public safety to identify the minimum actions for each element of the water system to consider taking in response to the incident, recover from the incident and to remediate the impacts of the incident. Response refers to actions immediately following awareness of the incident, recovery refers to actions to bring the system back into operation, and remediation refers to longer term restoration actions. Where applicable, each incident type was assessed as if it had occurred separately at each of the system elements and the potential impacts were assessed upstream and downstream of the incident location. Additionally, the guidance was developed considering the response needs of large, medium and small water and wastewater systems. Water utilities should apply the concepts contained in the guidance to meet their system configuration and capabilities.

III. Structure:

The guidance provides recommended actions in the categories of Response Actions, Recovery Actions, and Remediation Actions in separate tables for each incident type. Each of these categories contain a section on notifications and utility actions. Where applicable, specific actions for each element of the water system are provided under the utility actions section.

The Notification Considerations section recommends standard notifications for any suspicious or threatened intentional man-made or technological emergency. Supplemental notifications are recommended within the incident tables for some events based on the potential impact of the event.

Response Planning:

This response, recovery and remediation guidance to intentional acts can be used to supplement existing water utility emergency operations plans (EOPs) developed to prepare for and respond to natural disasters and emergencies. EPA recommends that established policies and procedures contained in existing plans be used to the maximum extent while incorporating the recommendations in this guidance.

A high quality water utility EOP clearly delineates the organizational structure within the water system that will be responsible for incident response and management. This structure should identify specific individual roles and responsibilities for decision-making, logistics, operations, incident response control and finance. The structure could be based on the Incident Command System, or other similar system, that is compatible with the system(s) used by other elements (Fire, Law Enforcement, Emergency Management, Emergency Medical Services (EMS), etc.) of the community's incident response and management structure. It would be helpful to coordinate potential response requirements and expectations with local response organizations prior to an incident to ensure that the water utility's response needs are met.

Notification Considerations:

Water utilities that have established notification procedures to meet a regulatory requirement, such as the Emergency Planning and Community Right-to-Know Act (EPCRA), should use them as the starting point for developing broader notification procedures. Utilities that do not have established notification procedures should work with their Local Emergency Planning

Committee (LEPC) or similar local emergency planning organization, prior to an incident, to coordinate the specific procedures for contacting local, state and federal officials when an incident occurs. You can find the LEPC for your location at <http://www.epa.gov/ceppo/lepclist.htm>.

EPA expects that the facility would first call local law enforcement officials to initiate local emergency response actions. This may be accomplished by calling 911 or direct call to local law enforcement. The local notification coordination effort should determine which additional emergency response and management agencies (fire, Emergency Medical Services (EMS), the community emergency management organization and state agencies) need to be notified. For instance, do fire and EMS need to be notified in addition to law enforcement for a water-related incident?

The notification procedures developed within the local notification coordination effort should provide agency-specific names and contact numbers for these notifications on a 24-hour basis and define what information about the incident needs to be provided, who will make the notifications and which authorities are notified when a call is placed. As a minimum, these notification procedures should include protocols for notifying local and state health and environmental authorities, local critical care facilities (hospitals, dialysis centers, etc.) and others as identified in state and local requirements.

An intentional act to disrupt the operations of a water utility or to jeopardize public health is a criminal act. This creates the need for notifications to the appropriate FBI field office, National Response Center and other entities that may not normally be contacted in response to a natural disaster or emergency. Water utilities should work with the LEPC or similar organization, in conjunction with appropriate state offices, to verify how these additional notification requirements will be met and who has responsibility for the notifications.

The procedures developed within the local notification coordination effort should ensure that all of the entities listed below are notified, identify who the utility must contact to initiate the notifications and identify who within the organization should make the notifications. These organizations are not listed in any particular order of preference.

- Notify local law enforcement
- Notify local FBI Field Office (to begin the threat assessment process) Your local FBI field Office can be located by visiting <http://www.fbi.gov/contact/fo/info.htm> or in the front pages of your local telephone book
- Notify National Response Center 1-800-424-8802 (to notify pre-determined federal response agencies) for more information on NRC see <http://www.nrc.uscg.mil>
- Notify state/local emergency management organization
- Notify Governor's office
- Notify local EPA CID Special Agent in Charge (SAC)
- Notify other associated system authorities (wastewater, water)
- Notify local government official (responsible authority for the water utility)
- Notify state/local health, water and/or environmental department
- Notify critical care facilities
- Notify employees
- Notify EMS and Fire Department as deemed necessary
- Consider when to notify customers and what notification to issue

The recommendations provided in this guidance are supplemental to regulatory or other promulgated reporting requirements. Normal reporting/notification to state health and/or environmental agencies, or the EPA for states without approved state programs, will still be required when the impacts of an incident result in an inability to meet Water Quality or National Primary Drinking Water Standards or to meet CERCLA and/or EPCRA requirements.

Sampling:

The results of sample analysis after a threatened or actual contamination event can serve a critical role in determining response, recovery and remediation actions; assessing the potential impacts of the contaminant; and, providing data for eventual prosecution. Sampling requirements (quantity, type of sample container, environmental controls, type of sample, sample locations, etc.) can vary significantly depending upon the properties of the contaminant and where the contaminant was introduced into the system. This guidance provides recommendations for when sampling might be beneficial but can not provide specific sampling requirements for every potential contaminant.

It is important to ensure that sampling is conducted by trained personnel and that the safety of sampling and other personnel is fully considered while conducting sampling activities. The diversity of sampling capabilities and resources among large and small water utilities makes it difficult to establish standard requirements for all water utilities. Water utilities should work with their LEPC and appropriate local, state and federal agencies to develop procedures for obtaining requirements or recommendations on taking samples, sample control, sample distribution and use of sample analysis results on an event-by-event basis. The water utility's sampling capabilities and procedures for obtaining sampling recommendations should be contained within the utility's EOP.

In the event of an incident that is suspected or confirmed to be the result of an intentional act to disrupt the operations of a water utility or to jeopardize public health, law enforcement officials may also require/take additional samples for evidence preservation.

Annexes:

Annex I provides a Sample Collection, Identification and Chain-of-Custody Form and instructions for its use. The form is an example of the information needed for recording data on samples taken in response to an intentional act and for maintaining a record for chain-of-custody of the sample.

Annex II provides incident-specific response, recovery and remediation guidance for each of the five (5) incident types.

Annex I – Sample Collection, Identification and Chain-of-Custody Form

Sample Collection, Identification and Chain-of-Custody Form			
Sample ID # (Place ID Label Here)		Sample Date/Time	
Sample Description		Sample Location	
Comments			
Sampler Signature	Date/Time	Witness Signature	Date/Time
Print	Sample ID	Print	Location
1. Released by: Signature	Date/Time	Received by: Signature	Date/Time
Print	Sample ID	Print	Location
2. Released by: Signature	Date/Time	Received by: Signature	Date/Time
Print	Sample ID	Print	Location
3. Released by: Signature	Date/Time	Received by: Signature	Date/Time
Print	Sample ID	Print	Location
4. Released by: Signature	Date/Time	Received by: Signature	Date/Time
Print	Sample ID	Print	Location

Instructions for Sample Collection, Identification and Chain-of-Custody Form

Whether from an epidemiological or evidentiary standpoint, it is critically important that samples taken in response to an intentional act against a water system be taken in a systematic manner. Each sample collected should have a separate identifying number (Sample ID #) and the transfer of each sample should be documented. The Sample Collection, Identification and Chain-of-Custody Form provides a standardized format for annotating this information.

Sample Identification Number (Sample ID #)

Each sample should have separate identification number. A uniform system should be established for assigning sample identification numbers.

Sample Date/Time

Annotate the date and time that the sample was taken.

Sample Description

Describe the type of sample taken (water, sludge, sediment basin, etc.)

Sample Location

Annotate as specifically as possible where the sample was taken so that later samples can be taken (if necessary) from the exact same location.

Comments

Provide any additional comments that may assist in sample analysis (water temperature, humidity, how sample was taken or materials used to take sample, etc.).

Sampler Identification

The person taking the sample should sign his/her name in the **Signature** block, annotate the date/time of signature in the **Date/Time** block, print the sampler's name in the **Print** block and annotate the sample ID number from the **Sample ID#** block at the top of the form.

Witness Identification

The person witnessing the taking of the sample should sign his/her name in the **Signature** block, annotate the date/time of signature in the **Date/Time** block, print the sampler's name in the **Print** block and annotate the location of where the sample was taken from the **Sample Location** block at the top of the form.

Chain-of-Custody Tracking

A record of control for all samples should be maintained. Each person who releases control of the sample should maintain a copy of who the sample was released to. Persons who receive samples should verify the sample identification number **ON THE SAMPLE** before signing for receipt of the sample. The original copy of the form, with original signatures should remain with each sample until final disposition.

The person releasing the sample should sign his/her name in the **Signature** block, annotate the date/time of release in the **Date/Time** block, print the releaser's name in the **Print** block and annotate the sample ID number from the **Sample ID#** block at the top of the form.

The person receiving the sample should sign his/her name in the **Signature** block, annotate the date/time of receipt in the **Date/Time** block, print the receiver's name in the **Print** block and annotate the location where the sample was received in the **Location** block.

Other Considerations

Photographs

When possible a photograph should be taken of each collected sample at the sample location. Ideally, the photograph would show the completed sample ID label and security seals in-place. Photographs should be annotated or dated-stamped with the date and time that the photo was taken.



I. Contamination Event: (Articulated Threat with Unspecified Material)

Event Description: This event is based on the threat of intentional introduction of a contaminant into the water system (at any point within the system) without specification of the contaminant by the perpetrator.

Initial Notifications:	<ul style="list-style-type: none"> • Notify local Law Enforcement • Notify local FBI Field Office • Notify National Response Center 	<ul style="list-style-type: none"> • Notify local/state emergency management organization • Notify ISAC 	<ul style="list-style-type: none"> • Notify other associated system authorities (wastewater, water) • Notify local government official 	<ul style="list-style-type: none"> • Notify local/state health and/or environmental department • Notify critical care facilities 	<ul style="list-style-type: none"> • Notify employees • Consider when to notify customers and what notification to issue • Notify Governor
	Source Water	Drinking Water Treatment Facility	Water Distribution / Storage	Wastewater Collection System	Wastewater Treatment Facility
RESPONSE ACTIONS	<ul style="list-style-type: none"> • Increase sampling at or near system intakes • Consider whether to isolate the water source if possible 	<ul style="list-style-type: none"> • Preserve latest full battery background test as baseline • Increase sampling efforts • Consider whether to continue normal operations (if determination is made to reduce or stop water treatment – provide notification to customers/issue alerts) • Coordinate alternative water supply 	<ul style="list-style-type: none"> • Consider whether to isolate the water in the affected area if possible 	<ul style="list-style-type: none"> • Assess what to do with potentially contaminated water within the system based on contaminant, contaminant concentration, potential for system contamination, and ability to by-pass treatment plant. • If by-passed-notify local & appropriate state authorities, & downstream users. Increase monitoring of receiving stream. 	<ul style="list-style-type: none"> • Preserve latest full battery background test as baseline • Increase sampling efforts • Consider whether to continue normal operations (if determination is made to reduce or stop water treatment – provide notification to customers/issue alerts)



I. Contamination Event: (Articulated Threat with Unspecified Material)

RECOVERY ACTIONS	Recovery actions should begin once the contaminant is through the system.		
Recovery Notifications:	<ul style="list-style-type: none"> • Notify Customers • Notify Media • Notify ISAC 		
Appropriate Utility Elements:	<ul style="list-style-type: none"> • Sample appropriate system elements (storage tanks, filters, sediment basins, solids handling) to determine if residual contamination exists. 	<ul style="list-style-type: none"> • Flush system based on results of sampling • Monitor health of employees 	<ul style="list-style-type: none"> • Plan for appropriate disposition of personal protection equipment (PPE) and other equipment
REMEDIAL ACTIONS	<ul style="list-style-type: none"> • Based on sampling results – assess need to remediate storage tanks, filters, sediment basins, solids handling. 	<ul style="list-style-type: none"> • Plan for appropriate disposition of PPE and other equipment 	<ul style="list-style-type: none"> • If waste water treatment plant was by-passed – sample and establish monitoring regime for receiving stream and potential remediation based on sampling results.

Notes:

1. Response, recovery and remediation actions may be tailored to a specified (identified) material if the physical properties for the material are known.



II. Contamination Threat at a Major Event

Event Description: This event is based on the threat of, or actual, intentional introduction of a contaminant into the water system at a sports arena, convention center or similar facility.

- Initial Notifications:**
- Notify local Law Enforcement
 - Notify local FBI Field Office
 - Notify National Response Center
 - Notify ISAC
 - Notify local/state emergency management organization
 - Notify wastewater facility
 - Notify Governor
 - Notify other associated system authorities (wastewater, water)
 - Notify local government official
 - Notify local/state health and/or environmental department
 - Notify critical care facilities
 - Notify employees
 - Consider when to notify customers and what notification to issue

	Source Water	Drinking Water Treatment Facility	Water Distribution / Storage	Wastewater Collection System	Wastewater Treatment Facility
RESPONSE ACTIONS	<ul style="list-style-type: none"> • No recommended action to take 	<ul style="list-style-type: none"> • No recommended action to take 	<ul style="list-style-type: none"> • Coordinate isolation of water • Assist in plan for draining the contained water • Assist in developing a plan for sampling water for potential contamination based on threat notification • Provide alternate water source 	<ul style="list-style-type: none"> • Coordinate acceptance of isolated water • Monitor accepted water • Assist in plan for draining the contained water • Assist in developing a plan for sampling water for potential contamination based on threat notification 	



II. Contamination Threat at a Major Event

RECOVERY ACTIONS	Recovery actions should begin once the contaminant is through the system.		
Recovery Notifications:	<ul style="list-style-type: none"> • Notify customers in the area of the facility of actions to take • Notify customers in affected area once contaminant-free clean water is re-established • Notify down-stream users such as water suppliers, irrigators, electric generating plants, etc. 		
Water Distribution / Storage	<ul style="list-style-type: none"> • Consider flushing system via hydrants in distribution systems 		
REMEDIALTION ACTIONS:	Water Distribution/Storage	<ul style="list-style-type: none"> • Assess need to decontaminate/replace distribution system components. 	
	Wastewater Treatment Plant	<ul style="list-style-type: none"> • Based on sampling results – assess need to remediate storage tanks, filters, sediment basins, solids handling. 	<ul style="list-style-type: none"> • Plan for appropriate disposition of PPE and other equipment

Notes:



III. Notification from Health Officials of Potential Water Contamination

Event Description: This event is based on the water utility being notified by Public Health officials of potential contamination based on symptoms of patients.

Initial Notifications:	<ul style="list-style-type: none"> • Ask notifying official who else has been notified and request information on symptoms, potential contaminants and potential area affected • Notify local Law Enforcement • Notify local FBI Field Office • Notify National Response Center • Notify local/state emergency management organization • Notify other associated system authorities (wastewater, water) • Notify local government official • Notify Governor • Notify local/state health and/or environmental department • Notify critical care facilities • Notify employees • Consider when to notify customers and what notification to issue • Notify ISAC 				
	Source Water	Drinking Water Treatment Facility	Water Distribution / Storage	Wastewater Collection System	Wastewater Treatment Facility
RESPONSE ACTIONS	<ul style="list-style-type: none"> • Increase sampling at or near system intakes • Consider whether to isolate 	<ul style="list-style-type: none"> • Preserve latest full battery background test result as baseline • Increase sampling efforts • Consider whether to continue normal operations (if determination is to reduce or stop water treatment – provide notification to customers/issue alerts) • Coordinate alternative water supply (if needed) 	<ul style="list-style-type: none"> • Increase sampling in the area potentially affected and at locations where the contaminant could have migrated to. It is important to consider the time between exposure and onset of symptoms to select sampling sites • Consider whether to isolate • Consider whether to increase residual disinfectant levels 	<ul style="list-style-type: none"> • Increase sampling at pumps stations and specifically in the area potentially affected • Assess what to do with potentially contaminated water within the system based on contaminant, contaminant concentration, potential for system contamination, and ability to by-pass treatment plant • If by-passed – notify local & appropriate state authorities, downstream users (especially drinking water treatment facilities) & increase monitoring of receiving stream 	



III: Notification from Health Officials of Potential Water Contamination

RECOVERY ACTIONS	Recovery actions should begin once the contaminant is through the system.		
Recovery Notifications:	<ul style="list-style-type: none"> • Assist health department with notifications to customers, media, downstream users and other organizations 		
Appropriate Utility Elements:	<ul style="list-style-type: none"> • Sample appropriate system elements (storage tanks, filters, sediment basins, solids handling) to determine if residual contamination exists. 	<ul style="list-style-type: none"> • Flush system based on results of sampling • Monitor health of employees 	<ul style="list-style-type: none"> • Plan for appropriate disposition of personal protection equipment (PPE) and other equipment
REMEDATION ACTIONS	<ul style="list-style-type: none"> • Based on sampling results – assess need to remediate storage tanks, filters, sediment basins, solids handling and drinking water distribution system 	<ul style="list-style-type: none"> • Plan for appropriate disposition of PPE and other equipment 	<ul style="list-style-type: none"> • If waste water treatment plant was by-passed – sample and establish monitoring regime for receiving stream and potential remediation based on sampling results.

Notes: Patient symptoms should be used to narrow the list of potential contaminants.



IV. Intrusion through Supervisory Control and Data Acquisition (SCADA)

Event Description: This event is based on internal or external intrusion of the SCADA system to disrupt normal water system operations.

Initial Notifications:	<ul style="list-style-type: none"> • Notify local Law Enforcement • Notify local FBI Field Office 	<ul style="list-style-type: none"> • Notify National Infrastructure Protection Center (NIPC) at 1-888-585-9078 (or 202-323-3204/5/6) 	<ul style="list-style-type: none"> • Notify other associated system authorities (wastewater, water) • Notify employees 	<ul style="list-style-type: none"> • If the water is assessed to be unfit for consumption, consider when to notify customers and what notification to issue
-------------------------------	---	---	--	--

RESPONSE ACTIONS	Source Water	Drinking Water Treatment Facility	Water Distribution / Storage	Wastewater Collection System	Wastewater Treatment Facility
		<ul style="list-style-type: none"> • Increase sampling at or near system intakes • Consider whether to isolate 	<ul style="list-style-type: none"> • Preserve latest full battery background test as baseline • Increase sampling efforts • Temporarily shut down SCADA system and go to manual operation using established protocol • Consider whether to shut down system and provide alternate water 	<ul style="list-style-type: none"> • Monitor unmanned components (storage tanks & pumping stations) • Consider whether to isolate 	<ul style="list-style-type: none"> • Temporarily shut down SCADA system and go to manual operation using established protocol • Monitor unmanned components (pumping stations) – required only if wastewater SCADA system is compromised • If SCADA intrusion caused release of improperly treated water consider whether to continue normal operations (if determination is made to reduce or stop water treatment – provide notification to customers/issue alerts)



IV. Intrusion through Supervisory Control and Data Acquisition (SCADA)

RECOVERY ACTIONS	Recovery actions should begin once the intrusion has been eliminated and the contaminant/unsafe water (if this occurs) is through the system.		
Recovery Notifications:	<ul style="list-style-type: none"> • Employees • Local law enforcement • Notify customers and media if the event resulted in contamination and the full range (see scenario I) of standard notifications were made 		
Appropriate Utility Elements:	<ul style="list-style-type: none"> • With FBI assistance, make an image copy of all system logs to preserve evidence. 	<ul style="list-style-type: none"> • With FBI assistance, check for implanted backdoors and other malicious code and eliminate them before re-starting SCADA system 	<ul style="list-style-type: none"> • Install safeguards before re-starting SCADA • Bring SCADA system up and monitor system
REMEDIATION ACTIONS	<ul style="list-style-type: none"> • Assess/implement additional protections for SCADA system. • Check for an NIPC water sector warning based on the intrusion that may contain additional protective actions to be considered. NIPC warnings can be found at www.NIPC.gov or at https://www.infragard.org for secure access Infragard members. 		

Notes:



V. Significant Structural Damage Resulting from an Intentional Act

Event Description: This event is based on intentional structural damage to water system components to disrupt normal system operations.

<p>Initial Notifications:</p>	<ul style="list-style-type: none"> • Notify local Law Enforcement • Notify local FBI Field Office • Notify National Response Center 	<ul style="list-style-type: none"> • Notify local/state emergency management organization • Notify Governor • Notify ISAC 	<ul style="list-style-type: none"> • Notify other associated system authorities (wastewater, water) • Notify local government officials 	<ul style="list-style-type: none"> • Notify local/state health and/or environmental department • Notify critical care facilities 	<ul style="list-style-type: none"> • Notify employees • Consider when to notify customers and what notification to issue
<p>RESPONSE ACTIONS</p>	<p>Source Water</p>	<p>Drinking Water Treatment System</p>	<p>Water Distribution / Storage</p>	<p>Wastewater Collection System</p>	<p>Wastewater Treatment Facility</p>
<ul style="list-style-type: none"> • Deploy damage assessment teams, if damage appears to be intentional then treat as crime scene – Consult local/state law enforcement and FBI on evidence preservation • Inform law enforcement and FBI of potential hazardous materials • Coordinate alternate water supply, as needed • Consider increasing security measures • Based on extent of damage, consider alternate (interim) treatment schemes to maintain at least some level of treatment 					
<p>RECOVERY ACTIONS</p>	<p>Recovery actions should begin as soon as practical after damaged facility is isolated from the rest of the utility facilities.</p>				
<p>Recovery Notifications:</p>	<ul style="list-style-type: none"> • Employees • Law enforcement 		<ul style="list-style-type: none"> • Notify local FBI office 		
<p>Appropriate Utility Elements:</p>	<ul style="list-style-type: none"> • Dependent on the feedback from damage assessment teams 		<ul style="list-style-type: none"> • Implement damage recovery plan 		
<p>REMEDIATION ACTIONS</p>	<ul style="list-style-type: none"> • Repair damage. 		<ul style="list-style-type: none"> • Assess need for additional protection/security measures for damaged facility, and other critical facilities within the utility. 		

Notes:

Threat Identification Checklist

If your utility receives a threatening phone call, try to keep the caller on the line to obtain as much information as possible. Record as much information as possible, including:

1. What kind of threat is posed?
 - A. Contamination: What kind of poison? _____
How much? _____
 - B. Physical Damage: What kind of damage? _____
With what kind of device? _____
2. Where? _____
3. When? _____
4. Why? _____
5. By whom? _____
6. What is your (caller's) name? _____
7. What is your (caller's) affiliation, if any? _____
8. What is your (caller's) address/phone #? _____
9. What is the exact wording of the threat? _____

10. Is the caller male female well spoken illiterate foul irrational incoherent
11. Is the caller's voice calm angry slow rapid soft loud laughing crying
 normal slurred nasal clear lisping stuttering deep high
 cracking excited young old
 familiar - who did it sound like? _____
 accented - what nationality, region? _____
12. Is the connection clear? (Could it have been a wireless or cell phone?)
13. Are there background noises? street noises - what kind? _____
 machinery - what type? _____
 voices - describe _____
 children - describe _____
 animals- what kind? _____
 computer keyboard/office
 motors - describe _____
 music - what kind? _____
 other _____

Name of person receiving call _____ Date _____ Time _____

Notify Utility manager _____ phone: _____

Local FBI/Law Enforcement, Phone _____

Other _____ phone: _____

**Texas Natural Resource Conservation
Commission**

**Public Drinking Water System
Security Evaluation Plan
and
Emergency Response Plan**

**Texas Natural Resource Conservation Commission
Public Water System**

Security Evaluation Plan

KNOW YOUR WATER SYSTEM

- Physically locate and inventory all water system facilities.
- Tour your watershed and wellhead protection areas to identify any changes that might have occurred that would make your source more vulnerable to contamination.
- Visit and inspect surface water intakes routinely.
- Review and update distribution maps. Access to these maps should be restricted, but readily available to authorized personnel. Emphasis should be placed on the location of all valves including isolation valves, flush valves, air release valves, and fire hydrants.
- Please note that you should continue to operate your system according to TNRCC rules and regulations.

BE PREPARED

- Make sure all employees are aware of how to communicate in case of an emergency. Maintain an up to date list of emergency contacts including local law enforcement, fire, local EMS and the TNRCC (TNRCC phone numbers are attached). Provide these groups your emergency call list.
- Develop emergency plan and procedures and update at least annually.
- Develop a list of all other public water systems and their contacts that you serve or that serve you.
- Make sure key utility personnel (both on and off duty) have access to crucial telephone numbers and contact information at all times.
- Review your emergency evacuation plan and post it in a prominent location. This is particularly important for systems that utilize chlorine gas, chlorine dioxide, ammonia or any other hazardous or incompatible chemicals that could threaten public health or the environment if released.
- Keep an adequate supply of chemicals and repair parts on hand. Locate sources of equipment supplies such as pipe, emergency generators, repair clamps, dirt-moving equipment and maintain and update these lists periodically.
- Assemble a list of contacts for major repair services so they can be accessed quickly in case of an emergency. Maintain and update these lists periodically.
- Be sure staff is properly trained in how to take a bacteriological sample (correct procedures and sterile containers).
- Identify and contact an alternate source of water supply, and determine the distance and what equipment and supplies would be needed to make interconnection.

- Keep finished water storage levels maximized for interruptions, fire fighting and other emergencies.
- Service and exercise emergency generating equipment regularly to assure it is operational.

RESTRICT ACCESS TO YOUR WATER SYSTEM FACILITIES

- Reduce access points to water system facilities to as few as possible.
- Check that boat ramps are at least 1,000 feet from surface water intakes.
- Review facilities and maintain a list of staff that have access to the facilities. If you cannot account for all keys, you should consider re-keying or replacing locks.
- Issue specific badges and special visitors badges. All visitors should sign in and sign out and return visitor badges when leaving the site.
- Restrict all water system facilities to authorized personnel only. Post "Employee Only" signs in at all water system facilities.
- Lock all doors and set alarms at your office, pump houses, treatment plants, and vaults, and make it a rule that doors remain locked and alarms set at night and when unattended.

MONITOR YOUR FACILITIES

- Make sure that local law enforcement knows where all of your system facilities are located and ask that they include them in their patrols. Take time to explain to local law enforcement what is there and why it is important.
- Ask staff and the public to be vigilant and report any suspicious activities around water system facilities immediately to local law enforcement.
- Institute an ongoing testing program for all alarm and lock-up systems.
- Make more frequent visits to unmanned remote water facilities to assure that existing security measure have not been compromised.
- Check areas that have previously suffered damage due to vandalism as they may warrant additional security measures.
- Maintain a weekly inventory of all potentially hazardous chemicals. Verify that consumption and inventory equal the prior weeks total and any additional quantities purchased during the week. Notify local law enforcement of any missing potential hazardous chemicals.
- Remove meters or ensure that corporation stops are locked at inactive service connections.

- DRAFT**
- Increase chlorine monitoring and look for decreases in chlorine residual. If needed, increase chlorine levels in the distribution system.
 - Routinely check pressure in the distribution system and be aware of and respond to unusual changes in pressure (high or low). If pressure falls below 20 psi, report to the TNRCC and follow the flowchart in the appendix of the *Rules and Regulations for Public Water Systems*.
 - Check the distribution lines frequently for visible leaks, ask customers to report suspected leaks or breaks, and repair them as soon as possible.

SECURE YOUR FACILITIES and CHEMICALS

- Secure hatches, meter boxes, hydrants, manholes and other access points to the water distribution system;
- Make sure pumphouses, water storage tanks, treatment plants, and chemical storage facilities are secure, well lighted, locked and provided with alarms if possible. Alarms should sound locally and remotely to notify water system personnel and also security monitoring services, if available.
- Identify and inventory chlorine gas, chlorine dioxide, ammonia and any other hazardous or incompatible chemicals that could threaten human health or the environment.
- Seclude and secure dangerous chemicals. Avoid storing chemicals near the perimeter of the facility where someone who breaches your outer barrier (fence, gate, well house, etc.) could reach them more easily and quickly.
- Secure control access to computer networks and control systems, and change the passwords frequently.
- Protect all SCADA (Supervisory Control and Data Acquisition) sensing devices on equipment, especially offsite, from tampering by locked metal circuit boxes, metal conduit over open wiring, etc.
- Do not leave keys in equipment or vehicles at any time.

PLAN ON HOW TO COMMUNICATE

with your customers
with your neighboring water systems
with local law enforcement
with TNRCC

- Prepare a communications plan to deal with potential threats, infrastructure damage, and suspected or actual contamination incidents in advance. We have enclosed a checklist to assist you in handling threatening phone calls.
- Depending on the size of the water system, consider a 'communications command post' approach to centralize all public notices and press releases.

- Always alert local law enforcement to potential problems immediately - help them help you!
- Good customer relations is important. Make sure you do the following:
 - Involve the public.
 - Make your customers part of the process and your plans.
 - Give your customers the correct information as soon as possible through meetings, newspapers and newsletters, local radio, and television.
 - ***Keep it honest, keep it simple, and keep it consistent.***
 - Keep a list of phone contacts who can provide information or service to your customers in the event of a major water system failure.
 - Decide who will be your contact with the media, and make sure they have the latest, most accurate information.
 - Make sure your employees know when to direct inquiries to your media contact.

For more information you can visit the following web sites:

EPA Counterterrorism: <http://www.epa.gov/ebtpages/ecounterterrorism.html>

EPA Alert on Chemical Accident Prevention and Site Security:

<http://www.epa.gov/ceppo/pubs/secale.pdf>

U.S. Centers for Disease Control & Prevention: <http://www.bt.cdc.gov>

Association of Metropolitan Water Agencies: <http://www.amwa.net/isac/amwacip.html>

American Water Works Association: <http://awwa.org>

National League of Cities: http://www.nlc.org/nlc_org/site/newsroom/terrorism_response

Texas Natural Resource Conservation Commission Public Water System Emergency Response Plan

- Immediately report the following to local law enforcement:

- criminal threats
 - suspicious behavior
 - attacks on water facilities
 - suspicious containers
 - suspicious concentrated materials (such as powder or liquids)
 - breaches of your security systems
-
- If you have evidence of **suspicious containers or materials**, remove water system personnel from immediate area. Notify local law enforcement and hazardous materials response teams emergency response need to get updates from the personnel. If tanks or pumps can be removed from service without causing pressure problems, it would be advisable to do so until law enforcement has made a determination of the validity of the threat.
 - Once law enforcement has determined there is a credible threat, **notify the TNRCC Public Drinking Water Section and Regional Office** (numbers provided in attachments). TNRCC will provide appropriate support and additional support.
 - Report to TNRCC and county or State health officials any illness among the utility's customers that may be associated with water supplies.
 - Report any *unusual or out of the ordinary* drinking water problems or characteristics (taste, odor, color, drop in chlorine residual, emulsion, changes in conductivity, low or high pressure, high turbidity) to local law enforcement and TNRCC.
 - Contact your appropriate water system management and officials regarding the incident.
 - Notify EMS if operational staff have sustained injury or illness.
 - Call appropriate personnel listed on Emergency Contact phone list.
 - Isolate affected area if possible.
 - If loss of power, bring emergency power or alternate sources online as soon as possible.
 - Don't panic. Utilize all available resources.
 - Document date, time and decisions and actions taken.
 - Cooperate fully with local, state and federal authorities.

GUIDANCE FOR THREATENING CALLS

When you receive such a call, stay calm. Every effort should be made to **NOTE THE EXACT TIME OF THE CALL AND THE EXACT WORDS OF THE PERSON MAKING THE CALL**. Additional efforts should be made to determine the following details, if not already provided by the caller:

TORTION OR TAMPERING THREAT
at facility is being threatened?

DRAFT

What is the nature of the threat?

When is the threat to occur or has tampering already occurred?

What does the caller want?

Will the caller call back?

If not, who else will be called?

What is the caller's name, address and/or location?

What telephone number did the caller call and from what number?

BOMB THREAT

When is the bomb going to explode?

Where is it right now?

What does it look like?

What kind of bomb is it?

What will cause it to explode?

Where has the bomb been placed? Why?

What will it damage?

What is your address?

What is your name?

REPORT IMMEDIATELY AFTER THE CALL while information is still fresh on your mind. Note whether the caller male/female, had an accent or other speech characteristic, and the time the caller hung up. The following checklist may be helpful gathering information regarding the call. **INFORM LOCAL LAW ENFORCEMENT OFFICIALS IMMEDIATELY AND PREPARE A BRIEF WRITTEN REPORT.**

CHECK LIST TO NOTE ON CALLS:

CALLER'S VOICE:

_____ Calm
_____ Angry
_____ Excited

_____ Slow
_____ Rapid
_____ Soft

_____ Loud
_____ Laughter
_____ Crying
_____ Normal
_____ Distinct
_____ Slurred
_____ Whispered

_____ Nasal
_____ Stutter
_____ Lisp
_____ Raspy
_____ Deep
_____ Ragged
_____ Clearing Throat
_____ Deep Breathing
_____ Cracked Voice
_____ Disguised
_____ Accent
_____ Familiar

IF VOICE IS FAMILIAR, WHO DID IT SOUND LIKE?

BACKGROUND SOUNDS:

_____ Street Noises
_____ Kitchen Sounds
_____ Voices
_____ PA Systems
_____ Music
_____ House Noises
_____ Booth
_____ Office Machinery

_____ Factory Machinery
_____ Animal Noises
_____ Clear
_____ Static
_____ Long Distance
_____ Local
_____ Motor
_____ Cell Phone
_____ Other

THREAT LANGUAGE:







_____ Well Spoken (articulate)
_____ Foul
_____ Irrational

_____ Incoherent
_____ Taped
_____ Message read by threat maker

**IF ANY SUCH CALLS ARE RECEIVED ON A TELEPHONE ANSWERING DEVICE,
DO NOT ERASE THE TAPE, SINCE IT MAY BECOME EVIDENCE IN AN INVESTIGATION.**

Jim Pierce

From: Grover.Greg@epamail.epa.gov
Sent: Friday, January 24, 2003 2:55 PM
To: jpierce@ci.addison.tx.us
Subject: Security Effort Information

 020920Aug Rpt
access letter 2....
 001112plans1030.d
oc
 5 Emergency
Contact list.doc
 6Threat
Identification Checkli
 7 water
stewater incident
 8
ergencyResponseGui

Jim,

Thank you for your call! Access information for the Baseline Threat Document is attached below. At this time I am told that we need to follow non-internet access instructions.

(See attached file: 020920Aug Rpt access letter 2.wpd)

The latest information on vulnerability assessment tools and other EPA security effort information is located at our main website at:
<http://www.epa.gov/safewater/security>.

We are aware of the following VA requirements and/or potential sources of financial assistance for public water suppliers:
PL 107-188, known as the "Bioterrorism Act," has recently been signed into law. It requires VAs for all community water systems which serve more than 3,300 people. It also authorizes \$160 million for USEPA to use in assisting public water systems in conducting vulnerability assessments (VA), preparing emergency response plans, initiating basic security enhancements, and alleviating urgent vulnerabilities. However, the money has not yet been allocated. Should money be allocated (available), the funding vehicles and mechanisms for distribution, including the application process will be well-defined and publicized. The VA methodology will require the 6 basic elements outlined in the Baseline Threat Document. The complete text of the Act is located on our web site.

Until grants become available, States may provide drinking water state revolving funds (DWSRF) or other assistance to public water systems to allow them to complete VAs, emergency response plans, and many types of infrastructure improvements. Drinking water source protection may also be funded through DWSRF set-asides. Ultimately, it is the state's decision whether they can or will provide assistance. More information about the DWSRF and eligible activities is available at our web site located at:
<http://www.epa.gov/safewater/dwsrf/security-fs.pdf>.

Here is some emergency response plan guidance I promised you:
The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (BT Act) includes the following language which addresses Emergency Response Plan (ERP) requirements:

The emergency response plan shall include, but not be limited to, plans, procedures, and identification of equipment that can be implemented or utilized in the event of a terrorist or other intentional attack on the public water system. The emergency response plan shall also 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. Community water systems shall, to the extent possible, coordinate 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 or revising an emergency response plan under this subsection. Each community water system serving a population greater than 3,300 shall prepare or revise, where necessary, an emergency response plan that incorporates the results of vulnerability assessments that have been completed. Each such community water system shall certify to the Administrator, as soon as reasonably possible after the enactment of this section, but not later than 6 months after the completion of the vulnerability assessment under subsection (a), that the system has completed such plan.

The Large Water System Security Grant requires that the emergency operations plan (EOP) be a guide for water Utilities upon which actions and decisions can be based to govern the immediate response to an emergency, including how a Utility will remedy the problems caused by the emergency and recover from it. The intent of the EOP is to identify certain responsibilities delegated to various teams and employees, present details of notification procedures, and describe alternate measures and response actions. The EOP is not intended to be inclusive for each situation or problem that arises, and it should be updated periodically for continued relevance and viability. It must also comply with applicable state and local ordinances.

In addition to EPA's Model Emergency Response Guidelines which is attached and can also be located at the EPA's web site listed below, a number of major water system organizations, such as the American Water Works Association (AWWA), are offering emergency response plan (ERP) guidance which includes electronic templates. One AWWA product that we are aware of is Emergency Planning for Water Utilities (AWWA Manual M19). Their web site is: <http://www.awwa.org>.

We have attached additional EPA Region 6 and State of Texas (Nov. 2001) emergency response checklists/guidance for your information.

Essential for any emergency response plan is a proper incident notification sequence in the event of a potentially malevolent act against a facility. We recommend the following notification sequence:

1. Your local emergency responder (usually 911).
2. The EPA National Emergency Response Center: 1-800-424-8802.
3. Your State Drinking Water Agency (emergency number): Texas Commission on Environmental Quality, 1-800-832-8224.

Security checklist/emergency response templates have also been posted at our EPA Region 6 website at:
<http://www.epa.gov/earthlr6/6wq/swp/security/index.htm>.

Security Contacts:

For EPA Wastewater security efforts and guidance, please call Mike Tillman at 214-665-7531. The Texas Commission on Environmental Quality drinking water security contact is Tony Bennett at 512-239-6029.

Jim, I hope this information helps. Please let us know how we may further assist you.

I'll talk with you soon,
Greg

Greg Grover
Drinking Water Security Coordinator
EPA Region 6
Dallas, TX
214-665-2776

(See attached file: 001112plans1030.doc) (See attached file: 5 Emergency Contact list.doc) (See attached file: 6Threat Identification Checklist.wpd) (See attached file: 7 water wastewater incident report.wpd) (See attached file: 8

The national organizations are part of the Local Officials for Transportation (LOT) coalition, formed to develop and advocate policy recommendations for reauthorization. At a news conference in Washington, DC, Tarrant County Commissioner Glen Whitley, Fort Worth Mayor Kenneth L. Barr and Dallas Councilmember Sandy Greyson said that increased investment is needed to improve safety and combat congestion. The three elected officials said that the coalition's goals also entail protecting the strong gains of TEA-21, including maintaining its funding firewalls; increasing the role of local officials in planning transportation projects and funding decisions by sub-allocating resources to the regional level. The news conference was held February 10, 2003.

Coalition members include: NACo, NLC, USCM, APWA, the National Association of County Engineers, the Association of Metropolitan Planning Organizations, National Association of Regional Councils, National Association of Development Organizations, International City/County Management Association, National Association of City Transportation Officials and Public Technology, Inc.

Pipeline Safety

RULE TO REQUIRE INTEGRITY MANAGEMENT IN HIGH CONSEQUENCE AREAS

The US Department of Transportation's Research and Special Programs/Office of Pipeline Safety (RSPA/OPS) has issued a notice of proposed rulemaking to require operators to develop integrity management programs for gas transmission pipelines that, in the event of a failure, could impact high consequence areas (HCAs). The notice was published January 28, 2003 in the *Federal Register*. The deadline to submit comments is March 31, 2003.

For more information contact Mike Israni at 202-366-4571, or mike.israni@rspa.dot.gov. General information about the RSPA/OPS programs may be obtained by accessing RSPA's internet page at <http://RSPA.dot.gov>.

Roadway Safety

BILL WOULD PROVIDE \$3 BILLION ANNUALLY FOR ROAD SAFETY INFRASTRUCTURE

Representative Jay Inslee (D-WA) has introduced legislation to provide \$3 billion annually to fund the Roadway Safety and Congestion Mitigation Improvements Act, HR 288. It would target \$2.55 billion to specific risks, such as intersections, run off the road crashes, pedestrian and bicycle safety and work zones, and would provide \$300 million for safety improvements on roads off of the federal-aid highway system.

Design-Build Contracting

FHWA ISSUES FINAL RULE FULFILLING TEA-21 REQUIREMENT

The Federal Highway Administration has issued a final rule which implements regulations to allow design-build contracting as mandated by the Transportation Equity Act for the 21st Century (TEA-21). The regulation does not require the use of design-build contracting, but allows state DOTs to use it as an optional technique in addition to traditional contracting methods. Effective January 9, 2003, the final regulations list the criteria and procedures that will be used by FHWA in approving the use of design-build contracting by state transportation departments.

For more information contact FHWA's Gerald Yakowenko, 202-366-1562, or, for legal information, contact Harold Aikens, 202-366-1373.

Highway Environmental Review

QUESTION/ANSWER GUIDANCE ON INDIRECT AND CUMULATIVE EFFECTS ISSUED

Interim guidance, presented as a question and answer document, on considering indirect and cumulative effects of transportation projects as part of the environmental review process was issued by FHWA January 31, 2003. Twelve questions are addressed which cover definitions of "direct, secondary, indirect and cumulative effects and impacts. The guidance also provides resources including state transportation agency procedures and training opportunities. *For the guidance text go to <http://nepa.fhwa.dot.gov/RENepa/ReNepa.nsf/home> and click the cumulativ/direct impacts tab.*

Road Weather Management

NEW WEBSITE TO HELP WITH ADVERSE WEATHER RESPONSE

The Federal Highway Administration's new Road Weather Management website offers tools, resources and information to assist in managing weather-caused road problems. *The web address is: www.ops.fhwa.dot.gov/weather/index.htm.*

ENVIRONMENT

FY04 US EPA Budget

PROPOSED BUDGET WOULD CUT FUNDING FOR CLEAN WATER INFRASTRUCTURE

President Bush has proposed a 2004 fiscal year budget for the US Environmental Protection Agency (US EPA) at \$7.63 billion, a decline from \$7.7 billion the Administration sought in FY03 for which a request is still pending in Congress. EPA received \$7.9 billion in fiscal 2002. The biggest cut would be to the clean water state revolving fund. US EPA

Administrator Whitman said the agency would see an increase of about \$280 million to about \$4.25 billion for its core operating programs, an increase from the \$4.1 billion requested in FY03. The core programs refer to the Agency's priorities for the year-- clean air, clean and safe water, land and enforcement activities. Specific allocations include:

- \$7.7 million for the President's Clean Air program- a plan to eliminate emissions of sulfur dioxide, nitrogen oxides, and mercury from power plants by 70 percent, named EPA's top priority;
- \$850 million for Clean Water State Revolving Loan Fund, down about \$360 million from the FY03 request;
- \$850 million for Drinking Water State Revolving Loan, same as FY03 request;
- EPA will extend its commitment to the Clean Water program from 2005 to 2011, boosting the amount of money in the SRF by about \$800 million to \$2.8 billion in coming years;
- \$200 million for Clean Water Section 106 grants, an increase from FY03 request of \$180 million;
- \$238 million for nonpoint source funding under Section 319 of the Clean Water Act;
- \$20 million for watershed program, an increase of \$15 million from the FY03 request;
- \$210 million for the Brownfields program; an increase of \$10 million from the amount requested in FY03;
- \$21 million for enforcement funding;
- \$3.12 billion for state and tribal grants for FY04.

For further EPA budget information go to <http://www.epa.gov/ocfo/budget/2004/2004bib.pdf>

Water Security

EPA RELEASES SECURITY PROTOCOLS FOR VULNERABILITY ASSESSMENTS

US EPA has developed the *Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA*. The document is a list of strict measures developed to ensure the security of vulnerability assessments that drinking water utilities must submit to the agency under a new bioterrorism law. The protocol includes keeping assessments under lock and key and only attainable by individuals designated by the Administrator.

The Protocol was required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, signed by the President on June 12, 2003. Title IV of the law amends the Safe Drinking Water Act to require all utilities serving more than 3,300 people to assess the vulnerability of their systems to terrorism and other harmful acts and submit their assessments to the US EPA. Six months later, utilities are required to prepare emergency response plans.

Water Security Information

WATER INFORMATION AND ANALYSIS CENTER LAUNCHED

The Water Information Sharing and Analysis Center, or WaterISAC, has been launched to provide centralized security information and terrorist threat alerts to America's drinking water and wastewater utilities. All U.S. drinking water and wastewater systems are eligible to subscribe to the WaterISAC.

The WaterISAC was developed by utility managers for utility managers through Presidential direction and Executive Order 13231. A secure Web-based environment, the WaterISAC specific products and services include:

- Alerts on potential terrorist activity.
- Information on water security
- Databases of chemical, biological and radiological agents.
- Notification of cyber vulnerabilities and technical fixes.
- Vulnerability assessment tools and resources.
- Secure electronic bulletin boards and chat rooms on security topics.

Analysts for the WaterISAC have government security clearances and operate under strict protocols. The computer servers for the WaterISAC's secure portal reside in a protected, government-approved facility. *Information on subscribing to the WaterISAC is available online at www.WaterISAC.org.*

Water Pollution

US EPA PROPOSES TO WITHDRAW MAJOR CHANGES TO TMDL

The U.S. Environmental Protection Agency (EPA) has announced it is proposing to withdraw the July 2000 final rule which revised EPA's Total Maximum Daily Load (TMDL) program under the Clean Water Act. EPA has claimed the rule to be "unworkable." and its schedules for completing plans, requirement of implementation plans and emphasis on nonpoint sources of pollution were problematic for agriculture, state and environmental interests. The proposal to remove the 2000 TMDL rule is expected to generate comments from environmental groups who supported it.

Implementation of the 2000 TMDL rule was barred by Congress. The Bush Administration pulled the rule back for 18 months and considered significant changes. Proposed December 20, 2002, the withdrawal rule must become final before April or the 2000 regulation will become effective. The current TMDL program continues to function.



PUBLIC WORKS DEPARTMENT

(972) 450-2871

Post Office Box 9010 Addison, Texas 75001-9010

16801 Westgrove

VIA Fax 202-785-1845

February 18, 2003

US Environmental Protection Agency
Washington, D.C.

Attention: G. Tracy Mehan, III, Assistant Administrator

Gentlemen:

This is to request a copy of *Baseline Threat Information for Vulnerability Assessments of Community Water Systems*.

I have Internet access and my E-mail address is jpierce@ci.addison.tx.us

Thank you for your attention to this matter.

Very truly yours,

Town of Addison

James C. Pierce, Jr., P.E.
Assistant Public Works Director
Community Water System Manager

cc: Chris Terry, Assistant City Manager
Michael E. Murphy, P.E., Director of Public Works

Attachment

Attachment

Directions to Access the Document

Baseline Threat Information for Vulnerability Assessments of Community Water Systems

Provide the following information on the individual designated to access the document. Follow directions below.

Name (printed): James C. Pierce, Jr
Name (signature): James C. Pierce, Jr
Title: Asst. Public Works Director, Water System Manager
Organization: Town of Addison, Texas
Phone: 972-450-2879
E-mail: jpierce@ci.addison.tx.us
Public Water System Identification # TX0570031
(PWS ID)

If You Have Internet Access

- Fax your request for the document on your organization's letterhead stationery along with this page with requested information. *The letter should be signed by the community water system manager.* The fax number is: 202-785-1845.
- The designee will receive an encrypted E-mail reply with unique password and user identification. You will also receive an access code to open the document in Adobe Acrobat Reader. Please take all reasonable precautions to protect this information.
- Once you have received your username and password by E-mail, go to the Web site: <http://www.waterisac.org/EPAdocument.asp> and log-in. Follow directions on the web site to access the document. You may download a copy of Adobe Acrobat Reader from the WaterISAC web site to open the document.
- For technical assistance in accessing the document, E-mail your question to: info@waterisac.org or call: 866-h2o-ISAC (426-4722). For questions about the content of the document, E-mail Brian Frazer with EPA's Water Protection Task Force at, frazer.brian@epa.gov.

If You DO NOT Have Internet Access

Fax or mail your request for the document on your organization's letterhead stationery along with this page with requested information. *The letter should be signed by the community water system manager.* The fax number is 202-564-8513. The express mail delivery address is: Environmental Protection Agency, Attn: Documents, Room 2104A EPA East, 1201 Constitution Ave. NW, Washington DC, 20004. *If you send the letter by U.S. Postal Service there will be a significant delay.* You will receive the document by registered U.S. mail.

HP LaserJet 3200se



TOWN OF ADDISON
9724502837
FEB-18-2003 17:32

Fax Call Report

Job	Date	Time	Type	Identification	Duration	Pages	Result
16	2/18/2003	17:31:14	Send	912027851845	0:42	2	OK



PUBLIC WORKS DEPARTMENT
Fax Office 361 0010 Addison, Texas 75001-4010

(972) 450-2837
10801 Wargrove

Via Fax 202-785-1845

February 18, 2003

US Environmental Protection Agency
Washington, D.C.

Attention: G. Tracy Mehan, III, Assistant Administrator

Gentlemen:

This is to request a copy of *Baseline Threat Information for Vulnerability Assessments of Community Water Systems*.

I have Internet access and my E-mail address is jpierce@ci.addison.tx.us

Thank you for your attention to this matter.

Very truly yours,

Town of Addison

James C. Pierce, Jr., P.E.
Assistant Public Works Director
Community Water System Manager

cc: Chris Terry, Assistant City Manager
Michael E. Murphy, P.E., Director of Public Works

Attachment

Water/Wastewater System Incident Checklist

**NOTE: All emergencies should first be reported to 911
then to EPA's National Response Center at
1-800-424-8802**

1. Nature of Incident (explain):					
Contamination	Cyber attack	Brief description of incident:			
Biological	Bombs, explosives, etc.				
Chemical	Wastewater treatment plant Interference and/or pass through				
Radiological	Other (explain)				
Physical Destruction					
2. System Name		3. Party Responsible for Incident (Name and Address)			
Address:					
Telephone:					
System Contact Name:					
Title:					
4. Location of Incident					
Raw Water Source	Water Treatment Plant	Water Storage Facilities	Distribution Line	Receiving Stream	
Other (explain):			Wastewater Collection and/or Treatment System		
5. Date and Time of Incident					
6. Alternate Water Source Exists: Yes / No If yes, give name, type and location:					
7. Type(s) of Contaminants, Source and Quantity:					
Basis of Information:					
8. Caller's Name, Address, Organization and Telephone Number					
9. Was an emergency crew dispatched (911 called)?					
Yes	No	911	National Response Center	Regional Response Center	other
10. Which of the following are on scene:					

Police	Fire	Ambulance	FBI	Other
Hazardous Materials Team	FEMA	EPA	State Agency (describe)	
Weather conditions at incident site:				
Number and types of injuries and/or fatalities (if any):				
11. Who else has been notified (Local/State Agencies, Media)?				
12. PWS and/or Wastewater Resources Status:				
Additional Monitoring (what type?)				
Intakes (number and location)				
Wastewater Collection and/or Treatment System Status				
Conservation initiated (describe)				
Fire Suppression Capacity				
Storage Capacity				
Treatment (describe normal treatment and if other has been initiated)				
Communication (alerts to public?)				
Other				
13. Call Received By:				
Date/Time Call Received:				

Threat Identification Checklist

If your utility receives a threatening phone call, try to keep the caller on the line to obtain as much information as possible. Record as much information as possible, including:

1. What kind of threat is posed?
 - A. Contamination: What kind of poison? _____
How much? _____
 - B. Physical Damage: What kind of damage? _____
With what kind of device? _____
2. Where? _____
3. When? _____
4. Why? _____
5. By whom? _____
6. What is your (caller's) name? _____
7. What is your (caller's) affiliation, if any? _____
8. What is your (caller's) address/phone #? _____
9. What is the exact wording of the threat? _____

10. Is the caller male female well spoken illiterate foul irrational incoherent
11. Is the caller's voice calm angry slow rapid soft loud laughing crying
 normal slurred nasal clear lisping stuttering deep high
 cracking excited young old

familiar - who did it sound like? _____

accented - what nationality, region? _____

12. Is the connection clear? (Could it have been a wireless or cell phone?)

13. Are there background noises? street noises - what kind? _____

machinery - what type? _____

voices - describe _____

children - describe _____

animals- what kind? _____

computer keyboard/office _____

motors - describe _____

music - what kind? _____

other _____

Name of person receiving call _____ Date _____ Time _____

Notify Utility manager _____ phone: _____

Local FBI/Law Enforcement, Phone _____

Other _____ phone: _____

CONTACT LIST¹ EMERGENCY PLAN INFORMATION

PUBLIC WATER SYSTEM INFORMATION

PWS Name: _____ County: _____

PWS ID#: _____

Address: _____

Phone: _____ Office _____ Plant _____ Fax _____

Key Personnel (i.e., Mayor, City Manager, President, Owner, etc.) - Mark with * if authorized to spend money.

1. Name _____ Position _____
Phone: Office _____ Home _____ Mobile _____
Fax _____ Pager _____ Radio _____

2. Name _____ Position _____
Phone: Office _____ Home _____ Mobile _____
Fax _____ Pager _____ Radio _____

3. Name _____ Position _____
Phone: Office _____ Home _____ Mobile _____
Fax _____ Pager _____ Radio _____

Operations Personnel: (Manager, Operator, Superintendent, etc.) - Mark with * if authorized to spend money.

1. Name _____ Position _____
Cert. Level _____
Phone: Office _____ Home _____ Mobile _____
Fax _____ Pager _____ Radio _____

2. Name _____ Position _____
Cert. Level _____
Phone: Office _____ Home _____ Mobile _____
Fax _____ Pager _____ Radio _____

3. Name _____ Position _____
Cert. Level _____
Phone: Office _____ Home _____ Mobile _____
Fax _____ Pager _____ Radio _____

4. Back-up/fill-in Operator when Primary Operator is not available:

1. Prepared by EPA, Region 6 and TNRCC Satellite Downlink, produced by TX AWWA, August 6, 2002

Name _____ Position _____
Cert. Level _____
Phone: Office _____ Home _____ Mobile _____
Fax _____ Pager _____ Radio _____

OTHER RESOURCES

State Emergency Spill Line Phone _____ Fax _____

State Program Office Phone _____ Fax _____

Regional State Office Phone _____ Fax _____

LOCAL RESOURCES

Police: Phone _____ Radio _____ Other _____ Fax _____

Fire: Phone _____ Radio _____ Other _____ Fax _____

City/Community Emergency Manager: _____
Phone: Office _____ Home _____ Mobile/Pager _____

County Emergency Manager: _____
Phone: Office _____ Home _____ Mobile/Pager _____

TV Station _____ Person _____
Phone _____ Fax _____

TV Station _____ Person _____
Phone _____ Fax _____

Radio Station _____ Person _____
Phone _____ Fax _____

Radio Station _____ Person _____
Phone _____ Fax _____

Newspaper _____ Person _____
Phone _____ Fax _____

Newspaper _____ Person _____
Phone _____ Fax _____

MUTUAL AID AGREEMENTS

Other Water Company
Person _____

Phone _____ Fax _____ Other _____
Summary of Agreement _____

Other Water Company _____
Person _____
Phone _____ Fax _____ Other _____
Summary of Agreement _____

SUPPLIERS (Place if emergency contract is in place)

Equipment

1. Equipment Supplied _____
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

2. Equipment Supplied _____
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

3. Equipment Supplied _____
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Chemicals

Chemicals Supplied _____
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Chemicals Supplied _____
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Chemicals Supplied _____
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Construction

List Heavy Equipment Available _____
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____
Expertise _____

List Heavy Equipment Available _____
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____
Expertise _____

Utilities

Gas Company
Phone _____ Fax _____ Other _____

Electric Company
Phone _____ Fax _____ Other _____

Sewer
Phone _____ Fax _____ Other _____

Telephone Company
Phone _____ Fax _____ Other _____

Alternative Water Supplies (List bottled water suppliers, tank truck owners, etc.)

Provides
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Provides
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Provides
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Engineering Services

Area of Expertise
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Area of Expertise
Company _____ Person _____ Position _____
Phone _____ Fax _____ Other _____

Laboratory Services

Service Provided
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____

Service Provided
Company _____ Person _____

Position _____
Phone _____ Fax _____ Other _____

Repair

Radio Repair
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____

Telemetry Repair
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____

Other
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____

Well Supplies/Drillers

Service _____
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____

Service _____
Company _____ Person _____
Position _____
Phone _____ Fax _____ Other _____

EMERGENCY EQUIPMENT AVAILABLE

Transportation (List boats, trucks, etc.)

Type _____	Owner _____	Storage Location _____
Type _____	Owner _____	Storage Location _____
Type _____	Owner _____	Storage Location _____

Communications (List mobile phones, pagers, radios)

Type _____	Owner _____	Storage Location _____
Type _____	Owner _____	Storage Location _____
Type _____	Owner _____	Storage Location _____

Pumps

Type _____	Size _____
Owner _____	Storage Location _____
Type _____	Size _____
Owner _____	Storage Location _____

Generators

Type _____ Owner _____
Storage Location _____

Type _____ Owner _____
Storage Location _____

Chlorine Response Kit

Type _____ Owner _____
Storage Location _____

Type _____ Owner _____
Storage Location _____

Other

Type _____ Owner _____
Storage Location _____

Type _____ Owner _____
Storage Location _____

Type _____ Owner _____
Storage Location _____



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

10/4/02 CC: JD
JP ✓

SEP 13 2002

OFFICE OF
WATER

C: Row
MIKE 10-4-02

Dear Community Water System Manager:

This letter describes how you can access important new information concerning water security. It also provides information about new requirements for community water systems under the Safe Drinking Water Act, as amended by recent legislation on security and bioterrorism.

On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Preparedness and Response Act) into law (PL 107-188). The Bioterrorism Preparedness and Response Act added Section 1433 (a)(1) to the Safe Drinking Water Act, instructing the Environmental Protection Agency (EPA) to "provide baseline information to community water systems required to conduct vulnerability assessments regarding which kinds of terrorist attacks or other intentional acts are the probable threats to: (a) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or (b) otherwise present significant public health concerns."

In response to the new Bioterrorism Preparedness and Response Act, EPA has completed the *Baseline Threat Information for Vulnerability Assessments of Community Water Systems* document to assist water utilities in conducting vulnerability assessments. This report is not a blueprint for developing a vulnerability assessment; however, it does present an overview of threats, methodologies, and strategies for water utilities to consider as you develop the vulnerability assessments required under the new law. You may obtain a copy of this document through the Water Information Sharing and Analysis Center (WaterISAC). The WaterISAC is a new service intended to provide a secure forum to share and convey security-related information. Directions for obtaining access to the document through the Web-based WaterISAC are described in the Attachment to this letter. Hold all information contained in the document in confidence and take reasonable precautions to protect it.

As noted above, the Bioterrorism Preparedness and Response Act requires every community water system serving a population of greater than 3,300 persons to: (1) conduct a vulnerability assessment; (2) certify and submit a copy of the assessment to the EPA Administrator (within a specified schedule); (3) prepare or revise an emergency response plan that incorporates the results of the vulnerability assessment; and (4) certify to the EPA

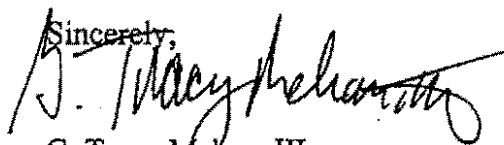
Administrator, within 6 months of completing the vulnerability assessment, that the system has completed such a plan.

The Bioterrorism Preparedness and Response Act establishes the following due dates for certification and submission of the vulnerability assessments, and for certification of the emergency response plans:

Systems serving population of:	Certify and submit VA by:	Certify ERP within 6 mos. of VA but no later than:
100,000 or greater	March 31, 2003	September 30, 2003
50,000 – 99,999	December 31, 2003	June 30, 2004
3,301 – 49,999	June 30, 2004	December 31, 2004

Finally, the Bioterrorism Preparedness and Response Act requires EPA to conduct studies in the areas of: (1) prevention, detection, and response to the intentional introduction of contaminants into community water systems and source water for those systems; (2) methods and means by which terrorists could disrupt the supply of safe drinking water or take actions against drinking water infrastructure; and (3) methods and means by which alternative supplies of drinking water could be provided in the event of the destruction, impairment or contamination of public water systems. As required by the Bioterrorism Preparedness and Response Act, EPA will make this information available, as appropriate, to community water systems through the WaterISAC or other means.

I hope you find the *Baseline Threat Information for Vulnerability Assessments of Community Water Systems* document helpful as you undertake the very important task of improving the security of our nation's drinking water infrastructure.

Sincerely,


G. Tracy Mehan, III
Assistant Administrator

Attachment

Attachment

Directions to Access the Document

Baseline Threat Information for Vulnerability Assessments of Community Water Systems

Provide the following information on the individual designated to access the document. Follow directions below.

Name (printed): _____
Name (signature): _____
Title: _____
Organization: _____
Phone: _____
E-mail: _____
Public Water System Identification # _____
(PWS ID)

If You Have Internet Access

- Fax your request for the document on your organization's letterhead stationery along with this page with requested information. *The letter should be signed by the community water system manager.* The fax number is: 202-785-1845.
- The designee will receive an encrypted E-mail reply with unique password and user identification. You will also receive an access code to open the document in Adobe Acrobat Reader. Please take all reasonable precautions to protect this information.
- Once you have received your username and password by E-mail, go to the Web site: <http://www.waterisac.org/EPAdocument.asp> and log-in. Follow directions on the web site to access the document. You may download a copy of Adobe Acrobat Reader from the WaterISAC web site to open the document.
- For technical assistance in accessing the document, E-mail your question to: info@waterisac.org or call: 866-h2o-ISAC (426-4722). For questions about the content of the document, E-mail Brian Frazer with EPA's Water Protection Task Force at, frazer.brian@epa.gov.

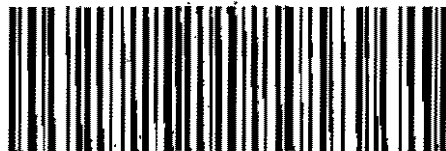
If You DO NOT Have Internet Access

Fax or mail your request for the document on your organization's letterhead stationery along with this page with requested information. *The letter should be signed by the community water system manager.* The fax number is 202-564-8513. The express mail delivery address is: Environmental Protection Agency, Attn: Documents, Room 2104A EPA East, 1201 Constitution Ave. NW, Washington DC, 20004. *If you send the letter by U.S. Postal Service there will be a significant delay.* You will receive the document by registered U.S. mail.

UNITED STATES
ENVIRONMENTAL PROTECTION AGENCY
P.O. BOX 42419
CINCINNATI, OH 45242

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300
AN EQUAL OPPORTUNITY EMPLOYER

CERTIFIED MAIL



7000 0520 0012 0621 3773

PRESORTED
FIRST-CLASS MAIL
POSTAGE AND FEES PAID
EPA PERMIT NO. G-35

T. 25 / P 125
SCOTT WHEELER
MAYOR
CITY OF ADDISON
PO BOX 9010
ADDISON, TX 75001-9010



75001-9010 30

