[redacted]UMENT

2004 VULNERABILITY ASSESS FINAL DOCUMENTS

Appendix 1

VULNERABILITY ASSESSMENT CERTIFICATION

Public Water System ID number: TX 0570031

System Name: Town of Addison

City where system is located: Addison, Texas

State : Texas

Printed Name of Person Authorized to Sign this Certification on behalf of the System: Mike Murphy

Title: Director of Public Works

Address : P.O. Box 9010

City: Addison

State and ZIP Code: Texas 75001

Phone: 972-450-2871 **Fax:** 972-450-2837 **Email:** mmurphy@ci.addison.tx.us

I certify to the Administrator of the U.S. Environmental Protection Agency that this community water system has conducted a vulnerability assessment that complies with Section 1433(a)(1) of the Safe Drinking Water Act, as amended by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law 107-188, Title IV— Drinking Water Security and Safety).

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

The vulnerability assessment this community water system conducted addresses the following components of my system (Check YES if the CWS has the element in its system; check N/A if the element is not applicable to the system.):

YES	N/A	
☑	☐	pipes and constructed conveyances
☑	☐	physical barriers

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

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

Signed: [signature] **Date:** 6/28/07

Primary contact person that EPA can call if there are questions about this Certification and VA submission:
Name: Jim Pierce
Address (if different than that of the Authorized Representative):

Phone: 972-450-2879
Email Address: jpierce@ci.addison.tx.us

Alternate Contact Person:
Name: Jerry Davis
Address (if different than that of the Authorized Representative):

Phone: 972-661-1693
Email Address: jdavis@ci.addison.tx.us

HARDENING TARGETS/ ASSESSING YOUR VULNERABILITY

Teleconference – August 6, 2002

Presented by the
USEPA Region 6/ Texas Natural Resource Conservation Commission/
Texas Section of the American Water Works Association
10a – 2p Central Time/ 9a – 1p Mountain Time

1. **UNDERSTANDING THE BIO TERRORISM ACT – Greg Grover, USEPA Region 6**

2. **RISK OF BIOLOGICAL/CHEMICAL CONTAMINANTS AND PHYSICAL RISKS - Anthony Bennett, TNRCC**

3. **UTILITY VULNERABILITY ASSESSMENTS – William Adams, CDM**

    a. **Understanding the Sandia Model and How it Applies to Medium and Small Systems**
    b. **Performance Based Risk Assessment for Medium and Small Utilities**
        i. **The 8 Criteria of an Assessment**
    c. **What to Look for in Your Assessment – Actual Onsite Assessment**
    d. **Round Table Discussion**

4. **BREAK - CENTRAL TIME ZONE LUNCH – 10 Minutes (Approximately 11:55 am Central Time)**

5. **DEVELOPING CREDIBILITY THROUGH COMMUNICATIONS – Wendy Nero, CH2MHill**
    a. **How to Communicate with Your Customers**

6. **BREAK – MOUNTAIN TIME ZONE LUNCH – 10 Minutes (Approximately 11:20 am Mountain Time)**

7. **EMERGENCY RESPONSE PLANS - William Adams, CDM**
    a. **How to Prepare a Plan**
    b. **How to Integrate Your Vulnerability Assessment**
    c. **Involving First Responders in Your Planning**

(more)

8. WHAT HAPPENS IF YOU HAVE AN EVENT?
    a. The Emergency Response Process
        i. Just Who is in Charge?
            a. Simulated Onsite Emergency Response
        ii. Implementing Your Emergency Response Plan
    b. Reporting Protocols

9. RISK COMMUNICATIONS - Wendy Nero, CH2MHill

10. QUESTIONS AND ANSWERS – Panel Discussion

11. OTHER CONSIDERATIONS

12. RESOURCES

Contact us at:

TAWWA
P.O. Box 80150
Austin, Texas 78708
512-238-9292
512-238-0496 FAX
mikhowe@aol.com
www.tawwa.org

How to CALL or FAX the Teleconference With Your Question.

WHY YOU SHOULD SEND YOUR QUESTION

Your participation in today's teleconference is important because if you have a question, then most likely one or more of the hundreds of your colleagues in the water profession who are watching all over Texas, Oklahoma, Arkansas, Louisiana and New Mexico who wants the answer to the same question. Our experts cannot possibly think of every question, so we need your help.

WHAT TO DO

CALLING IN A QUESTION

You may call us toll free at 1-888-935-2010. Your call will taken by a screener who will take down your question and other information and then pass it on to the production team.

FAXING IN A QUESTION

FAXES can be sent toll free to 1-888-935-2012

Let your site manager know you want to FAX a question. They will show you where the FAX at your site is located if one is available.

IN EITHER CASE, Write your question down as concisely as possible make it easier for our screener to copy down your question. QUESTIONS WILL BE ADDRESSED LATER IN THE PROGRAM. WE WILL TRY TO COVER A MANY AS POSSIBLE WITHIN TIME CONSTRAINTS.

YOU CAN WRITE YOUR QUESTION BELOW AND FAX THIS PAGE.

_____

_____

_____

_____

_____

_____

_____

_____

_____

NAME _____ LOCATION _____

American Water Works Association

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002

Greg Grover
U.S. Environmental Protection Agency
Region 6 – Dallas Office

New Requirements on Public Water Systems

- Conduct a vulnerability assessment
- Develop or revise an emergency response plan
- Certify its completion to EPA by a date certain
- Send a copy to EPA by a date certain

Vulnerability Assessments

- Who is required? - Utilities serving more than 3,300 persons
- What is needed? On a one time basis:
  - Certify to EPA that an assessment was conducted
  - Submit a written copy to EPA
  - Assessments are to include specified items.

Vulnerability Assessment Deadlines

- Submit to EPA by:
  - March 31, 2003 if serving 100,000 or more people.
  - December 31, 2003 if serving 50,000 or more, but less than 100,000 people
  - June 30, 2004 if serving more than 3,300, but less than 50,000 people.

Emergency Response Plans

- Who must prepare: Systems > 3,300 people
- Certify to EPA that plan is complete.
- Maintain copy of plan for five years.
- Incorporate results of vulnerability assessments.
- Include specified items.
- Coordinate with Local Emergency Planning Committees.

New Requirements on EPA

- Baseline threat report
- Develop protocols to protect VAs
- Provide guidance to water systems < 3,300 for conducting VAs

New EPA Research and Development

- Focus is on methods, means, and equipment to prevent, detect, and respond to:
  - contamination
  - supply disruption
- Mandatory, but no deadline
- Results to be shared with water community through the Water Information Sharing and Analysis Center (ISAC)

New EPA Authorities and Penalties

- If there is a threatened or potential terrorist attack and the utility or the state aren't responding, EPA can step in
- Significantly increases penalties for tampering with a water system

New Resources

- $160 million authorized for this year, but not yet allocated
- Money for utilities to conduct VAs, do plans, and address security needs
- $ 5 million of that for systems < 3,300 to conduct VAs
- $15 million extra for EPA research activities

Risk of Biological and Chemical Contaminants

Chemical Agents

- Pulmonary Intoxicants
- Blister Agents
- Nerve Agents
- "Blood" Agents

Pulmonary Intoxicants

- Inhalation Hazard
- Common Chemicals
  - Chlorine Gas
  - Ammonia

Blister Agents

- Topical Eye, Skin, and Airway Damage
- Military Vesicants
  - Mustard
  - Lewisite
- Other
  - Poison Ivy
  - Industrial Chemicals
  - Chemotherapeutics

Nerve Agents

- Glandular Activity and Loss of Muscle Control (SLUD)
- Military Agents
  - Tabun (GA)
  - Sarin (GB)
  - VX
- Other
  - Carbamates
  - Organophosphate Pesticides

Blood Agents

- Interferes with cell uptake of oxygen
- Common Chemicals
  - Hydrogen Cyanide
  - Cyanogen Chloride
  - Other Cyanides

List of very toxic Chemicals

- amanitin (mushrooms)
- saxitoxin (algae)
- sodium fluoroacetate
- sarin (GB)
- chlorophenol, m-
- dimefox
- dichloropropane, 1,2-
- benzyl alcohol
- sulfolane
- terbufos
- fensulfothion
- carbofuran
- parathion
- strychnine
- aldicarb
- tetrahydrofuran
- TEPP
- aminopyridine, 4-
- cyanides
- hydrogen cyanide

Biological Agents

- Bacteria
- Viruses
- Protozoa

Most Likely Biological Agents

- NATO NBC Handbook Narrows the list to 31
- USAMRIID Criteria Narrows the list to 6 based on
  - Availability
  - Ease of Production
  - Lethality
  - Stability (Deliverability)
  - Infectivity

Most Likely Biological Agents

- Anthrax
- Smallpox
- Plague
- Tularemia
- Botulism Toxin
- Viral Hemorrhagic Fevers

CDC Category A Bioterrorism Agents

- Smallpox
- Anthrax
- Plague
- Botulism Toxin
- Tularemia
- Hemorrhagic Fevers

Biological vs Chemical and other agents of Mass Destruction

- Inexpensive / relatively easy to produce
- 1970 study cost to produce 50% casualties in a 1sq/km area
  - Conventional weapons - $2000
  - Nuclear - $800
  - Chemical - $600
  - Anthrax $1

Components of Bio/Chemical Terrorism

- Capability
- Intent
- Vulnerability

What makes an effective Agent

- Easy Method of Delivery
- Physical/chemical properties make the delivery effective
- Lethality

Drinking Water

- Delivery
  - Source
    - dilution effects the lethality
    - treatment removes or Inactivates the agent
  - Storage Tanks
    - dilution
    - ineffective dispersion
    - Inactivation of Agent (contact time)

Drinking Water

- Physical/Chemical Properties
  - Military bio/chemical agents
    - air delivery
    - persistence in concentration delivered by air
    - these properties make the agent effective more than the lethality
  - Physical treatment and disinfection effect many potential agents

Drinking Water

- Lethality
  - Based on Dose
  - Water dilutes the dose
  - Disinfection inactivation

Source Vulnerability

- Agent Risk
  - Massive Dilution
  - Physical Treatment
  - Chemical Treatment
- Physical Disruption Risk
  - ?

Treatment Vulnerability

- Agent Risk
  - Large Dilution
  - Physical Removal
  - Chemical Treatment
- Physical Disruption Risk
  - High

Distribution Vulnerability

- Agent Risk
  - Lack of dilution
  - Lack of physical removal
  - Insufficient contact time for inactivation
- Physical Disruption Risk
  - limited except for large transmission lines and large pump stations

Conclusion

- Biological Agents may be cheaply produced (Anthrax)
- Certain Commercially available pesticides have solubility and lethality to cause concern

Conclusion

- Ineffective/missing barriers increase vulnerability
  - Weaker Disinfectants/oxidants
  - No/post physical treatment
- Dilution reduces lethality

Vulnerability Assessment

A systematic analysis used to determine the malevolent risks posed to the operations of water supply, treatment, and distribution systems/ wastewater systems.

Vulnerability Assessment

1. Determination of water system objectives by:
   - Identifying the important missions/functions of the system to be assessed,
   - Identifying the undesirable consequences that could affect the missions/functions,
   - Determining the assets that need to be protected to minimize the impacts of the undesirable events/consequences,
   - Determining the malevolent acts that could reasonably cause these events/consequences.

Vulnerability Assessment

2. Prioritization of adverse events/consequences affecting the water system and the surrounding community including:
   - Loss of critical function and/or major service disruption,
   - Intentional attack on public safety via water Utility assets, contamination of the water supply, and chemical releases or chemical theft.

Vulnerability Assessment

3. Definition of how the malevolent acts might be conducted, such as:
    - Physical damage,
    - Chemical, biological, and radiological contamination,
    - Cyber attacks on the Supervisory Control and Data Acquisition (SCADA) or other process control systems,
    - Interdependency disruptions (e.g., electrical, transportation, etc.)

Vulnerability Assessment

4. Assessment of the likelihood (qualitative probability) of such malevolent acts from defined threat sources (e.g. terrorist, insider, determined vandal, casual vandal, etc.)

Vulnerability Assessment

5. Systematic site characterization of the water system to include the collection of performance data on:
    - Important facilities, processes, and assets,
    - Physical protection system features of deterrence, detection, delay, and response,
    - Cyber protection system features,
    - Security policies and procedures and compliance with same

Vulnerability Assessment

6. The approach to the V/A is "performance-based," meaning that it evaluates the risk to the water system based on the effectiveness of the security system against the specific malevolent acts determined in the initial step.

Vulnerability Assessment

7. The V/A determines the most critical assets (targets) in a water system, details their interrelationships within other assets in the system, identifies the consequences of malevolent acts that could be directed against them, and evaluates the effectiveness of both existing and proposed protection systems.

Vulnerability Assessment

8. The V/A identifies a system's vulnerabilities and provides a prioritized plan for security upgrades, modifications of operational procedures, and/or policy changes to mitigate identified risks to critical assets. The V/A also provides a basis for comparing the cost of protection against the risks posed.

Vulnerability Assessment

The overall goal of the V/A is to develop recommendations that lead to a cost-effective, balanced security protection system with regards to the malevolent acts identified

Goals of Security Measures

- Detect
  - Alarms Systems
- Delay
  - Locks, Gates, Fencing, & Signage
- Respond
  - Law Enforcement
  - Water System Staff

Vulnerability of Water Supply

Areas Include:

- Raw Water Source
- Treatment Facilities
- Connections to Water Distribution System Pipes
- Pump Stations and Valves
- Finished Water Tanks and Reservoirs

Hardening of Water Supply

- **Perimeter Intrusion Detection**
  - Fence Mounted Systems
  - Door Switches
  - Motion Detectors
  - Vibration or Shock Sensors
  - Video Motion Detector
- **Access Control Systems (ACS)**
  - Conventional Lock and Key
  - Electronic ACS
- **Closed Circuit (CCTV) Systems**
  - Cameras

Real Time Monitoring

- Water Quality Monitoring
- System Performance
  Indicators:
  - Chlorine
  - Pressure
  - Tank Levels
  - Flow Meters

Training

- Awareness Training
  - AWWA
- Risk Assessment / Vulnerability Analysis
  - EPA / AWWARF
- Employee
  - Call Takers
  - Suspicious Activity Sensitivity
  - Emergency Response
  - Sampling

EPA Region 6 Water Security[1]

July 2002

The Environmental Protection Agency (EPA), Region 6 office is located in Dallas, Texas and includes the states of Arkansas, Louisiana, New Mexico, Oklahoma and Texas. The regional drinking water and wastewater programs work with the State agencies in administering the federal drinking water and wastewater rules and regulations.

Security issues are a priority for EPA. In June 2002, the President signed PL 107-188, the Public Health, Security, and Bioterrorism Preparedness and Response Act that includes provisions to help safeguard the nation's public drinking water and wastewater systems against terrorist and other intentional acts. On a national level, the EPA has been designated as the lead for water and wastewater infrastructure security so Region 6 has a vested interest in preparing for an incident of catastrophic proportions. Such effects could potentially impact the water and wastewater infrastructure and/or water quality within Region 6. The events of 9/11 have resulted in new legislation, funds and responsibility for EPA and other federal agencies. EPA is working with numerous other federal and state agencies in these endeavors as well.

The Region 6 office has formed a regional team to deal with drinking water and wastewater issues. Drinking water and wastewater systems can contact the regional contacts directly for information on security issues; however, in the event of an emergency, remember to first contact 911, then the EPA Regional Emergency Response Center and the appropriate State drinking water and wastewater emergency response contact. Please refer to the following page for important Regional contact information.

EPA encourages drinking water and wastewater systems to take action to protect their assets from tampering. The handouts being provided are inexpensive steps that can be taken to enhance security and protect our drinking water and wastewater systems.

Handouts

Security Awareness for Industrial and Municipal Facilities – *overview on steps to take to protect your facility, your products and your community*
Pipe Hanger – *top ten list for emergency preparedness and security for small groundwater suppliers*
General Security Checklist – *questions to consider for safe security practices at your facility*
Emergency Contact List – *to summarize various contacts needed in an emergency*
Threat Identification Checklist – *to be used if your utility receives a threatening phone call*
Water/Wastewater System Incident Checklist– *to be used to report an actual incident*
Guidance for Water Utility, Response, Recovery & Remediation Actions for Man-made and/or Technological Emergencies – *guidance for responding to a catastrophic emergency*
Vulnerability Self-Assessment Guide – *guidance intended for systems 3,300 or less and does not include most of the 8 essential elements necessary for adequate vulnerability assessment at larger systems*

---

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

REGION 6
HOMELAND SECURITY
CONTACT LIST

In the event of an emergency, always first call 911.

EPA Emergency Response Center: National (800) 424-8802
Region 6 (866) 372-7745

STATES (Drinking Water)

Agency	Phone	Email
Arkansas Department of Health Division of Engineering	501/661-2623 After Hours & Emergencies: 501/661-2136	safewater@healthyarkansas.com
Louisiana Department of Health and Hospitals Safe Drinking Water Program Karen S. Irion, P.E., Administrator	24-hour Hotline: 800/256-4609 225/765-5046	kirion@dhh.state.la.us
New Mexico Environment Department Drinking Water Bureau	24-hour Hotline: 505/827-7536 505/827-1400	retta_prophet@nmenv.state.nm.us
Oklahoma Department of Environmental Quality Public Water Supply Section	24-hour Hotline: 800/522-0206 405/702-8100	mike.harrell@deq.state.ok.us
Texas Commission on Environmental Quality Public Drinking Water Section	24-hour Hotline: 800/832-8224 512/239-4691	MLannen@tnrcc.state.tx.us

- continued on back page -

STATES (Wastewater)

Agency	Area of Expertise	Phone	Email
Arkansas Department of Emegency Management		24-hour Hotline: 800/322-4012	
- Richard McDuffy	Emergency Response	501/682-0716	mcduff@adeq.state.ar.us
- Richard Merritt	Emergency Response	501/682-0713	merritt@adeq.state.ar.us
Louisiana Department of Environmental Quality		24-hour Hotline: 225/342-1234	
- Jeff Meyers	Emergency Response	225/765-2566	jeff_m@deq.state.la.us
- Chris Roberie	Surveillance	225/765-2953	c_roberie@deq.state.la.us
New Mexico Environmental Division		24-hour Hotline: 505/827-9329	
- Debbie Brinkerhoff	Hazardous Waste Emergency Response	505/428-2528	
Oklahoma Department of Environmental Quality		24-hour Hotline:	
- Lynne Moss	Emergency Response	800/522-0206	
- Larry Gales	Emergency Response	405/702/8142	larry.gales@deq.state.ok.us
Texas Natural Resource Conservation Commission		24-hour Hotline: 800/832-8224	
Environmental Response	Hotline telephone	512/239-2507	
- Tom Weber	Emergency Response	512/239-6928	tweber@tnrcc.state.tx.us
- Buck Henderson	Emergency Response	512/239-0990	ehenders@tnrcc.state.tx.us

EPA (Water Quality Protection Division)

Name	Area of Expertise	Phone	Email
Larry Wright Branch Chief	Source Water Protection	214/665-7150	wright.larry@epa.gov
Jim Brown Section Chief	Drinking Water	214/665-7155	brown.jamesr@epa.gov
Greg Grover	Drinking Water	214/665-2776	grover.greg@epa.gov
Dawn Ison	Drinking Water	214/665-2162	ison.dawn@epa.gov
Andy Waite	Drinking Water	214/665-7332	waite.andrew@epa.gov
Blake Atkins	Drinking Water - Tribes	214/665-2297	atkins.blake@epa.gov
Mike Tillman	Wastewater	214/665-7531	tillman.Michael@epa.gov
Debora Browning	Outreach/Public Involvement	214/665-8025	browning.debora@epa.gov
Cindy Wolf	Outreach/Public Involvement	214/665-7291	wolf.cynthiap@epa.gov

U.S. Environmental Protection Agency, Region 6 - July 2002

Security Awareness for Industrial and Municipal Facilities

Because of the tragic events on 9-11-01, homeland security is one of the nation's highest priorities. Each of us can play a role in safeguarding our country from terrorism. The purpose of this document is to suggest what steps you may take to protect your facility, your products, and your community.

EMERGENCY CONTACTS

Local Law Enforcement: _____

Local Emergency Planning Committee: _____

State Police: _____

EPA National (24-hour) Response Center Hotline for Incidents: 800/424-8802

EPA Region 6 (24-hour) Emergency Response Center: 866/372-7745

REPORT SUSPICIOUS ACTIVITIES TO LAW ENFORCEMENT AUTHORITIES

If a breach of security or suspicious activity does occur, timely cooperation with authorities is crucial. In addition to cooperation with your local police department, it is suggested that you expeditiously report any threats or suspicious behavior to your local law enforcement office. You should provide the following information:

- Description of individual and vehicle, including license plat number;
- Any break-ins;
- Missing chemicals, equipment or blank documentation forms (such as shipping papers).

SUSPICIOUS ACTIVITIES

Be alert if you observe someone engaging in any of the following activities, especially if the individual is a stranger to the area:

- The individual, a non-regular customer, requests to purchage large amounts of chemical, pesticide, product(s) etc., with cash;
- The individual is loitering on your premises or around toxic materials with no legitimate reason for being there;
- The individual hesitates or hedges when asked for information such as name, address, or photo identification;
- The individual provides personal identification that appears to have been altered, or commercial certification alterations;
- The individual asks specific questions about toxicity of a chemical or operation of equipment;
- You notice a person or persons loitering on or near the chemical storage area;
- The individual ask nervous, avoids eye contact and/or is uneasy.

SECURITY SUGGESTIONS

- Develop and implement written security procedures to address potential risks and potential vulnerabilities;
- Complete employee background checks;
- Assess overall physical security of the facility and identify potential threats, vulnerabilities, risks and countermeasures;
- Develop written plan to coordinate with local law enforcement authorities;
- Develop written plan to coordinate with local fire department and to alert them of the chemicals that are on-site and their storage location;
- Establish proper authorization for employees who work in sensitive or restricted areas;
- Check identification of employees and visitors;
- Review emergency shutdown procedures;
- Limit access to sensitive areas;
- Ensure protection of network from internet hacking;

(continued...)

(...continued)

- Limit removal of hazardous materials or sensitive documents to authorized personnel only;
- Obtain back-up power source(s);
- Training for employees and contractors concerning security awareness, operation of emergency equipment, and procedures for emergency response;
- Perform periodic unscheduled, undercover security inspections and assessments; make adjustments as necessary.

SITE SECURITY

Facility security needs may differ for every business, some of the fundamental security control points may include:

- Establish perimeter protection which uses fences, trenches, natural barriers, turnstiles, and security lighting;
- Change locks, passwords, etc., following termination of an employee;
- Implement access control measures, such as signs, security doors and window locks, alarm systems, and card-based access control systems;
- Protect and backup critical communications equipment and utilities;
- Remove security-sensitive information from facility internet site;
- Periodically analyze computer transaction histories to look for irregularities that might indicate security breaches;
- Back-up data and critical material at an alternate location;
- All hazardous materials and/or deliveries coming into the facilities should be accompanied by shipping papers and driver photo identification;
- Employee security personnel if necessary to ensure site security.

EMERGENCY PREPAREDNESS

- Routinely update emergency telephone numbers and post in a prominent location;
- Develop written communications plan to coordinate with employees and local hospitals;
- Test sirens or other alarm systems on a regular basis;
- Practice emergency evacuation procedures;
- Provide training to emergency coordinators;
- Ensure that first-aid supplies are on-hand, inventoried, and fully stocked for the number of employees at the facility.

ADDITIONAL RESOURCES FOR SITE SECURITY

EPA's Drinking Water Website:
www.epa.gov/safewater/security

EPA's General Site Security Information Website:
www.epa.gov/swercepp/p-small.htm

EPA's Site Security Fact Sheet on Chemicals:
www.epa.gov/ceppo/pubs/secale.pdf

EPA's Local Emergency Planning Committee and Deliberate Releases Fact Sheet:
www.epa.gov/ceppo/factsheet/lepcct.pdf

EPA's Ammonia Theft Fact Sheet:
www.epa.gov/ceppo/pubs/csalert.pdf

EPA's Fact Sheet on Chemical Releases Related to Electrical Power Outages:
www.epa.gov/ceppo/pubs/power.pdf

American Chemistry Council's (ACC's) Site Security Guidelines and Transportation Security Guidelines for the Chemical Industry:
www.americanchemical.com

Homeland Security Office Website:
www.whitehouse.gov/homeland

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

Checklist of General Security Practices

Buildings and facility grounds:

Are all unoccupied buildings always locked and alarms set?

Are "Authorized Personnel Only" signs posted at the entrance to all facilities?

Are important telephone numbers posted on the outside of each building and/or on the inside of fences, and readily visible for emergency use by the public?

Are the facility grounds randomly and frequently patrolled?

Are daily security sweeps conducted?

Are all parts of the facility regularly and thoroughly inspected, including those portions not readily visible?

Are deliveries inspected, packages X-rayed?

Is parking designated or otherwise controlled on the facility?

Is access controlled to chemical and pesticide products and waste locked and/or fenced?

Are entrance gates adequately protected and access controlled by security personnel?

Is protection provided (i.e., with concrete barriers) to prevent a speeding vehicle (including along facility driveway) from hitting plant or other facilities?
Are all outside stored chemicals protected from theft and vandalism?

Is there a backup or redundant exterior electrical connection to the utility grid?

Are fire/smoke alarms provided within all building structures?

Are all buildings (including walls, roofs, windows, etc) constructed to commercial grade standards?

Is there adequate setback from exterior thoroughfares for key facility buildings, tanks, etc.?

Keys:

Are distribution and number of keys known and controlled?

Are all keys labeled as "DO NOT DUPLICATE"?

Are local police departments provided with access keys?

Are keys always removed from all unattended equipment?

Fencing:

Do entrance barriers and fences present credible deterrent to unauthorized entry?

Are entrance gate(s) kept locked?

Is all fencing at least 10' high, with inward-facing barbed wire on top, including on entrance gate(s)?

Is all fencing, including gate(s), secure to ground to prevent access under fence?

Is fence at least 4' higher than any structure or landscaping located directly outside of fence which may provide climbing access over fence?

Is fence at least 6' away from any structure or landscaping located directly outside of fence which may provide climbing access over fence?

Lighting:

Is entire perimeter of facility property illuminated with street-type lighting fixtures?

Is entire perimeter of facility illuminated so that all shadows and dark areas are eliminated?

Is lighting mounted at approximately a second story level?

Are exterior light bulbs of commercial grade and break resistant?

Is lighting provided in parking lots and other areas with limited staffing?

Are lights provided over entrance doors?

Entrance doors:

Are all doors:

Built of commercial grade with metal frame construction?

Outside hinges hidden/protected from vandalism?

Fitted tightly and free from mail slot and excessive air gaps, including at floor/threshold?

Provided with commercial grade, one-sided lock?

Provided with push ("panic") bar release on inside of door?

Visitor entrances provided with an audible annunciator?

Doors and locks in good condition?

Electronically controlled so that each employee must use swipe card or enter a pin number to enter the plant? Is a computer record made of the date, time, and employee who entered the plant?

Windows:

Are all windows (including on doors) covered with metal security mesh?

In case broken or opened, are all windows wired to loud audible alarm and to automatic telephone dialer or central station alarm?

Electronic surveillance:

Is entire perimeter of facility installed with infrared or microwave motion sensors in area between building and fence?

Are motion sensors electrically connected to automatic telephone dialer or central station alarm company?

Is a closed-circuit television video (CCTV) system provided to monitor property perimeter?

Is this system monitored by facility security personnel?

Is this system always on or activated by connection to motion sensors?

Is a CCTV system provided to monitor all vital parts of the plant, including the main entrance and control room and recorded on a slow speed security VCR (tapes not reused/recycled for predetermined time)?

Forms & Written Plans:

Are emergency telephone numbers (including ambulance, police, FBI, spill response) current and prominently displayed at each telephone?

Are MSDS and chemical response information present for all stored chemicals?

Is a chain of command and emergency call list established, updated annually, and prominently displayed (must include 24/7 telephone numbers for system superintendent and chief municipal officer)?

Does a written security program plan exist, are employees frequently trained in the plan, and is the plan reevaluated periodically?

Are all employees, including Customer Service staff, trained and checklists provided on how to handle a threat or incident if called in?

Are practice drills conducted frequently?

Have detection, response, and notification issues been discussed with local public health officials and a

protocol established?

If facility is subject to the Emergency Planning and Community Right-to-Know Act (EPCRA), do local emergency management officials have the most recent emergency plan and information on chemical storage areas?

Procedures:

Can operational procedure times be varied so as not to reveal work patterns?

Is a daily log used and initialed by the last person who leaves the plant to verify that all appropriate doors and windows are locked, appliances are off, night lights are on, and that entrance doors are locked and alarm set?

Is access controlled to computer networks and control systems, and passwords changed frequently?

Are visitors/delivery vehicles stopped at the gate, signed-in, and authorization to enter verified before admission to facility?

Are vehicles plate numbers recorded?

Law enforcement agencies:

Are police departments (daytime and nighttime coverages) familiar with facility layout and systems; do they conduct routine patrols of facilities; and, are protocols established for reporting and responding to threats and other emergencies (and updated annually)?

Are staff instructed to immediately report to the police and FBI any criminal threat, security breach, suspicious behavior, or attack on their facility?

Are copies of operational procedures, including contacts and current telephone numbers, provided to police departments and emergency management personnel?

Was a facility security survey conducted?

Employees:

Does each employee display their sealed photo ID at all times?

Are background security checks conducted on employees at hiring and periodically thereafter?

Upon employee termination, are pass codes changed, and keys and access cards returned?

Non-employee access:

Is a visitor and contractor policy established for employees to limit/question/scrutinize stranger(s) to the facility? Are procedures established in the event that an unscheduled visitor or stranger arrives after normal business hours requiring the person to use the intercom for initial contact. Is access restricted unless the person has the proper credentials and clearance.

Are all chemical and other supply deliverers required to show proper identification and sign-in?

Do facility personnel observe delivery personnel during delivery and until delivery vehicles leaves property?

Are non-employees accompanied and/or observable at all times?

Surrounding Environment:

Are there other buildings in the immediate area that are vulnerable to unauthorized entry?

Are there storage tanks or possible sources of an explosion in the immediate area?

Is the area well lighted and adequately patrolled?

Are important facility telephone numbers given to neighbors to report suspicious activity at the facility?

Is a formal or informal "Neighborhood Watch" program established around the facility?

CONTACT LIST[1]
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 _____

<u>SUPPLIERS</u> (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_____

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: _____

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
  - ❑ Biological
  - ❑ Chemical
  - ❑ Radiological
- ❑ Physical Destruction
- ❑ Cyber attack
- ❑ Bombs, explosives, etc.
- ❑ Wastewater treatment plant Interference and/or pass through
- ❑ Other (explain)
- ❑ **Brief description of incident:**

2. System Name

Address:

Telephone:

System Contact
Name:
Title:

3. Party Responsible for Incident (Name and Address)

Phone Number (from caller ID):

4. Location of Incident

- ❑ Raw Water Source
- ❑ Water Treatment Plant
- ❑ Water Storage Facilities
- ❑ Distribution Line
- ❑ Wastewater Collection and/or Treatment System
- ❑ Receiving Stream
- ❑ Other (explain):

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:

United States
Environmental Protection
Agency

Office of Water
Water Protection Task Force

April 15, 2002

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 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:	• Notify local Law Enforcement • Notify local FBI Field Office • Notify National Response Center	• Notify local/state emergency management organization • Notify ISAC	• 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 • Notify Governor
	Source Water	**Drinking Water Treatment Facility**	**Water Distribution / Storage**	**Wastewater Collection System**	**Wastewater Treatment Facility**
RESPONSE ACTIONS	• Increase sampling at or near system intakes • Consider whether to isolate the water source if possible	• 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	• Consider whether to isolate the water in the affected area if possible	• 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.	• 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)

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

RECOVERY ACTIONS	Recovery actions should begin once the contaminant is through the system.		
Recovery Notifications:	• Notify Customers • Notify Media • Notify ISAC		
Appropriate Utility Elements:	• Sample appropriate system elements (storage tanks, filters, sediment basins, solids handling) to determine if residual contamination exists.	• Flush system based on results of sampling • Monitor health of employees	• Plan for appropriate disposition of personal protection equipment (PPE) and other equipment
REMEDIATION ACTIONS	• Based on sampling results – assess need to remediate storage tanks, filters, sediment basins, solids handling.	• Plan for appropriate disposition of PPE and other equipment	• 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	• No recommended action to take	• No recommended action to take	• 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	• 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:	• 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	• Consider flushing system via hydrants in distribution systems			
REMEDIATION ACTIONS:	**Water Distribution/Storage**	• Assess need to decontaminate/replace distribution system components.		
	Wastewater Treatment Plant	• Based on sampling results – assess need to remediate storage tanks, filters, sediment basins, solids handling.	• Plan for appropriate disposition of PPE and other equipment	• If waste water treatment plant was by-passed – sample and establish monitoring regime for receiving stream and potential remediation based on sampling results.

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:	• 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	• Increase sampling at or near system intakes • Consider whether to isolate	• 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)	• 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	• 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:	• Assist health department with notifications to customers, media, downstream users and other organizations		
Appropriate Utility Elements:	• Sample appropriate system elements (storage tanks, filters, sediment basins, solids handling) to determine if residual contamination exists.	• Flush system based on results of sampling • Monitor health of employees	• Plan for appropriate disposition of personal protection equipment (PPE) and other equipment
REMEDIATION ACTIONS	• Based on sampling results – assess need to remediate storage tanks, filters, sediment basins, solids handling and drinking water distribution system	• Plan for appropriate disposition of PPE and other equipment	• 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:	• Notify local Law Enforcement • Notify local FBI Field Office	• Notify National Infrastructure Protection Center (NIPC) at 1-888-585-9078 (or 202-323-3204/5/6)	• Notify other associated system authorities (wastewater, water) • Notify employees	• If the water is assessed to be unfit for consumption, 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	• Increase sampling at or near system intakes • Consider whether to isolate	• 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	• Monitor unmanned components (storage tanks & pumping stations) • Consider whether to isolate	• 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:	• 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:	• With FBI assistance, make an image copy of all system logs to preserve evidence. • With FBI assistance, check for implanted backdoors and other malicious code and eliminate them before re-starting SCADA system • Install safeguards before re-starting SCADA • Bring SCADA system up and monitor system
REMEDIATION ACTIONS	• 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.

Initial Notifications:	• Notify local Law Enforcement • Notify local FBI Field Office • Notify National Response Center	• Notify local/state emergency management organization • Notify Governor • Notify ISAC	• Notify other associated system authorities (wastewater, water) • Notify local government officials	• 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 System**	**Water Distribution / Storage**	**Wastewater Collection System**	**Wastewater Treatment Facility**
RESPONSE ACTIONS	• 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 alternative 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				
RECOVERY ACTIONS	Recovery actions should begin as soon as practical after damaged facility is isolated from the rest of the utility facilities.				
Recovery Notifications:	• Employees • Law enforcement		• Notify local FBI office		
Appropriate Utility Elements:	• Dependent on the feedback from damage assessment teams		• Implement damage recovery plan		
REMEDIATION ACTIONS	• Repair damage.		• Assess need for additional protection/security measures for damaged facility, and other critical facilities within the utility.		

Notes:

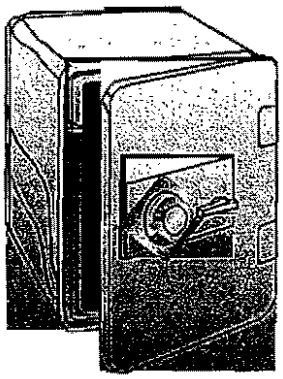
Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems

Association of State Drinking Water Administrators

National Rural Water Association

May 30, 2002

A Note about Security for this Document



This document contains sensitive information about the security of your water system. Therefore, it should be treated as **Confidential Information** and should be stored in a secure place at your water system. A duplicate copy should also be stored in a secure off-site location.

Acknowledgments

This document is the result of collaboration among the Association of Drinking Water Administrators (ASDWA), the U.S. Environmental Protection Agency (U.S. EPA), the U.S. EPA Drinking Water Academy, and the National Rural Water Association (NRWA). We also thank NWRA for the template that was used as the foundation for this project.

Contents

SECURITY VULNERABILITY SELF-ASSESSMENT GUIDE FOR SMALL WATER SYSTEMS 4

INTRODUCTION 4
HOW TO USE THIS SELF-ASSESSMENT GUIDE 4
KEEP THIS DOCUMENT 4

SECURITY VULNERABILITY SELF-ASSESSMENT 5

RECORD OF SECURITY VULNERABILITY SELF-ASSESSMENT COMPLETION 5
INVENTORY OF SMALL WATER SYSTEM CRITICAL COMPONENTS 6

SECURITY VULNERABILITY SELF-ASSESSMENT FOR SMALL WATER SYSTEMS 7

GENERAL QUESTIONS FOR THE ENTIRE WATER SYSTEM 7
WATER SOURCES 10
TREATMENT PLANT AND SUPPLIERS 10
DISTRIBUTION 12
PERSONNEL 12
INFORMATION STORAGE/COMPUTERS/CONTROLS/MAPS 13
PUBLIC RELATIONS 14

ATTACHMENT 1. PRIORITIZATION OF NEEDED ACTIONS 16

ATTACHMENT 2. EMERGENCY CONTACT LIST 17

SECTION 1. SYSTEM IDENTIFICATION 17
SECTION 2. NOTIFICATION/CONTACT INFORMATION 18
SECTION 3. COMMUNICATION AND OUTREACH 21

ATTACHMENT 3: THREAT IDENTIFICATION CHECKLISTS 22

WATER SYSTEM TELEPHONE THREAT IDENTIFICATION CHECKLIST 22
WATER SYSTEM REPORT OF SUSPICIOUS ACTIVITY 24

CERTIFICATION OF COMPLETION 27

Security Vulnerability Self-Assessment Guide for Small Water Systems

Introduction

Water systems are critical to every community. Protection of public drinking water systems must be a high priority for local officials and water system owners and operators to ensure an uninterrupted water supply, which is essential for the protection of public health (safe drinking water and sanitation) and safety (fire fighting).

Adequate security measures will help prevent loss of service through terrorist acts, vandalism, or pranks. If your system is prepared, such actions may even be prevented. The appropriate level of security is best determined by the water system at the local level.

This Security Vulnerability Self-Assessment Guide is designed to help small water systems determine possible vulnerable components and identify security measures that should be considered. A "vulnerability assessment" is the identification of weaknesses in water system security, focusing on defined threats that could compromise its ability to provide adequate potable water, and/or water for firefighting. This document is designed particularly for systems that serve populations of 3,300 or less. This document is meant to encourage smaller systems to review their system vulnerabilities, but it may not take the place of a comprehensive review by security experts.

The Self-Assessment Guide has a simple design. Answers to assessment questions are "yes" or "no," and there is space to identify needed actions and actions you have taken to improve security. For any "no" answer, refer to the "comment" column and/or contact your state drinking water primacy agency.

How to Use this Self-Assessment Guide

This document is designed for use by water system personnel. Physical facilities pose a high degree of exposure to any security threat. This self-assessment should be conducted on all components of your system (wellhead or surface water intake, treatment plant, storage tank(s), pumps, distribution system, and other important components of your system).

The Assessment includes an emergency contact list for your use. This list will help you identify who you need to contact in the event of an emergency or threat and will help you develop communication and outreach procedures. Filling out the Emergency Contact List is an important step toward developing an Emergency Response Plan, which provides detailed procedures on how to respond to an emergency.

You may be able to obtain sample Emergency Response Plans from your state drinking water primacy agency.

Security is everyone's responsibility. We hope this document helps you to increase the awareness of all your employees, governing officials, and customers about security issues.

Once you have completed this document, review the actions you need to take to improve your system's security. Make sure to prioritize your actions based on the most likely threats. Please complete the Certificate of Completion on page 27 and return only the certificate to your state drinking water primacy agency. Do not include a full copy of your self-assessment.

Keep this Document

This is a working document. Its purpose is to start your process of security vulnerability assessment and security enhancements. Security is not an end point, but a goal that can be achieved only through continued efforts to assess and upgrade your system.

Don't forget that this is a sensitive document. It should be stored separately in a secure place at your water system. A duplicate copy should also be retained at a secure off-site location.

Access to this document should be limited to key water system personnel and local officials as well as the state drinking water primacy agency and others on a need-to-know basis.

Security Vulnerability Self-Assessment

Record of Security Vulnerability Self-Assessment Completion

The following information should be completed by the individual conducting the self-assessment and/or any additional revisions.

Name: _____

Title: _____

Area of Responsibility: _____

Water System Name: _____

Water System PWSID: _____

Address: _____

City: _____

County: _____

State: _____

Zip Code: _____

Telephone: _____

Fax: _____

E-mail: _____

Date Completed: _____

Date Revised: _____ **Signature:** _____

Date Revised: _____ **Signature:** _____

Date Revised: _____ **Signature:** _____

Date Revised: _____ **Signature:** _____

Date Revised: _____ **Signature:** _____

Inventory of Small Water System Critical Components

Component	Number & Location (if applicable)	Description
Source Water Type		
Ground Water		
Surface Water		
Purchased		
Treatment Plant		
Buildings		
Pumps		
Treatment Equipment (e.g., basin, clearwell, filter)		
Process Controls		
Treatment Chemicals and Storage		
Laboratory Chemicals and Storage		
Storage		
Storage Tanks		
Pressure Tanks		
Power		
Primary Power		
Auxiliary Power		
Distribution System		
Pumps		
Pipes		
Valves		
Appurtenances (e.g., flush hydrants, backflow preventers, meters)		
Other Vulnerable Points		
Offices		
Buildings		
Computers		
Files		
Transportation/ Work Vehicles		
Communications		
Telephone		
Cell Phone		
Radio		
Computer Control Systems (SCADA)		

Security Vulnerability Self-Assessment for Small Water Systems

General Questions for the Entire Water System

The first 13 questions in this vulnerability self-assessment are general questions designed to apply to all components of your system (wellhead or surface water intake, treatment plant, storage tank(s), pumps, distribution system, and offices). These are followed by more specific questions that look at individual system components in greater detail.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
1. Do you have a written emergency response plan (ERP)?	Yes • No •	It is essential that you have an ERP. If you do not have an ERP, you can obtain a sample from your state drinking water primacy agency. As a first step in developing your ERP, you should develop your Emergency Contact List (see Attachment 2). A plan is vital in case there is an incident that requires immediate response. Your plan should be reviewed at least annually (or more frequently if necessary) to ensure it is up-to-date and addresses security emergencies. You should designate someone to be contacted in case of emergency regardless of the day of the week or time of day. This contact information should be kept up-to-date and made available to all water system personnel and local officials (if applicable). Share this ERP with police, emergency personnel, and your state primacy agency. Posting contact information is a good idea only if authorized personnel are the only ones seeing the information. These signs could pose a security risk if posted for public viewing since it gives people information that could be used against the system.	
2. Is access to the critical components of the water system (i.e., a part of the physical infrastructure of the system that is essential for water flow and/or water quality) restricted to authorized personnel only?	Yes • No •	You should restrict or limit access to the critical components of your water system to authorized personnel only. This is the first step in security enhancement for your water system. Consider the following: • Issue water system photo identification cards for employees, and require them to be displayed within the restricted area at all times. • Post signs restricting entry to authorized personnel and ensure that assigned staff escort people without proper ID.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
3. Are facilities fenced, including wellhouses and pump pits, and are gates locked where appropriate?	Yes • No •	Ideally, all facilities should have a security fence around the perimeter. The fence perimeter should be walked periodically to check for breaches and maintenance needs. All gates should be locked with chains and a tamper-proof padlock that at a minimum protects the shank. Other barriers such as concrete "jersey" barriers should be considered to guard certain critical components from accidental or intentional vehicle intrusion.	
4. Are your doors, windows, and other points of entry such as tank and roof hatches and vents kept closed and locked?	Yes • No •	Lock all building doors and windows, hatches and vents, gates, and other points of entry to prevent access by unauthorized personnel. Check locks regularly. Dead bolt locks and lock guards provide a high level of security for the cost. A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place. Doors and hinges to critical facilities should be constructed of heavy-duty reinforced material. Hinges on all outside doors should be located on the inside. To limit access to water systems, all windows should be locked and reinforced with wire mesh or iron bars, and bolted on the inside. Systems should ensure that this type of security meets with the requirements of any fire codes. Alarms can also be installed on windows, doors, and other points of entry.	
5. Is there external lighting around the critical components of your water system?	Yes • No •	Adequate lighting of the exterior of water systems' critical components is a good deterrent to unauthorized access and may result in the detection or deterrence of trespassers. Motion detectors that activate switches that turn lights on or trigger alarms also enhance security.	
6. Are warning signs (tampering, unauthorized access, etc.) posted on all critical components of your water system? (For example, well houses and storage tanks.)	Yes • No •	Warning signs are an effective means to deter unauthorized access. "Warning - Tampering with this facility is a federal offense" should be posted on all water facilities. These are available from your state rural water association. "Authorized Personnel Only," "Unauthorized Access Prohibited," and "Employees Only" are examples of other signs that may be useful.	
7. Do you patrol and inspect your source intake, buildings, storage tanks, equipment, and other critical components?	Yes • No •	Frequent and random patrolling of the water system by utility staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol. Consider asking your local law enforcement agencies to conduct patrols of your water system. Advise them of your critical components and explain why they are important.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
8. Is the area around the critical components of your water system free of objects that may be used for breaking and entering?	Yes • No •	When assessing the area around your water system's critical components, look for objects that could be used to gain entry (e.g., large rocks, cement blocks, pieces of wood, ladders, valve keys, and other tools).	
9. Are the entry points to your water system easily seen?	Yes • No •	You should clear fence lines of all vegetation. Overhanging or nearby trees may also provide easy access. Avoid landscaping that will permit trespassers to hide or conduct unnoticed suspicious activities. Trim trees and shrubs to enhance the visibility of your water system's critical components. If possible, park vehicles and equipment in places where they do not block the view of your water system's critical components.	
10. Do you have an alarm system that will detect unauthorized entry or attempted entry at critical components?	Yes • No •	Consider installing an alarm system that notifies the proper authorities or your water system's designated contact for emergencies when there has been a breach of security. Inexpensive systems are available. An alarm system should be considered whenever possible for tanks, pump houses, and treatment facilities. You should also have an audible alarm at the site as a deterrent and to notify neighbors of a potential threat.	
11. Do you have a key control and accountability policy?	Yes • No •	Keep a record of locks and associated keys, and to whom the keys have been assigned. This record will facilitate lock replacement and key management (e.g., after employee turnover or loss of keys). Vehicle and building keys should be kept in a lockbox when not in use. You should have all keys stamped (engraved) "DO NOT DUPLICATE."	
12. Are entry codes and keys limited to water system personnel only?	Yes • No •	Suppliers and personnel from co-located organizations (e.g., organizations using your facility for telecommunications) should be denied access to codes and/or keys. Codes should be changed frequently if possible. Entry into any building should always be under the direct control of water system personnel.	
13. Do you have a neighborhood watch program for your water system?	Yes • No •	Watchful neighbors can be very helpful to a security program. Make sure they know whom to call in the event of an emergency or suspicious activity.	

Water Sources

In addition to the above general checklist for your entire water system (questions 1-13), you should give special attention to the following issues, presented in separate tables, related to various water system components. Your water sources (surface water intakes or wells) should be secured. Surface water supplies present the greatest challenge. Typically they encompass large land areas. Where areas cannot be secured, steps should be taken to initiate or increase law enforcement patrols. Pay particular attention to surface water intakes. Ask the public to be vigilant and report suspicious activity.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
14. Are your wellheads sealed properly?	Yes • No •	A properly sealed wellhead decreases the opportunity for the introduction of contaminants. If you are not sure whether your wellhead is properly sealed, contact your well drilling/maintenance company, your state drinking water primacy agency, your state rural water association, or other technical assistance providers.	
15. Are well vents and caps screened and securely attached?	Yes • No •	Properly installed vents and caps can help prevent the introduction of a contaminant into the water supply. Ensure that vents and caps serve their purpose, and cannot be easily breached or removed.	
16. Are observation/test and abandoned wells properly secured to prevent tampering?	Yes • No •	All observation/test and abandoned wells should be properly capped or secured to prevent the introduction of contaminants into the aquifer or water supply. Abandoned wells should be either removed or filled with concrete.	
17. Is your surface water source secured with fences or gates? Do water system personnel visit the source?	Yes • No •	Surface water supplies present the greatest challenge to secure. Often, they encompass large land areas. Where areas cannot be secured, steps should be taken to initiate or increase patrols by water utility personnel and law enforcement agents.	

Treatment Plant and Suppliers

Some small systems provide easy access to their water system for suppliers of equipment, chemicals, and other materials for the convenience of both parties. This practice should be discontinued.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
18. Are deliveries of chemicals and other supplies made in the presence of water system personnel?	Yes • No •	Establish a policy that an authorized person, designated by the water system, must accompany all deliveries. Verify the credentials of all drivers. This prevents unauthorized personnel from having access to the water system.	
19. Have you discussed with your supplier(s) procedures to ensure the security of their products?	Yes • No •	Verify that your suppliers take precautions to ensure that their products are not contaminated. Chain of custody procedures for delivery of chemicals should be reviewed. You should inspect chemicals and other supplies at the time of delivery to verify they are sealed and in unopened containers. Match all delivered goods with purchase orders to ensure that they were, in fact, ordered by your water system. You should keep a log or journal of deliveries. It should include the driver's name (taken from the driver's photo I.D.), date, time, material delivered, and the supplier's name.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
20. Are chemicals, particularly those that are potentially hazardous or flammable, properly stored in a secure area?	Yes • No •	All chemicals should be stored in an area designated for their storage only, and the area should be secure and access to the area restricted. Access to chemical storage should be available only to authorized employees. You should have tools and equipment on site (such as a fire extinguisher, drysweep, etc.) to take immediate actions when responding to an emergency.	
21. Do you monitor raw and treated water so that you can detect changes in water quality?	Yes • No •	Monitoring of raw and treated water can establish a baseline that may allow you to know if there has been a contamination incident. Some parameters for raw water include pH, turbidity, total and fecal coliform, total organic carbon, specific conductivity, ultraviolet adsorption, color, and odor. Routine parameters for finished water and distribution systems include free and total chlorine residual, heterotrophic plate count (HPC), total and fecal coliform, pH, specific conductivity, color, taste, odor, and system pressure. Chlorine demand patterns can help you identify potential problems with your water. A sudden change in demand may be a good indicator of contamination in your system. For those systems that use chlorine, absence of a chlorine residual may indicate possible contamination. Chlorine residuals provide protection against bacterial and viral contamination that may enter the water supply.	
22. Are tank ladders, access hatches, and entry points secured?	Yes • No •	The use of tamper-proof padlocks at entry points (hatches, vents, and ladder enclosures) will reduce the potential for of unauthorized entry. If you have towers, consider putting physical barriers on the legs to prevent unauthorized climbing.	
23. Are vents and overflow pipes properly protected with screens and/or grates?	Yes • No •	Air vents and overflow pipes are direct conduits to the finished water in storage facilities. Secure all vents and overflow pipes with heavy-duty screens and/or grates.	
24. Can you isolate the storage tank from the rest of the system?	Yes • No •	A water system should be able to take its storage tank(s) out of operation or drain its storage tank(s) if there is a contamination problem or structural damage. Install shut-off or bypass valves to allow you to isolate the storage tank in the case of a contamination problem or structural damage. Consider installing a sampling tap on the storage tank outlet to test water in the tank for possible contamination.	

Distribution

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

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
25. Do you control the use of hydrants and valves?	Yes • No •	Your water system should have a policy that regulates the authorized use of hydrants for purposes other than fire protection. Require authorization and backflow devices if a hydrant is used for any purpose other than fire fighting. Consider designating specific hydrants for use as filling station(s) with proper backflow prevention (e.g., to meet the needs of construction firms). Then, notify local law enforcement officials and the public that these are the only sites designated for this use. Flush hydrants should be kept locked to prevent contaminants from being introduced into the distribution system, and to prevent improper use.	
26. Does your system monitor for, and maintain, positive pressure?	Yes • No •	Positive pressure is essential for fire fighting and for preventing backsiphonage that may contaminate finished water in the distribution system. Refer to your state primacy agency for minimum drinking water pressure requirements.	
27. Has your system implemented a backflow prevention program?	Yes • No •	In addition to maintaining positive pressure, backflow prevention programs provide an added margin of safety by helping to prevent the intentional introduction of contaminants. If you need information on backflow prevention programs, contact your state drinking water primacy agency.	

Personnel

You should add security procedures to your personnel policies.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
28. When hiring personnel, do you request that local police perform a criminal background check, and do you verify employment eligibility (as required by the Immigration and Naturalization Service, Form I-9)?	Yes • No •	It is good practice to have all job candidates fill out an employment application. You should verify professional references. Background checks conducted during the hiring process may prevent potential employee-related security issues. If you use contract personnel, check on the personnel practices of all providers to ensure that their hiring practices are consistent with good security practices.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
29. Are your personnel issued photo-identification cards?	Yes • No •	For positive identification, all personnel should be issued water system photo-identification cards and be required to display them at all times. Photo identification will also facilitate identification of authorized water system personnel in the event of an emergency.	
30. When terminating employment, do you require employees to turn in photo IDs, keys, access codes, and other security-related items?	Yes • No •	Former or disgruntled employees have knowledge about the operation of your water system, and could have both the intent and physical capability to harm your system. Requiring employees who will no longer be working at your water system to turn in their IDs, keys, and access codes helps limit these types of security breaches.	
31. Do you use uniforms and vehicles with your water system name prominently displayed?	Yes • No •	Requiring personnel to wear uniforms, and requiring that all vehicles prominently display the water system name, helps inform the public when water system staff is working on the system. Any observed activity by personnel without uniforms should be regarded as suspicious. The public should be encouraged to report suspicious activity to law enforcement authorities.	
32. Have water system personnel been advised to report security vulnerability concerns and to report suspicious activity?	Yes • No •	Your personnel should be trained and knowledgeable about security issues at your facility, what to look for, and how to report any suspicious events or activity. Periodic meetings of authorized personnel should be held to discuss security issues.	
33. Do your personnel have a checklist to use for threats or suspicious calls or to report suspicious activity?	Yes • No •	To properly document suspicious or threatening phone calls or reports of suspicious activity, a simple checklist can be used to record and report all pertinent information. Calls should be reported immediately to appropriate law enforcement officials. Checklists should be available at every telephone. Sample checklists are included in Attachment 3. Also consider installing caller ID on your telephone system to keep a record of incoming calls.	

Information storage/computers/controls/maps

Security of the system, including computerized controls like a Supervisory Control and Data Acquisition (SCADA) system, goes beyond the physical aspects of operation. It also includes records and critical information that could be used by someone planning to disrupt or contaminate your water system.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
34. Is computer access "password protected?" Is virus protection installed and software upgraded regularly and are your virus definitions updated at least daily? Do you have Internet firewall software installed on your computer? Do you have a plan to back up your computers?	Yes • No •	All computer access should be password protected. Passwords should be changed every 90 days and (as needed) following employee turnover. When possible, each individual should have a unique password that they do not share with others. If you have Internet access, a firewall protection program should be installed on your computer. Also consider contacting a virus protection company and subscribing to a virus update program to protect your records. Backing up computers regularly will help prevent the loss of data in the event that your computer is damaged or breaks. Backup copies of computer data should be made routinely and stored at a secure off-site location.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
35. Is there information on the Web that can be used to disrupt your system or contaminate your water?	Yes • No •	Posting detailed information about your water system on a Web site may make the system more vulnerable to attack. Web sites should be examined to determine whether they contain critical information that should be removed. You should do a Web search (using a search engine such as Google, Yahool, or Lycos) using key words related to your water supply to find any published data on the Web that is easily accessible by someone who may want to damage your water supply.	
36. Are maps, records, and other information stored in a secure location?	Yes • No •	Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only. You should make back-up copies of all data and sensitive documents. These should be stored in a secure off-site location on a regular basis.	
37. Are copies of records, maps, and other sensitive information labeled confidential, and are all copies controlled and returned to the water system?	Yes • No •	Sensitive documents (e.g., schematics, maps , and plans and specifications) distributed for construction projects or other uses should be recorded and recovered after use. You should discuss measures to safeguard your documents with bidders for new projects.	
38. Are vehicles locked and secured at all times?	Yes • No •	Vehicles are essential to any water system. They typically contain maps and other information about the operation of the water system. Water system personnel should exercise caution to ensure that this information is secure. Water system vehicles should be locked when they are not in use or left unattended. Remove any critical information about the system before parking vehicles for the night. Vehicles also usually contain tools (e.g., valve wrenches) that could be used to access critical components of your water system. These tools should be secured and accounted for daily.	

Public Relations

You should educate your customers about your system. You should encourage them to be alert and to report any suspicious activity to law enforcement authorities.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
39. Do you have a program to educate and encourage the public to be vigilant and report suspicious activity to assist in the security protection of your water system?	Yes • No •	Advise your customers and the public that your system has increased preventive security measures to protect the water supply from vandalism. Ask for their help. Provide customers with your telephone number and the telephone number of the local law enforcement authority so that they can report suspicious activities. The telephone number can be made available through direct mail, billing inserts, notices on community bulletin boards, flyers, and consumer confidence reports.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
40. Does your water system have a procedure to deal with public information requests, and to restrict distribution of sensitive information?	Yes • No •	You should have a procedure for personnel to follow when you receive an inquiry about the water system or its operation from the press, customers, or the general public. Your personnel should be advised not to speak to the media on behalf of the water system. Only one person should be designated as the spokesperson for the water system. Only that person should respond to media inquiries. You should establish a process for responding to inquiries from your customers and the general public.	
41. Do you have a procedure in place to receive notification of a suspected outbreak of a disease immediately after discovery by local health agencies?	Yes • No •	It is critical to be able to receive information about suspected problems with the water at any time and respond to them quickly. Procedures should be developed in advance with your state drinking water primacy agency, local health agencies, and your local emergency planning committee.	
42. Do you have a procedure in place to advise the community of contamination immediately after discovery?	Yes • No •	As soon as possible after a disease outbreak, you should notify testing personnel and your laboratory of the incident. In outbreaks caused by microbial contaminants, it is critical to discover the type of contaminant and its method of transport (water, food, etc.). Active testing of your water supply will enable your laboratory, working in conjunction with public health officials, to determine if there are any unique (and possibly lethal) disease organisms in your water supply. It is critical to be able to get the word out to your customers as soon as possible after discovering a health hazard in your water supply. In addition to your responsibility to protect public health, you must also comply with the requirements of the Public Notification Rule. Some simple methods include announcements via radio or television, door-to-door notification, a phone tree, and posting notices in public places. The announcement should include accepted uses for the water and advice on where to obtain safe drinking water. Call large facilities that have large populations of people who might be particularly threatened by the outbreak: hospitals, nursing homes, the school district, jails, large public buildings, and large companies. Enlist the support of local emergency response personnel to assist in the effort.	
43. Do you have a procedure in place to respond immediately to a customer complaint about a new taste, odor, color, or other physical change (oily, filmy, burns on contact with skin)?	Yes • No •	It is critical to be able to respond to and quickly identify potential water quality problems reported by customers. Procedures should be developed in advance to investigate and identify the cause of the problem, as well as to alert local health agencies, your state drinking water primacy agency, and your local emergency planning committee if you discover a problem.	

Now that you have completed the "Security Vulnerability Self-Assessment Guide for Small Water Systems," review your needed actions and then prioritize them based on the most likely threats. A Table to assist you in prioritizing actions is provided in Attachment 1.

Attachment 1. Prioritization of Needed Actions

Once you have completed the "Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems," review the actions you need to take to improve your system's security. Note the questions to which you answered "no" on this worksheet. You can use it to summarize the areas where your system has vulnerability concerns. It can also help you prioritize the actions you should take to protect your system from vulnerabilities. Make sure to prioritize your actions based on the most likely threats to your water system.

Question Number	Needed Action	Scheduled Completion

Attachment 2. Emergency Contact List

We urge all public water systems to adopt an emergency response plan (ERP). Emergency plans are action steps to follow if a primary source of drinking water becomes contaminated or if the flow of water is disrupted. You can obtain sample ERPs from your state drinking water administrator, or from your state primacy agency.

This sample document is an "Emergency Contact List." It is an essential part of your ERP. It contains the names and telephone numbers of people you might need to call in the event of an emergency. This is a critical document to have at your disposal at all times. It gives you a quick reference to all names and telephone numbers that you need for support in the case of an emergency.

Filling out this Emergency Contact List reminds you to think about all of the people you might need to contact in an emergency. It also may encourage you to talk with these people about what you and they would do if an emergency were to occur.

Section 1. System Identification

Public Water System (PWS) ID Number		
System Name		
Town/City		
Telephone Numbers	System Telephone	Evening/Weekend Telephone
Other Contact Information	System Fax	Email
Population Served and Number of Service Connections	People Served	Connections
System Owner (The owner must be listed as a person's name)		
Name, title, and telephone number of person responsible for maintaining this emergency contact list	Name and title	Telephone

Section 2. Notification/Contact Information

Local Notification List

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Fire Department				
Police Department				
FBI Field Office				
Health Department				
Primacy Agency District Office				
Local Hospital				
Local Emergency Planning Committee				
EMS				
Local Pharmacy				
Local Nursing Homes				
Local Schools				
Local Prisons				
Local Government Official				
Local Hazmat Team				
Water System Operator				
Neighboring Water System				
Neighboring Water System				
Other				

Service/Repair Notification List

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Electrician				
Electric Utility Company				
Gas Utility Company				
Sewer Utility Company				
Telephone Utility Company				
Plumber				
Pump Specialist				
"Dig Safe" or local equivalent				
Soil Excavator/Backhoe Operator				
Equipment Rental (Power Generators)				
Equipment Rental (Chlorinators)				
Equipment Rental (Portable Fencing)				
Equipment Repairman				
Radio/Telemetry Repair Service				
Bottled Water Source				
Bulk Water Hauler				
Pump Supplier				
Well Drillers				
Pipe Supplier				
Chemical Supplier				
Local/Regional Analytical Laboratory				

State Notification List

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Drinking Water Primacy Agency				
Department of Environmental Protection (or state equivalent)				
Department of Health				
Emergency Management Agency				
Hazmat Hotline				

Media Notification List

ORGANIZATION	CONTACT NAME/TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Designated Water System Spokesperson				
Newspaper - Local				
Newspaper – Regional/State				
Radio				
Radio				
Radio				
Television				
Television				
Television				

Section 3. Communication and Outreach

Communication

Communications during an emergency poses some special problems. A standard response might be to call "911" for local fire and police departments. But what if your emergency had disrupted telephone lines and over-loaded cell phone lines? Talk with your state drinking water primacy agency about local emergency preparedness and solutions to these problems. Increasingly, state emergency agencies are establishing secure lines of communication with limited access. Learn how you can access those lines of communication if all others fail.

Outreach

If there is an incident of contamination in your water supply, you will need to notify the public and make public health recommendations (e.g., boil water, or use bottled water). To do this, you need a plan.

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

Attachment 3: Threat Identification Checklists

Water System Telephone Threat Identification Checklist

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

1. Types of Tampering/Threat:

- Contamination
- Biological
- Chemical
- Threat to tamper
- Bombs, explosives, etc.
- Other (explain)

2. Water System Identification:

Name:
Address:

Telephone:

PWS Owner or Manager's Name:

3. Alternate Water Source Available: Yes/No **If yes, give name and location:**

4. Location of Tampering:

- Distribution Line
- Water Storage Facilities
- Treatment Plant
- Raw Water Source
- Treatment Chemicals
- Other (explain):

5. Contaminant Source and Quantity:

7. Date and Time of Tampering/Threat:

8. Caller's Name/Alias, Address, and Telephone Number:

9. Is the Caller (check all that apply):

- Male
- Female
- Foul
- Illiterate
- Well Spoken
- Irrational
- Incoherent

10. Is the Caller's Voice (check all that apply):				
• Soft	• Calm	• Angry	• Slow	• Rapid
• Slurred	• Loud	• Laughing	• Crying	• Normal
• Deep	• Nasal	• Clear	• Lisping	• Stuttering
• Old	• High	• Cracking	• Excited	• Young

? Familiar (who did it sound like?)

? Accented (which nationality or region?)

11. Is the Connection Clear? (Could it have been a wireless or cell phone?)

12. 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	

13. Call Received By (Name, Address, and Telephone Number):

Date Call Received:

Time of Call:

14. Call Reported to: **Date/Time**

15. Action(s) Taken Following Receipt of Call:

Water System Report of Suspicious Activity

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

1. Types of Suspicious Activity:

- Breach of security systems (e.g., lock cut, door forced open)
- Unauthorized personnel on water system property.
-
-
- Presence of personnel at the water system at unusual hours
- Changes in water quality noticed by customers (e.g., change in color, odor, taste) that were not planned or announced by the water system
- Other (explain)

2. Water System Identification:

Name:
Address:

Telephone:

PWS Owner or Manager's Name:

3. Alternate Water Source Available: Yes/No **If yes, give name and location:**

4. Location of Suspicious Activity:

- Distribution Line
- Water Storage Facilities
- Treatment Plant
- Raw Water Source
- Treatment Chemicals
- Other (explain):

5. If Breach of Security, What was the Nature of the Breach?

- Lock was cut or broken, permitting unauthorized entry.

  Specify location

- Lock was tampered with, but not sufficiently to allow unauthorized entry.

  Specify location

- Door, gate, window, or any other point of entry (vent, hatch, etc.) was open and unsecured

  Specify location

- Other

  Specify nature and location

6. Unauthorized personnel on site?

Where were these people?

Specify location

What made them suspicious?

- Not wearing water system uniforms
- Something else? (Specify)

What were they doing?

7. Please describe these personnel (height, weight, hair color, clothes, facial hair, any distinguishing marks):

8. Call Received By (Name, Address, and Telephone Number):

Date Call Received:

Time of Call:

9. Call Reported to: **Date/Time:**

10. Action(s) Taken Following Receipt of Call:

Disclaimer

This document contains information on how to plan for protection of the assets of your water system. The work necessarily addresses problems in a general nature. You should review local, state, and federal laws and regulations to see how they apply to your specific situation.

Knowledgeable professionals prepared this document using current information. The authors make no representation, expressed or implied, that this information is suitable for any specific situation. The authors have no obligation to update this work or to make notification of any changes in statutes, regulations, information, or programs described in this document. Publication of this document does not replace the duty of water systems to warn and properly train their employees and others concerning health and safety risks and necessary precautions at their water systems.

Neither the Association of State Drinking Water Administrators, the National Rural Water Association, the U. S. Environmental Protection Agency, or the Drinking Water Academy, nor its contractor, The Cadmus Group, Inc., assume any liability resulting from the use or reliance upon any information, guidance, suggestions, conclusions, or opinions contained in this document.

Certification of Completion

A final step in completing the "Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems" is to notify the state drinking water primacy agency that the assessment has been conducted. Please fill in the following information and send this page only to the appropriate state drinking water primacy agency contact so that this certification can be included in the records that the state maintains on your water system.

Public Water System (PWS) ID: _____

System Name: _____

Address: _____

Town/City: _____ **State:** _____

ZIP Code: _____

Phone: _____ **Fax:** _____

Email: _____

Person Name: _____

Title: _____

Address: _____

Town/City: _____ **State:** _____

ZIP Code: _____

Phone: _____ **Fax:** _____

Email: _____

I certify that the information in this vulnerability assessment has been completed to the best of my knowledge and that the appropriate parties have been notified of the assessment and recommended steps to be taken to enhance the security of the water system. Furthermore, a copy of the completed assessment will be retained at the pubic water system, in a secure location, for state review as requested.

Signed_____ **Date**_____

Please send this page only to the attention of the State Drinking Water Primacy Agency.

United States Environmental Protection Agency
Office of Solid Waste and Emergency Response (5104)
EPA 550-F-01-005
August 2001
www.epa.gov/ceppo

LEPCs and Deliberate Releases:

Addressing Terrorist Activities in the Local Emergency Plan

In recent years, the threat of terrorist incidents involving chemical and biological materials has increased. Local emergency planning committees (LEPCs) should consider the possibility of terrorist events as they review existing plans and consider how to incorporate counter-terrorism (CT) measures into their plans. CT planning and preparedness is often an extension of existing activities, rather than a totally new effort. This factsheet discusses how LEPCs can incorporate CT issues when they review and update their local plans. This factsheet builds on the National Response Team's Hazardous Materials Emergency Planning Guide (NRT-1) and supersedes "Thinking abut Deliberate Releases: Steps Your Community Can Take."

FACTSHEET

BUILD ON CURRENT ACTIVITIES

Local emergency planning committees (LEPCs), established under the Emergency Planning and Community Right-to-Know Act (EPCRA), prepare and maintain comprehensive emergency plans. These plans address the extremely hazardous substances listed under EPCRA as well as thousands of hazardous chemicals for which OSHA requires Material Safety Data Sheets. Many LEPCs are already addressing CT, even if they do not use the word "terrorism." If you have developed a plan for possible accidental releases of chemicals in your community, you can use the same general planning principles for deliberate releases caused by terrorists. You may need to spend some time considering biological agents. This factsheet includes some suggestions for how you can modify your current activities to include deliberate chemical and biological releases.

MAINTAIN BROAD-BASED MEMBERSHIP

LEPC membership includes a wide variety of stakeholders, such as elected State and local officials; police; fire, civil defense, public health, environmental, hospital, and transportation officials; representatives of facilities where chemicals are stored or used; community groups; public works departments; and the media. Identify any specific roles each of these groups might have in the event of a terrorist attack. In addition, you might add a few new members who would bring specific expertise during a release involving biological agents (e.g., the coroner, morticians, chemistry and biology labs, university experts).

UPDATE AND REVISE YOUR PLANS

LEPCs should review their emergency response plans annually. Before you begin specific consideration of CT issues, ensure that your emergency plan is up-to-date. Simply adding CT materials to an outdated plan will not create an effective emergency plan. For example, review your plan for outdated contact information, unique hazards presented by facilities that may have been constructed after the emergency response plan was first written, or new public works facilities. Also review the annual inventory reports filed under EPCRA Section 312 to determine if new chemicals or hazards are present in your community.

In addition, check Risk Management Plans submitted by facilities in your community to ensure that you address the specific hazards identified by each facility. After you have generally updated your plan, consider adding information and procedures related to potential terrorist incidents involving weapons of mass destruction (WMD). Table 1 (page 6) defines each type of WMD and explains the consequences and response difficulties associated with each type.

One overall difference in dealing with a WMD incident is that law enforcement officials will be involved in the response as investigators. Officials from local, State, and Federal agencies will be on the scene of an incident to collect evidence and interview survivors. Their priorities may create emergency response coordination challenges that your LEPC should address in its plan.

This portion of the factsheet suggests changes you can make to specific sections of your emergency plan.

Emergency Contact Information

In the event of a terrorist incident, rapid and secure communications will be crucial to ensure a prompt and coordinated response. Your plans should include current contact information for fire, emergency medical services (EMS), law enforcement, medical, and other local departments and supporting organizations. Contact information for State officials, including those at public health agencies, the State Emergency Response Commission (SERC), State Police, and emergency management agencies also should be included.

The emergency assistance telephone roster in your emergency response plan should include regular phone numbers, cell phone numbers, pager numbers, and other emergency contact information for those individuals (Federal, State, local, and private sector) who have specific CT functions. The National Response Center (NRC) continues to be the sole Federal point of contact for reporting oil and chemical spills, and now provides the service of the Chemical and Biological Hotline. The NRC telephone number (800-424-8802) should be part of your emergency plan. NRC Duty Officers take reports of actual or potential domestic terrorism and link emergency calls with the Department of Defense (DOD) for technical advice on dealing with weapons of mass destruction and with the FBI to initiate the Federal response actions. The NRC also provides reports and notifications to other Federal agencies as necessary. All local plans should also include contact information for the local FBI Field Office.

Response Functions

Incident Command/Unified Command. Your emergency plan should address direction and control of responders in the event of terrorist attack. Local responders respond to an incident scene and should notify local, State, and Federal authorities if terrorism appears to be involved. Local response authorities (such as a senior fire or law enforcement official) should establish control of the incident scene. The Incident Command System (ICS) that is initially established will likely transition into a Unified Command (UC). The UC structure used at the scene will expand as mutual-aid partners, and State and Federal responders arrive to assist with response operations.

The FBI is the overall Lead Federal Agency (LFA) for a domestic terrorist incident involving WMD and will lead the crisis management activities (including law enforcement activities) of the response.

The Federal Emergency Management Agency (FEMA) is the lead agency for coordination of Federal support to State and local responders during consequence management activities of the response. Although the FBI is always involved in response to a credible terrorist threat or attack, FEMA support is provided only after a Presidential declaration, typically after State and local agencies request their assistance. Consequence management includes measures to protect public health and safety after an explosion or release; restore essential government services; and provide emergency relief to governments, business, and individuals. When crisis management activities have been completed, the U.S. Attorney General may transfer the overall Lead Federal Agency role to FEMA. EPA, the Department of Health and Human Services (DHHS), and DOD also have specific CT-related functions. EPA's role in counter-terrorism activities is described in a factsheet by that name, available at www.epa.gov/ceppo/ct-publ.htm#factsheet.

Public Information. Rapid and secure communications help to ensure a prompt and coordinated response to terrorist activities. Therefore, strengthening communications among emergency responders, law enforcement officials, clinicians, emergency rooms, hospitals, and mass care providers is extremely important. Your emergency plan should include the use of accurate and timely public notification measures and warning systems in the event of a terrorist attack. Work in advance with local news media representatives to ensure their cooperation at the time of an incident. Ongoing communication of accurate and up-to-date information will help calm fears and limit the effects of the attack. The FBI will establish a Joint Information Center (JIC) to coordinate the collection and dissemination of public information.

EPA's Role in the Federal Response Plan

The multi-agency disaster response program that helps states during and after a disaster is the Federal Response Plan (FRP), which groups Federal assistance into 12 functional areas called Emergency Support Functions (ESFs). EPA is the primary agency for ESF 10, Hazardous Materials, which provides for a coordinated response to large-scale releases of hazardous materials by incorporating the response mechanisms of the National Contingency Plan (NCP). EPA assists in determining what sort of hazardous substance may be, or has been, released in a terrorist incident, and follows up with response to the incident, assisting with environmental monitoring, decontamination, and long-term site cleanup.

Activities of human services organizations, such as the Red Cross, should be included in the emergency plan. Among other activities, these organizations may use public information systems to provide human services information to the community, perform crisis counseling, provide insurance information and assistance, and provide translation services.

Public and First Responder Health and Safety. Your emergency plan should address public health and medical issues as they relate to terrorist events. The plan should include procedures to identify and treat victims, store and distribute antidotes, and handle fatalities. Mass care issues that may be different during a terrorist WMD event include decontamination, multihazard/multiagent triage, mortuary services, and notifying and working with families of any fatalities.

The emergency plan should also consider the personal safety of emergency responders in the event of a terrorist attack. A terrorist chemical, biological, or radiological release may not be immediately known or apparent. Caregivers, emergency response and law enforcement personnel, and other first responders are in danger of becoming casualties before anyone realizes that a crime has occurred. Incidents could escalate quickly from one scene to multiple locations and jurisdictions.

The emergency plan should be flexible enough to accommodate evacuation or in-place sheltering. Evacuation may be required outside the perimeter of the scene to guard against further casualties from contamination by a released agent or from the possibility of additional WMD. In-place sheltering may be required if the area must be quarantined or if people are safer in a particular location.

Hazards Analysis

The hazards analysis section of an emergency plan should identify potential hazards, determine the vulnerability of an area as a result of hazards, and assess the risk of a hazardous materials release or spill. In the identification step, you should consider explosive, chemical, biological, and nuclear WMD as potential hazards.

As you conduct your hazards analysis, identify potential targets and review their vulnerability to attack. Consider the population, accessibility, impact on daily life, economic impact, and symbolic value of areas at risk. Terrorists and criminals who want to attack a particular group based on a conflict with their personal beliefs might target Federal, State, or local government offices and facilities, health clinics, or religious structures. Those who want to cause maximum casualties might target public gathering places (such as sports and entertainment complexes or tourist attractions), modes of transportation (such as buses and trains – including subways), routes of transportation(including bridges), or transportation facilities (such as airport terminals). In order to damage infrastructure and interrupt day-to-day functions, a terrorist might target utilities or water and wastewater treatment plants. LEPCs should also consider emergency procedures in the event of

multiple, or simultaneous, terrorist attacks. Terrorists might target first responders (e.g., fire houses, police department offices, response vehicles, and individuals) to hinder them from responding to another terrorist incident. A terrorist may seek to transform a target into a weapon by focusing on facilities that handle explosive, toxic, or volatile chemicals.

Because most public buildings and public areas must be accessible to everyone, they are highly vulnerable to attack. Other facilities, such as water treatment plants and industrial facilities, especially those with chemical or explosives storage, should have site security measures in place. You may want to discuss site security measures with these facilities to ensure that they are adequately protected. You may want to ask the facility the following questions:

- Is the facility or critical equipment and chemicals protected by fences or buildings?
- Are there systems to detect intruders (e.g., patrols, video surveillance)?
- Are there alarm systems?
- Is access to the critical areas controlled?

Do not, however, include details of the security systems in your emergency plan, because it is available to the general public.

Public works facilities and workers will assume a support role, if so requested by State and local agencies. This support role might include damage assessment, debris clearance, search and rescue, traffic control, restoration of lifeline systems, building inspection, provision of potable water and sanitation services, and flood control.

For more information on site security, read CEPPO's Chemical Safety Alerts *Chemical Accident Prevention: Site Security* (EPA K-550-F00-002) and *Anhydrous Ammonia Theft* (EPA-F-00-005), available at www.epa.gov/ceppo/p-small.htm#alerts.

Mitigation Procedures and Ongoing Assessment

Mitigation procedures and ongoing assessment involve consequence management activities to assess and protect the public from further exposure to hazards presented by terrorist activities. Public health officials, hazmat teams, coroners and/or medical examiners, and criminal investigators should work together to mitigate residual hazards as well as identify potentially large numbers of fatalities. Federal assistance should be available to support this task. Ongoing assessment activities may include environmental sampling of air, water, and soil, and insect and animal screening for chemical, biological, or radiological agents.

The criminal investigation of a terrorist attack will be a joint effort that includes many agencies. In the event of a biological attack, an epidemiological investigation may also be performed to assess the distribution of cases and sources of outbreak. The emergency plan could include a checklist of basic questions to ask when conducting interviews with victims in hospitals, sick officers, and other individuals in affected population groups. (It may be necessary to train people in how to ask such questions appropriately in stressful circumstances.)

Equipment

Your emergency response plan should include standard operating procedures on when to use specialized WMD response equipment. Local responders should be trained to use, maintain, and calibrate this specialized equipment. The Department of Justice's Office for State and Local Domestic Preparedness Support (OSLDPS) provides equipment grants and technical assistance to eligible communities. Visit their website at http://www.ojp.usdoj.gov/terrorism/funding.htm for more information and grant application kits.

Training

The 1996 Nunn-Lugar-Domenici (NLD) legislation authorized funding to form a Domestic Preparedness (DP) training initiative. This initiative was recently transferred from DOD to the Department of Justice (DOJ), and includes a range of specialized courses, from basic awareness to discipline-specific advanced level training and exercises.

Training is available for identified cities and is directed at a broad spectrum of emergency responders from a variety of response disciplines, including fire, hazardous materials, law enforcement, emergency medical services, public health, emergency management, and public works. Additional advanced level courses involving the use of real-time experiences, live agents, and explosives are taught at cutting edge training facilities.

The NLD DP Program also includes three exercises: a chemical weapons tabletop, a biological weapons tabletop, and a chemical weapons full-scale exercise. Both types of exercises allow participants to test their knowledge and training, as well as increase the overall preparedness of responders across the jurisdiction.

FEMA independently offers the following:

- Course materials on WMD and preparedness and response for terrorist incidents that can be downloaded from www.fema.gov/emi/termng.htm.
- A terrorism consequence management course at their Mount Weather Emergency Assistance Center. Contact the training officer in your State Training Office of Emergency Services for information on course schedules and application procedures. A list of offices and contact information is located at www.fema.gov/emi/sttrgo.htm.
- Information on the Incident Command System (ICS) training conducted by each State Training Office of Emergency Services. Visit www.fema.gov/emi/nrcrs.htm for more details.
- In conjunction with the National Fire Academy, an independent study course in emergency response to terrorism, located at www.fema.gov/emi/crslist.htm.

RESOURCES

LEPCs seeking assistance in terrorism-related emergency planning should begin with their SERCs. The SERC can direct LEPCs to appropriate assistance at the national and State level, and may be able to facilitate LEPCs in a given region working together to address possible terrorist activities.

There are currently many Federal agencies involved in some aspect of counter-terrorism. Many of these agencies support websites. Because of the continual changes in the world of CT, however, many websites become outdated or are even discontinued without warning. Therefore, we recommend that LEPCs consult EPA's Chemical Emergency Preparedness and Prevention Office (CEPPO) website at www.epa.gov/ceppo/cntr-ter.html. This address is updated every two months and includes the latest links to the following types of information: Federal departments and agencies, health and medical, technical information and resources, and international sources.

For More Information:
Contact the EPCRA Hotline at:
(800) 424-9346 or (703) 412-9810
TDD (800) 553-7672
Monday - Friday, 9 AM to 6 PM, EST

Visit the CEPPO Home Page at:
www.epa.gov/ceppo/

Table 1
Weapons of Mass Destruction (WMD) Definitions, Consequences, and Response Difficulties

Type of WMD	Definition (according to Title 18, USC 2332a)	Consequences	Response Difficulties
Explosives	Any explosive, incendiary, or poison gas bomb, grenade, rocket ... missile ... mine or device similar to the above	Deaths, injuries, damaged structures	Similar to that of other explosions and large fires
Chemical	Poison gas, blister gas	Deaths, injuries, possible contamination, possible long-term effects	Similar to accidents planned for in current LEPC emergency response plan, but could be more extensive in effect (e.g., VX release in a crowded convention center or school)
Biological	Any weapon involving a disease organism	Deaths, injuries, contamination, long-term, far-reaching geographic effects	Agents may be unknown; Locations may vary and multiply as people travel
Nuclear	Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life	Deaths, injuries, contamination, possible long-term, far-reaching effects	Similar to that of other explosions and large fires plus radiation; could have long-term far-reaching effects

DRINKING WATER SYSTEM

EMERGENCY RESPONSE GUIDEBOOK

August 2001

Kim Dyches
Emergency Response Coordinator
Division of Drinking Water

TABLE OF CONTENTS

	Page
INTRODUCTION	3
NORMAL PROBLEMS	4
ORGANIZATION	4
Lines of Authority	
Classification of the Emergency or Disaster	
Facility Damage Assessment	
Map of the Drinking Water System and Facilities	
IMPLEMENTATION	9
General Information	
Emergency Medical Facilities	
Emergency Assignments	
Emergency Personnel Roster	
Fire Fighting / Law Enforcement Agencies	
PRIORITIZE WORK/REPAIR NEEDED	11
General Information	
Possible Emergency Equipment and Material Rosters	
Maps of Critical Water Needs by Service Areas	
DISPATCHING PERSONNEL AND EQUIPMENT	13
Emergency Assignments	
Emergency Personnel Roster	
REQUESTS/RESPONSE FOR EMERGENCY AID	14
Authorization to Request and to Provide Assistance	
Commercial Suppliers of Equipment and Materials	
Neighboring Agencies and Agreements	
PUBLIC NOTIFICATION/PRESS RELEASES	14
General Information	
News Media Contacts	

INTRODUCTION

The purpose of this guidebook is to assist the drinking water system management prepare a disaster and/or emergency response plan. It is not meant to be a guide for routine complaints or system maintenance problems. These issues should be dealt with by policy established by the drinking water system management.

A disaster or emergency can strike any drinking water system at any time. In preparing your response plan keep in mind that when, ***not if***, an emergency or disaster occurs, drinking water will become one of the top priorities in emergency medical services, fire fighting, sanitation, and general recovery of the emergency or disaster.

In designing your response plan keep it as simple and practical as possible. A complicated plan will only add to the confusion, and that's exactly what you don't want to happen!

After you have designed your drinking water system's "Emergency Response Plan," train the system personnel. Mistakes made during training and rehearsals don't cost much, ***but mistakes made during the "real thing" could easily cost lives!*** Re-training or rehearsing the emergency response plan every 6 months will help new personnel become familiar with their role in the emergency plan, and will remind the experienced personnel of their role and perhaps identify areas of the plan that need improvement. Tabletop exercises are excellent ways to rehearse each individual role.

There are excellent training resources available to assist you in developing your emergency response plan. The American Water Works Association publishes a manual entitled, ***Emergency Planning for Water Utility Management (M19)***, which is available as well as an excellent video entitled, ***Emergency Planning: The Big Picture for Water Utilities***. These and other helpful publications are available by contacting the American Water Works Association at 1-800-926-7337.

The Rural Water Association of Utah, the Intermountain Section of the American Water Works Association, and the Division of Drinking Water can provide additional assistance.

NORMAL PROBLEMS

During the course of normal operations a drinking water system will have problems--some minor, some major.

Take, for example, a major backflow incident:

- What should I do? Should I notify the public? If yes, do I just notify the area that is contaminated or everyone on the whole system? And how do I go about putting out an emergency notice to my consumers?

- Should I flush the system now, or isolate it, or get sample results first? Should I let anyone know about the problem (Local and/or State Health Departments), or should I keep it to myself?

These are the questions that should be thought out now! And a plan must be drawn up ***and used*** when a problem occurs that will directly affect the safety of the drinking water system. This booklet will help design such a plan, and help you plan for a major emergency or disaster.

ORGANIZATION

Lines of Authority

Initial reaction to any emergency or disaster will be confusion. Therefore, a pre-planned line of authority, including alternates in case the key people are unavailable, must be designed and ready for immediate implementation, with those individuals in these positions being aware of their designated authority during an emergency operation.

An office or area should be set aside and designated as an Emergency Command Center. The Command Center should be equipped with telephones, radios, drinking water system maps and records and any other emergency equipment, which may be needed. During any emergency situation the Emergency Command Center would be activated and the personnel listed below would report for duty to the Command Center rather than their individual offices.

Types of authority positions could include:

1. *Emergency Coordinator:* This individual would coordinate all emergency actions, water system personnel and equipment within the drinking water system. The Emergency Coordinator will also coordinate with the law enforcement, fire fighting, medical personnel, and any other requests for aid, volunteer efforts, mutual assistance (other neighboring water system personnel or equipment and any contracted private assistance) (the Emergency Coordinator is usually the Water Superintendent or equal).

2. *Public Relations Coordinator:* This individual would be responsible for news releases to the media, issuing emergency information bulletins to the public, and act as liaison between the drinking water system and general public in answering questions and addressing concerns (the Public Relations Coordinator is usually the Mayor or Public Relations Specialist).
   It is essential that the Emergency Coordinator and the Public Relations Coordinator work closely together. It is also important that they be separate individuals because at the onset of any emergency a lot of people need to be mobilized in a coordinated effort (directed by the Emergency Coordinator) and the press and public need answers to their questions. Initially the Public Relations Coordinator will probably only be able to say, "This event has occurred, and we are taking the following actions, (list the actions), and we will report more as we know more". The Emergency Coordinator will then feed information from the field to the Public Relations Coordinator, who then responds to the questions and concerns of the public and news media.

3. *Assessment Coordinator:* This individual would coordinate the inspection of all drinking water system physical facilities to determine the degree of damage to the facility and in coordination with the Emergency Coordinator, prioritize the repair, replacement or abandonment of any system physical facilities.

4. *Crew Foreman:* This individual would coordinate, supervise and schedule personnel, equipment and materials to facilitate the repair or replacement of critical drinking water system facilities which have been identified and prioritized by the Assessment and Emergency Coordinators. There may be several Crew Foremen if there are multiple sites of concern, or multiple crews working in the field.

For some very small water systems, all of these functions may be the responsibility of

one individual. In those situations, Board or Council members, clerical staff or even other interested volunteers must be trained and knowledgeable about the system and the response plan in the event that the operator is unavailable to respond during an emergency.

Classification of the Emergency or Disaster

Classifying the degree of the emergency or disaster will help in properly prioritizing activities and speeding the response time to implement the response plan. The classification phase, conducted during a training exercise will also be helpful in designing the training of the drinking water system personnel in their part of the emergency plan.

Remember that mistakes made during the training don't cost much, but mistakes made during the "real thing" could cost lives!

The classification of the emergency or disaster will be the decision of the Emergency Coordinator, which will be communicated by radio and/or telephone to the other personnel of the drinking water system:

LEVEL I - NORMAL (ROUTINE): Personnel and equipment presently on duty can handle system problems. The "Emergency Command Center" not activated or manned.

LEVEL II - ALERT (MINOR EMERGENCY): Personnel and equipment presently on duty can handle system problems, but may require off duty or additional personnel to be put on alert, be re-routed to other than their normal working areas, or work additional shifts. The "Emergency Command Center" activated and manned.

LEVEL III - MAJOR EMERGENCY: Problems somewhat beyond the capabilities of the drinking water system personnel and equipment, and may require a "Declaration of Emergency" to authorize shortcut procedures. Requires employees to work additional shifts and may need additional assistance of personnel and equipment, either by mutual aid or private contracts. The "Emergency Command Center" activated and manned.

LEVEL IV - DISASTER: Problems clearly and immediately beyond the capability of the drinking water system. Recovery time will exceed one week, costs will be great,

large amounts of assistance of personnel and equipment by mutual aid or private contracts will be required, extended shifts will be needed for at least one week. A "Declaration of Emergency" will be required; the "Emergency Command Center" activated and manned.

Facility Damage Assessments

The "Assessment Coordinator" will determine the preliminary damage assessment priorities. The physical status of *all* physical facilities must be assessed. The need to repair, replace, or abandon drinking water physical facilities is required at this point. Be sure to include an estimate of cost, including manpower and equipment, to restore the facility in order to help prioritize the repair work.

The Assessment Coordinator must consider the possible after effects of the repairs or replacement of the facilities, on the integrity of the drinking water system itself after the emergency. For example, a structural repair to a water storage tank may introduce chemical or bacteriological contamination into the drinking water.

Reservoirs: Check for seepage, leaks, cracks or problems with the reservoir itself. Landslides, embankment slumps, broken inlet-outlet pipes or underdrains could effect the stability of the reservoir itself. Estimate the remaining amount of water in the reservoir.

Deep Wells and Booster Pumps: Check power supplies, pump or motor failures, physical damage to piping or electrical controls. Check the building or structure for integrity of pump operations.

Distribution and Transmission pipelines: Check all air vacuum relief valves. Check for visible leaks, cracks, breaks, and pressure loss in pressure zones. Check automatic valve failure (pressure reducing, pressure sustaining, pressure relief, high altitude, solenoid controlled, etc) and all other facilities that would be useful in gauging the integrity of underground piping, including fire hydrants. Identify pressure zone valves and isolation valves in order to supply, divert, or isolate drinking water in the system.

Drinking Water Treatment Plant: Check the quality of the influent and surrounding water shed for signs of chemical spills or releases, and any changes in the raw

water quality, dosage rates of chemicals, disinfection levels and all equipment. Also check for any structural damage within the facility along with the power supply, electrical equipment and the condition of the mechanical equipment.

After the completion of the preliminary damage assessment the Assessment Coordinator and the Emergency Coordinator will then decide which damaged drinking water facility receives priority repair or replacement. This process of assessment and response coordination is usually quite informal and is facilitated by the nature of the emergency. For example, a staff member is informed of, or discovers a situation; he then reports it to his supervisor (the Emergency Coordinator) who then agrees with or expands the assessment and directs the employee to do some action. The Emergency Coordinator then works on mobilizing additional resources and sets up the command center.

The determination of priorities should be based on:

1. The unique design of the drinking water system.
2. Medical/emergency care requirements.
3. Drinking water and sanitation needs of the public.
4. Fire fighting requirements.
5. How much good drinking water is remaining in the system reservoirs?
6. How to transport that water to where it is needed the most.

Pre-planning in this area could save the Assessment and Emergency Coordinators a lot of worry and hassle. If the situation is thought through clearly now, rather than during an emergency, much better decisions will be made.

MAP OF THE DRINKING WATER SYSTEM AND FACILITIES

In your emergency response plan, inventory your system and identify the elements that would be most susceptible to damage in any emergency situation. Consider the different types of emergencies such as earthquakes, floods, explosions, traffic accidents, sabotage, and fires. Also consider susceptible facilities such as: underground storage tanks, booster pump stations, high pressure zones or areas, or any other facilities that are readily susceptible to damage and are also of a high repair priority. Also identify pressure zone valves and isolation valves to be used to divert, supply or isolate drinking water.

IMPLEMENTATION

General Information

Announce to employees the activation of the Emergency plan, using radio, telephone, or by any other means and have employees meet at their designated staging areas.

Maintain a ***written*** log of messages and directives given during the emergency. This will help reduce confusion in the Emergency Operation Center and will also help in preparing the "After Emergency Follow-up Report", particularly if outside aid and assistance were requested.

Plans should be in place for the use of volunteers who may show up to help. Water system personnel should supervise volunteer work so that it can be done safely.

Document the cost for supplies and equipment. Tracking all of the labor performed by system personnel and volunteers is essential in the event an emergency is declared a disaster. This will help in receiving reimbursement money from State and Federal agencies.

Individuals responding to telephone and other contacts must be briefed on the proper response to give customers and concerned callers. All information released must be coordinated through the Emergency Coordinator. Everyone contacting the agency should receive the same information.

Ensure that radio communication is limited to vital messages only. Direct and control radio channels by stating call number and announcing an emergency message is to be sent.

Liaison personnel should report to the proper Emergency Operation Center (City, County, District). Maintain communication with the EOC by making status reports at least once per hour during the emergency, however, some emergencies may require more frequent reporting.

Emergency Medical Facilities

Maintain a roster of emergency medical treatment facilities in your area for ease of maintaining drinking water supplies, transporting drinking water from another source, or transporting injured personnel. A source of drinking water (even bottled water) will be critical to emergency medical centers.

Emergency Assignments

Ensure all personnel are aware of the drinking water system emergency response plan, and their part in it. Personnel must be aware of the level of the emergency, staging areas, lines of authority, and their direct place within the organization.

In the event of an emergency or disaster, the employees will naturally take care of their families first. Provisions should be made to assure water system personnel that their immediate family members have been accounted for. Plans should include assisting employee's families in getting food, water, shelter and clothing. Employees will be better focused once their families have been taken care of.

Staging areas should be set up so all personnel know where to report to work when they are able. Alternate areas should be assigned in the event a staging area is unsafe.

Emergency Personnel Roster

Maintain a roster of personnel within the drinking water system for emergency response notification. This list must be updated with the individual's name, address, phone number, emergency job assignment, and primary staging area.

Issue identification cards to those employees who may require access to private property, cross police or fire lines, or who are authorized to request or grant mutual aid. This roster will ensure proper lines of authority and communication is being used.

During the emergency, be sure ALL personnel working in the drinking water system are placed on a duty roster, and appropriately tracked. This will ensure that they are being rotated for rest and food, and to keep track of where they are within the drinking water system should they be needed elsewhere, or should they get injured and need help.

Fire Fighting/Law Enforcement Agencies

Maintain an updated listing of contacts within the local and neighboring fire fighting and law enforcement agencies, including their phone numbers and Emergency Operation Center personnel, radio frequency, radio call signs and the EOC phone numbers. This listing and coordination will be critical for cooperation of the limited facilities and materials, particularly personnel, during the emergency.

Maintain a current State and County Emergency Operation Center listing within your area. These agencies can help provide technical expertise, personnel, equipment and laboratory liaison.

PRIORITIZE WORK/REPAIR NEEDED

General Information

Be aware that fire-fighting activities will seriously deplete drinking water supplies. This may mean that drinking water will have to be imported from other systems into your area. It can also mean that contamination could be drawn into the drinking water system due to low or negative pressures. Consequently, the drinking water system management should consider this situation and plan for contingencies. As a worse case scenario, ***preserve the remaining water in storage!*** If need be, limit fire fighting capabilities in critical water shortage areas. The fire fighters won't like it, but drinking water is top priority.

Isolate areas that will take the longest to restore service and arrange for emergency water distribution:

- Establish drinking water distribution points and ration remaining water.
  - Locate bottled water distribution points to serve immediate water needs.
  - Arrange for trucks and trailers with water tanks (National Guard Units) for water distribution.

Identify the areas that can be served with a minimum of repair and then prioritize the other service areas that will need more extensive repair.

Every area has its own general type of emergency or disaster, earthquake, periodic flooding and etc. Therefore, you can identify areas that will be more susceptible to damage and even, to an extent, what type of damage the area will have.

Set priorities on the repair work. In so doing, consider the following:

- Prepare a plan to restore each service area.
- Plan to restore the service areas one by one, not the entire system at once.

- Get input and advice from other agencies (local, county and state) on essential uses.
- Take into account the condition of the transmission lines from the water sources.
- Keep in mind the need for fire fighting (even if it will be limited).
- Determine if imported water is available and how to distribute it.
- When the repairs exceeds the capabilities of your water system, notify the County or State Emergency Operation Center for assistance and coordination of assistance.

Possible Emergency Materials and Equipment

Maintain a current listing of those agencies, private companies or manufactures within your local area that can provide assistance during an emergency. This assistance can be in materials, equipment, vehicles and/or trained personnel. Maintain emergency agreements or contracts with these private companies so they are aware of their part of your emergency plan, and that basic costs of materials or equipment have been agreed upon, and who is authorized to activate those agreements or contracts. Maintain these agreements and contracts at the Emergency Operation Center for quick access. Willingly agree to assist neighboring water utilities in the event they have an emergency.

Maps of Critical Water Needs by Service Areas

Maintain an updated map of critical water needs within each service area and maintain the maps at the Emergency Operations Center. The maps should include the locations of fire fighting equipment, medical facilities, preplanned imported water distribution points, pressure zones, booster pumps stations, and drinking water sources.

DISPATCHING PERSONNEL AND EQUIPMENT

Emergency Assignments

Ensure every affected individual is aware of the drinking water system's emergency response plan and their part in it. Personnel must be aware of the level of emergency, staging areas, lines of authority, and their direct involvement within the emergency organization.

The Emergency Coordinator will advise the Crew Foremen as to the work assignments. The Crew Foremen will assign additional personnel (including volunteers) to the work crews, as needed.

Emergency Personnel Roster

Maintain a list of personnel within the drinking water system's emergency response plan and their slot within the emergency organization. This list must be kept updated with the individuals home phone number, address, and primary and alternate staging areas.

Issue identification cards to those employees who may require access to private property, cross fire or police lines, or those who are authorized to request or grant mutual aid and assistance. This procedure ensures proper lines of authority are being used.

Ensure that ***every person*** working within the drinking water system, including all volunteers, are placed on a personnel roster which is organized by work crews, and maintained at the Emergency Operation Center. This will help ensure all personnel are being rotated for rest, food, and to keep track of where they are within the system should they be needed elsewhere, or if they get injured.

REQUESTS/RESPONSE FOR EMERGENCY AID

Authorization to Request and to Provide Assistance

Pre-authorization of the position to request or to provide emergency assistance within the drinking water system would enable the Emergency Coordinator the latitude to ensure all possible areas of assistance have been involved within the response effort. The elected officials of the drinking water system should do this pre-authorization, with advice from legal council. It should be passed as an ordinance or policy so that the designated person has the authority in writing for confirmation if needed.

Commercial Suppliers of Equipment Materials

A listing of commercial suppliers of equipment and materials within your local area should be kept up-to-date and available to the Emergency Coordinator.

Neighboring Agencies and Agreements

A listing of neighboring drinking water systems and government agencies and contact people within them should be kept at the Emergency Operation Center. This list should include the types of specialized equipment, vehicles and trained crews that would be available if needed during an emergency. A bilateral agreement of Emergency Aid and Mutual Assistance should be negotiated with these systems and agencies.

PUBLIC NOTIFICATION/PRESS RELEASES

General Information

The release of information to the public and news media must be accurate and issued through the Public Relations Coordinator. The type of information given will vary with the drinking water system and the type of emergency, but a generalized list must include:

- Centralized New Releases and statements to avoid contradictory or confusing statements.
- When responding to questions make only factual responses, ***never guess, speculate or exaggerate.*** If you don't know the answer to a question, tell the reporters "I don't know", and then give them an indication of when

you might know or an explanation as to why the answer is unknowable.

- Inform the public of any possible contamination of the drinking water and resulting boil orders.
- Inform the public of the availability and location of alternate sources of drinking water.
- Implement drinking water rationing.
- Arrange for an ***escorted*** news media tour. Only those media representatives who have proper identification should be allowed within the work areas or facilities, and only with an escort. These tours must be pre-authorized by the Emergency Coordinator and Public Relations Coordinator. For safety reasons, do not allow the news media to wander around the work sites.

RECOVERY CHECKLIST

Designate a Post Emergency Coordinator

The Post Emergency Coordinator's duties would include the following:

- Document all contracts, agreements and emergency work or materials used during the emergency to ensure proper payments and reimbursements.
- Conduct a detailed safety inspection of the drinking water system facilities.
- Coordinate the completion of all emergency repairs and schedule permanent repairs to the service area.
- Notify key agencies (local and state health departments) of emergency repair status and the scheduled completion of the system repairs.
- Release repaired facilities and equipment for normal usage.
- Replace or authorize replacement of materials and supplies used during the emergency.
- Complete permanent repairs and replacements of the system facilities.

This emergency response guidebook was written as a guide for the drinking water system personnel to help them prepare and maintain their own emergency/disaster response plan. Because each drinking water system is so unique, it does not cover every aspect of a response plan; therefore, a response plan must be designed by those individuals who are directly involved in maintaining that particular drinking water system.

If we can be of any service or assistance, either in the design of the emergency response plan or the implementation of it please call us any time. Our emergency phone number is:

(801) 536-4200 or 536-4123

Good luck, and let's hope we never have to implement a response plan, but let's be prepared just in case!

Department of Environmental Quality
Division of Drinking Water
150 North 1950 West
Salt Lake City, Utah 84114-4830
(801) 536-4200

National Infrastructure Protection Center

Swarming Attacks: Infrastructure Attacks for Destruction and Disruption

July 2002

Summary

The potential for compound cyber and physical attacks, referred to as swarming attacks, is an emerging threat to U.S. critical infrastructure. Trends in activity of both terrorist groups and protest groups indicate that this type of attack may be used to augment either destructive or disruptive actions, respectively.

Introduction

Political protests and terrorist attacks over the past year have raised the serious possibility of attacks directed at disrupting specific sectors of the U.S. infrastructure. Protests around the world against globalization, Western corporations and governments, and U.S. policies have become increasingly organized, violent, and disruptive. Terrorist attacks, especially those of September 11, 2001, have demonstrated an increasing level of complexity and destructiveness. Both of these trends indicate a natural progression to *swarming attacks*: coordinated attacks using different methods against a target and the surrounding infrastructure to cause multiplied or cascading effects.[1] A likely form of swarming attack is one in which an attacker uses cyber means to enhance the effects created by a traditional physical attack, such as a bomb. Terrorists or violent protestors may initiate the cyber component of a swarming attack well before the physical component and may execute it simultaneously with the physical attack or as a follow-up to a physical attack. Understanding swarming attacks requires knowledge of recent trends in terrorism and protests that has lead to this phenomenon, the potential effects of such attacks, and the probability of these types of attacks.

[1] The term swarming was used by William B. Scott, "Nation's 'infosec gaps' given new scrutiny post-September 11," *Aviation Week & Space Technology*, 156(4):59. Scott describes "swarming" as a cyber attack conducted simultaneously with other kinds of attacks.

The Foundation of Swarming Attacks

Terrorist groups and global protestors have displayed parallel trends in recent years that could lead both to engaging in swarming attacks. Both have become more sophisticated in their activities, more familiar with technology, and more innovative in their targeting. Although terrorists have not yet conducted cyber attacks and protestors have not directly targeted infrastructure, trends indicate that attacks on cyber components of the infrastructure are likely.

Trends in Terrorism

Increased Complexity

The last decade has witnessed a natural progression in the complexity of how terrorist organizations have coordinated and carried out attacks.

- The first level of complexity is where a group uses the same attack method (e.g., a bomb or hijacking) at the same location but with the phases of the attack timed sequentially. For example, in 1996 the Irish Republican Army (IRA) detonated a car bomb inside the British Army Headquarters installation at Lisburn, Northern Ireland. Between 5 and 10 minutes after the first bomb exploded a second car bomb exploded outside the base medical center (targeting existing victims and emergency services).
- The next level is represented by the ability to coordinate the almost simultaneous use of the same attack method (e.g., a bomb) at geographically dispersed locations. In 1998, terrorists detonated bombs within minutes of each other at the U.S. embassies in Tanzania and Kenya.
- The complexity of terrorist attacks reached a new level in the attacks of September 11, 2001. Terrorists used the same method (civil aircraft), launched from different points nearly simultaneously and converged on two geographically separated target sets. In addition, they may have planned to attack in sequence within each target set (i.e., first one tower of the World Trade Center and then the second).

Furthering this natural progression, several terrorist organizations will likely develop the capability to carry out coordinated attacks that do not use the same method. Instead, the attackers will use different methods that support or complement each other. In addition, these methods may be used at different times and cause direct effects in different geographic locations.

Interest in New Forms of Attack

Terrorists have already demonstrated a willingness to use chemical and biological agents, and if used in conjunction with other attack types, they could have devastating effects. Even so, these may not be the most likely tools in swarming attacks, as they require specialized knowledge and special handling facilities. They may also be easier to track. In contrast, the development of a cyber attack capability does not have readily identifiable physical and logistical signatures like those found in the development of a chemical, biological, or nuclear attack capability. Moreover, a cyber attack capability does not require special academic research centers or even an indigenous training facility. The skill to develop a cyber attack capability, unlike the skills needed to develop a chemical, biological, or nuclear capability, can be openly acquired can even be self-taught. Importantly, cyber components can be attacked in other ways, including small explosives or radio-frequency (RF) weapons.

Awareness of Infrastructure as a Target

Several recent terrorist events indicate an awareness of the effects of attacks on the components of infrastructure sectors.

• In 1996 six members of the IRA planned to destroy six electrical sub-stations in the London area. The attack would have disrupted the electrical supply to London and substantial parts of Southeast Britain for months, blacking out homes, businesses, and industries as well as rail and underground travel and traffic lights.[2]

• Rebels in Nepal have destroyed more than 50 repeater stations of the Nepal Telecommunications Corporation in an attempt to disrupt communications to rural areas.

However, attacks on the infrastructure do not necessarily involve kinetic energy weapons but may involve other physical or cyber means.

• On April 25, 2002, burglars stole 17 computers that coordinated the traffic lights in Santiago, Chile, resulting in traffic gridlock. The municipal authorities in Santiago estimated that it would take three days to reestablish the system and restore traffic to normal.[3]

Recent cyber activity, including the BAT 911 virus, the Code Red worm, and the NIMDA worm also demonstrate the disruptive potential for attacks on the infrastructure. The potential for such cyber attacks to disrupt a sector of the national infrastructure, and have cascading effects into other sectors, is as great as the potential from physical attacks.

---

[2] J. Bennetto, "How IRA plotted to switch off London," *The Independent*, April 12, 1997, p. 1

[3] *The Southland Times* (New Zealand), April 29, 2002, p.1

Trends in Protests

A similar progression is taking place in protests around the world. Although the press has labeled most recent protests as "anti-globalization" it is more accurate to describe them as "anti-corporation."[4] Seemingly divergent groups protesting the power of corporations, environmental degradation, exploitation of labor, as well as the policies of the World Bank and International Monetary Fund that are blamed for these ills, converged at the World Trade Organization summit in Seattle (1999). This gave rise to the "Blue–Green" coalition—a new alliance between labor activists and environmentalists. With subsequent events such as those at Quebec (April 2001), Barcelona (June 2001), and Genoa (July 2001), repeat protestors became more familiar with each other and began to form informal partnerships as they refined their common theme.

Use of Technology

The use of technology by protestors is also becoming more common and refined. Due in part to their familiarity, protestors have begun using the Internet to communicate, coordinate activities, and exchange protest techniques. Often, ideas are exchanged in chat rooms until there are enough activists to start an e-mail list and establish a web page.[5]

- During a January 2002 meeting of the World Economic Forum in New York, cyber protestors created a virtual "sit-in," in the form of a denial-of-service (DoS) attack, against several web sites including the home page for the forum. This was accomplished through a tool posted on web that was a simple point-and-click graphical user interface.
- Members of Raisethefist.com, an anarchist site, electronically discussed choosing a corporate target for a month-long cyber protest. The group was focusing on companies they perceive as having a history of environmental abuses or exploitation of workers.[6]

Protestors have already demonstrated the propensity to use information technology to expand their target set. The Internet allows protestors to build a profile of a target corporation, organization, or even sector of the infrastructure and to target it in depth. This means that protestors could disrupt target corporations or organizations by attacking their suppliers, investors, creditors, and employees. A recent example concerns the attacks of animal-rights activists on a major drug-testing firm. While engaging in traditional protest activities, the group used its web site to publish the names and addresses of the firm's employees as well as details on other physical attack tactics used by similar groups. This action led to an increase in violence by the group against the targeted firm; including beatings and vandalism. The activist group also targeted the firm's investors and bankers.[7]

---

[4] P. Kirby, "Genoa protestors signal coming of age in global politics," *The Irish Times*, August 4, 2001, p. 12.
[5] J. D. Harder, "'Rent-a-mobs' descend on D.C.," *Insight on the News*, February 12, 2001, p. 1.
[6] iDefense, Inc., iDefense Daily Alert, RaiseTheFist.com contemplates month-long cyber attack," April 12, 2002.
[7] M. Satchell, "Terrorize people, save animals," *U.S. News & World Report* 132(11):24.

Use of Violence

This ability to coordinate electronically, as well as protestors becoming bolder as they coalesce around a common theme, has given rise to an escalation of violence during protests. The level of violence during protests has progressed from minor property damage in Seattle (1999) to deliberate attacks on law enforcement, the use of firebombs, and $100 million in damages in Genoa (2001). Infrastructure is a natural target for these types of protestors.

- As they come in conflict with police forces and attempt to disrupt political or symbolic events, protestors have obstructed local law enforcement, blocked traffic, and interrupted mass transit.
- Local utilities, even if privately owned, may represent the local government to protestors and, therefore, may also be targeted.
- Shifting the focus of their cyber attacks from web page defacements or DoS attacks to more potent attacks against local government communication or the local area's information infrastructure could be an easy transition.

Cyber attacks may also be attractive because they can be perceived as non-violent attacks and therefore construed as peaceful protests or simple civil disobedience. Similarly, as governments improve measures to physically separate protestors from important events, such as the June 2002 Group of Eight (G-8) summit held at a remote location in Canada, the protestors might look for means to disrupt the event remotely. A cyber attack, in conjunction with a physical protest, could create a greater disruption and, therefore, enhance the protestor's goal of attracting attention to their cause. Cyber attacks, that include various forms of malicious code designed to cripple a network or delay official response, may become part of a swarming attack when coordinated with confrontational, disruptive, or violent activity.

Coordination of Swarming Attacks

As terrorists and protestors become more technologically skilled, or purchase the expertise from cyber mercenaries, they will be able to conduct network reconnaissance with some degree of stealth. The growing cyber competency of these attackers also gives them other advantages when initiating the cyber component of a swarming attack. An attacker may begin the cyber element of a swarming attack well in advance of the physical portion. This inhibits the detection of a swarming attack by making the cyber activities seem coincidental and not directly linked to physical threats. For example, a virus that disrupts the 911 system or a worm that shuts down the pumps in a water system may not be readily linked to a threat of violence during an upcoming protest. Attackers can also disguise the cyber attack by including it in the normal stream of cyber incidents. In addition, they can also avoid creating patterns that will draw the attention of network security personnel by including the intended target in a long-term series of attacks against disparate targets that are not related to the developing swarming attack. In some cases, even

after a physical attack has taken place, investigators may not recognize prior or ongoing cyber activity as a component in a swarming attack. Current methods available to attackers include:

- Placing a virus or Trojan horse that can reside on a system until activated;
- Creating a back door in the targeted system that can be accessed when needed;
- Developing, over a period of several weeks or months prior to a physical attack, a network large enough for a crippling distributed DoS attack and executing it as part of a swarming attack.

Effects of Swarming Attacks

The three principal effects of swarming attacks are separately described below. In addition, a swarming attack may also cause greater public panic than a physical attack alone. People not located in the vicinity of a physical attack may still believe that they are under attack and cut off when their vital or expected services are interrupted. This feeling can be perpetuated through an interruption in official information, the deliberate placement of false information on official or reputable news sites, or the rapid spreading of rumor—all a result of further cyber activity.

Effects that Complicate Response

One of the most likely uses of the cyber component of a swarming attack would be to slow or complicate the response to a physical attack. This can be done by delaying notification of emergency services, delaying the arrival of emergency services to the scene, and denying the resources needed to manage the consequences.

- Instances of attacks on 911 services have already occurred. For example, in 1996, a hacker managed to break into a U.S. regional telephone network. Using his computer connection, he was able to generate multiple, simultaneous telephone calls to a single public safety answering point (PSAP) and tie up the 911 systems of eleven Florida counties, thereby blocking any legitimate callers.
- Malicious code has also been used with this same effect. The 911 virus (BAT 911), first detected in April 2000, was designed to delete all data in a system on a given day of the month. However, the virus also obstructed the 911 system by generating multiple false emergency calls. To illustrate, a cyber-based disruption of the 911 telephone system, carried out in conjunction with the early morning truck bombing of the Alfred P. Murrah Building in Oklahoma City, may have complicated the response by delaying emergency aid to the victims.
- The actual progress of emergency services to the site of a physical attack can be slowed by a cyber attack that disrupts the traffic light network and creates traffic jams that block emergency services.
- With the advent of automated building control systems, fire alarms, environmental controls, and lighting can all be controlled from offsite using a dial-in system. If

these systems were to be manipulated in several buildings at once, forcing people to evacuate, the crowds in the street and the demands on emergency services to address numerous alarms would delay the response of the emergency services to an actual attack.

A similar effect of complicating the response to an attack (while possibly widening and worsening the effects of the attack) could be achieved through a cyber attack that disables the water supply just prior to a violent protest, or the disabling of the electrical system in conjunction with a physical attack. This would deny emergency services the necessary resources to manage the consequences such as controlling fires, coordinating actions, and creating light for operating at night.

Effects that Widen Destruction or Disruption

The physical and psychological effects of an attack or protest can be widened using a synchronized cyber attack. Therefore, a swarming attack, even one as narrowly focused as the above example, could greatly widen the span of disruption for that protest or attack from a single geographic location to numerous cyber locations. This widening effect could disrupt a sector of the infrastructure and even cause cascading effects into other sectors. In addition, the psychological effect on a populace from a swarming attack may be greater than the effect from a physical attack alone. This is especially true if the effects of the cyber portion of the attack last for several days or weeks.

• Although horrific, the effects of the September 11th attacks on the populace of Manhattan would have been far greater if a cyber attack had simultaneously disabled the New York City water or electrical system through disruption of their computer-based process control systems.

This type of attack on the critical infrastructure of the city would have affected far more citizens than the actual attack on the World Trade Center and turned many spectators into victims. Such an attack would also have the effect of overburdening public utilities and emergency services as they attempted to restore vital daily services to a wide populace while managing the consequences of a large physical attack.

Effects that Worsen Destruction or Disruption

A cyber attack may also worsen the effects of a physical attack by either increasing the destructiveness of the attack or by placing more people at the site of the attack, thus increasing casualties. Although there are no instances of a cyber attack worsening the effect of a physical attack, possibilities exist throughout the critical infrastructure.

• A cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuel or gas in the area of a planned physical attack would enhance the force of the physical attack.

• An additional example may be extrapolated from an historical event. The effects of the bomb detonated in the parking garage of the World Trade Center, in February 1993, would have been worse if a cyber attack on the Port Authority Trans-Hudson (PATH) railroad was synchronized with the physical attack. The PATH station was on level B-4. An attack on the railroad's computerized signaling and safety system could be designed to force trains to stop at the World Trade Center station and passengers to detrain. The bomb actually did collapse part of the station's ceiling and the effect of this would have been greater with scores of people gathered on the platforms. In addition, the evacuation routes from the station would have taken the passengers upward toward level B-3 and closer to the bomb that was detonated on level B-2.

Conclusion

Recent trends in terrorist attacks and political protests demonstrate a progression toward swarming attacks: coordinated attacks using different methods (cyber and physical) against a target and the surrounding infrastructure to cause multiplied or cascading effects. Swarming attacks will allow terrorists or protestors to enhance the desired effects of disruptive or destructive activities by using cyber means to worsen or widen the effects, or to complicate emergency response. Although not a swarming attack, the September 11 attack on the World Trade Center provides a glimpse of the potential consequences of a swarming attack. As a result of the attack, extensive damage to the local telephone company's hub next to the World Trade Center eliminated 4.5 million data circuits and 300,000 phone lines; 30 percent of lower Manhattan's capacity[8]. Although much of the disrupted service has been restored, the effects remained for several weeks. A cyber attack in conjunction with a physical attack has the potential to do this amount of disruption or more; possibly for a longer period.

A swarming attack will be difficult to recognize and interdict. The cyber portion of the attack may begin long before the physical attack takes place and culminate before, simultaneous with, or even after the physical attack. This variance in timing will make it difficult for law enforcement and counterterrorism specialists to link the cyber activity with a physical threat. In addition, the cyber portion of the attack can be launched and controlled from a location well removed from the site of the physical portion. The preparation for the cyber portion can be hidden amongst normal Internet activity and network reconnaissance can appear to security personnel as the work of unrelated hackers. Another factor that may inhibit intelligence collection concerning swarming attacks is the availability of the skills and tools necessary to conduct the cyber portion. Unlike weapons of mass destruction, cyber attacks require virtually no special training, handling procedures, equipment, or development facilities. In addition, a cyber attack gives off no signature that is readily detected by the usual intelligence collection means. A swarming attack can have a localized or national impact on a sector of the critical national infrastructure. This impact may not remain in one sector but cascade into other sectors causing widespread disruption of the critical national infrastructure. Awareness of the trend toward

[8] S. Young, "Terror attack highlights problem in telecom sector's monopoly legacy," *Wall Street Journal*, October 19, 2001, p.1.

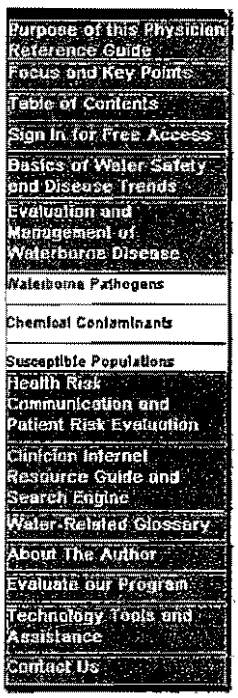
swarming attacks is the first step in being able to recognize and counter such an attack. Analysts and investigators need to look for cyber clues that may uncover future physical threats that the cyber activity may be meant to compliment. A more significant step, however, is to integrate physical and cyber protective measures within the national infrastructure to counter the potential disruption and destruction from swarming attacks.

This product was completed with support from the CRUCIAL PLAYER project. CRUCIAL PLAYER is an interagency project initiated in 1999 by the Deputy Secretary of the Department of Defense (DoD), the Deputy Director of the Federal Bureau of Investigation (FBI), and the Deputy Director of the Central Intelligence Agency, and funded by DoD and FBI. The project is managed by the National Infrastructure Protection Center, Washington D.C. Major contributors to this product were Scott Curthoys and Geoffrey French. Forward comments or questions to NIPC at 202-324-2084.

Recognizing Waterborne Disease and the Health Effects of Water Contamination
What Every Physician In Your Community Needs To Know

Funded by American Water Works Association and Arnot Ogden Medical Center
Author: Patricia L. Meinhardt, MD, MPH, MA

Maintaining water quality and securing the safety of water supplies in the United States requires a collaborative partnership between the medical community and water utility practitioners. The importance of this collaboration has been underscored by the growing threat to the security of our nation's infrastructure that includes the possibility of intentional contamination of US water reserves by covert terrorism. **Practicing physicians are likely to be the first to observe unusual illness patterns or disease trends resulting from intentional biological or chemical contamination of water supplies and must understand their critical role in detecting water-related disease and in cooperating with water utilities to protect their community's public health.**

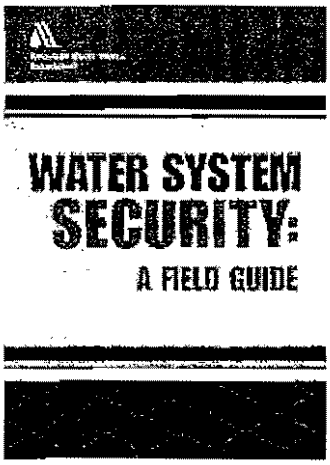


A **new medical website** has been launched to assist healthcare providers recognize and manage waterborne disease and the health effects of water pollution resulting from either **natural OR intentional** contamination of water. The contents of this medical website, *Recognizing Waterborne Disease and the Health Effects of Water Pollution: A Physician On-Line Reference Guide*, are posted on the menu bar to the left and are accessible at www.WaterHealthConnection.aomc.org. Unique features of this medical website include:

- "24/7" availability with free access to 366 webpages of comprehensive information
- Clinically relevant information detailing detection and management of water-related disease from both waterborne pathogen and chemical contaminant exposure
- Repository of physician anti-terrorism preparedness and readiness resources
- Special risk communication and patient risk evaluation guidelines for both healthy and susceptible populations regarding water-related disease
- "Ease of use" technology tools and website support for busy physician users
- Targeted search engines providing quick and easy access to 200 websites covering a diverse array of waterborne disease and water contamination issues
- Peer-reviewed content by leading medical and public health experts from medical academia and public health agencies including CDC, ATSDR, and EPA
- CME accreditation for credits toward AMA Physician's Recognition Award

Please share this important resource with your medical, public health, and water utility colleagues!

Safedrinkingwater.com News describes WaterHealthConnection.aomc.org as:
"New website on drinking water-related diseases co-sponsored by AWWA makes excellent info user-friendly for healthcare providers: Filling a long-existing void, this outstanding website will help fill the gaps in the knowledge of primary care physicians about a variety of illnesses that may (or may not) be related to drinking water. Utilities may want to consider how they can make the medical community in their service area aware of this service." *(April 10, 2002)*



Water System Security: A Field Guide
Managers and operations personnel of small to medium-size water utilities will find this guidebook very helpful as they assess and upgrade the physical and operational security of their systems. This guide emphasizes measures a water utility can take for better security against man-made threats. It covers the emergency preparedness plan; vulnerability assessments; mitigation measures for critical components; emergency response and recovery; and crisis communications. Supplied forms include security checklist, system component list, potential biological and chemical threats, emergency contacts, and more. Forms are provided in print and on diskette. Spiral-bound. ISBN 1-58321-193-4. 2002. **Catalog No.** 20501

Non-member Price: $85.00
Member Price: $55.00

Mail
AWWA Bookstore
6666 W. Quincy Ave.
Denver, CO 80235
- OR -

Call 1-800-926-7337

DRINKING WATER PROGRAM CONTACTS

EPA REGION 6
Drinking Water Section
James Brown
214-665-7155
brown.james@epa.gov

TEXAS
Texas Commission on Environmental Quality (formerly TNRCC)
Public Drinking Water Section
24-hour: 800-832-8224
512-239-4691
Mlannen@tnrcc.state.tx.us

LOUISIANA
Louisiana Department of Health and Hospitals
Safe Drinking Water Program
Ms. Karen Irion, Administrator
Center for Environmental and Health Services
24-hour: 800-256-4609
E-mail: Kirion@dhh.state.la.us

ARKANSAS
Arkansas Department of Health- Division of Engineering
After Hours & Emergencies: 501-661-2136
501-661-2623
safewater@healthyarkansas

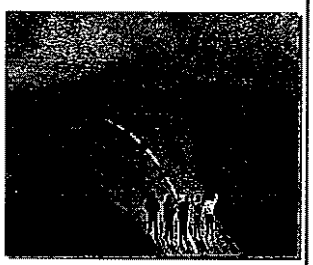
OKLAHOMA
Oklahoma Department of Environmental Quality
Public Water Supply Section
24-hour: 800-522-0206
405-702-8100
Mike.Harrell@deq.state.ok.us

NEW MEXICO
New Mexico Environment Department
Drinking Water Bureau
24-hour: 505-827-7536
505-827-1400
Toll Free: 877-654-8720
retta_prophet@nmenv.state.nm.us

Developing Credibility Through Communications

Powerful trends are shaping the water profession

- Competition
- Increasing regulations
- Scientific uncertainty
- Political intervention
- Public expectation



Qual-Serv found better performing utilities share common characteristics

- Sound fiscal policies and asset management
- Highly skilled/trained staff
- Customer focus/satisfaction
- Willingness to take risks
- High Level of credibility in the community

Credibility according to Webster's

- Credibility
  - that can be believed; reliable
- Credibility Gap
  - a disparity between a statement and the true facts
  - inability to have one's truthfulness or honesty accepted

Editorial: Distrusting the tap

Weariness over water reflects public's mood

"...Only a quarter of Californians routinely drink the water that comes from a tap. In Los Angeles .... only 18 percent trust the tap. Another 32 percent take it filtered and 48 percent stick to water out of a boule..."

"...public skepticism can be a positive force for government to keep pressing ahead on challenges... That said, there appears to be a gap between fact and fear, particularly when it comes to water."

Source: Sacramento Bee, July 23, 2002

"Gatorade Declares War on Tap Water" (AP Headline)

"When we're done, tap water will be relegated to showers and washing dishes."

"We're not against water - it just has its place. We think it's good for irrigation and cooking."

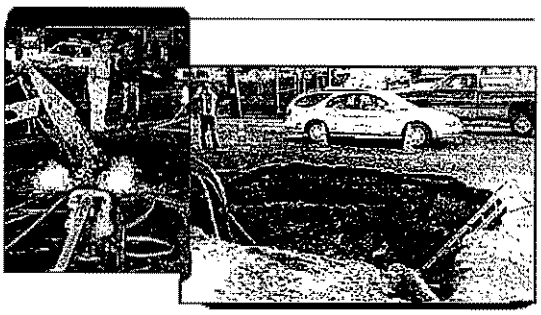
(Quaker Oats, US President of Beverage Division)

Fort Worth Water Main Breaks for Second Time in Three Days

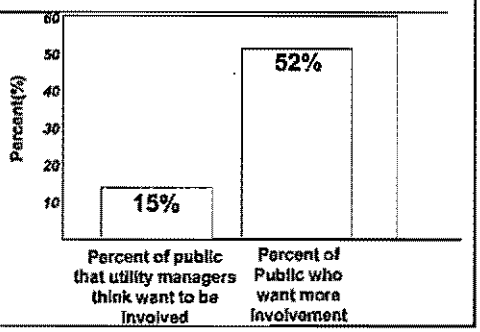
The first break happened around 10 p.m. Thursday. Officials blamed it on the heat wave, saying it probably happened because of high demand, metal fatigue and extremely dry conditions.

Water Main Break in Loop Area May Have Damaged L Track

Broken main leaves150 customers without water



The public expects to be involved.



Managers must make a paradigm shift

- Public involvement in utility decisions is essential to building and maintaining credibility
- -which must be managed as a crucial asset to the longevity and ultimate success of the utility

Credibility is evaluated through honest self-evaluation.

- There may be places in your organization where you have poor credibility.
- Ask questions internally and externally to determine credibility.
- Credibility may differ between groups

Assess the Utilities Readiness to invest in public trust

- What is the leadership style of the utility?
- Does the utility embrace a team-based environment or separation between functions
- Does the utility value stakeholder input?
- Is there a successful history of public involvement?

Corporate culture determines public involvement success

	Column 1	Column 2	Column 3
1 Leadership Approach	Command and Control	Mixed	Supportive/ empowering
2 Organizational Culture	Top down	Team based	Interdisciplinary teams
3 Cultural Alignment with Mission	Fragmented	Partial	Full Alignment
4 Information Access	Close to vest	Limited information provided	Full disclosure
5 Stakeholder Interaction	See little need	Educational based	Value stakeholder input
6 Resource Availability	No staff or money	Available, but stretched thin	Available and allocated to projects
7 Past Experience	No experience	Limited, negative	Positive
8 Media Relations	Avoid	Communicate through releases	Seek out relationships
9 Awareness of external trends	None	Understand major pressures on utilities	Leading industry in responding to change

How to determine what people care about

- Ask
- Provide avenues for two way communication
- Professional market research/surveys
- Talk to employees
- Call local reporter or talk show host
- Consult with other utilities in the area

Establishing trust and credibility

- Keep commitments
- State purpose/issue clearly and restate often
- Don't promise anything you cannot deliver
- Don't speculate about things you do not know
- Be patient and stick to purpose and goals
- Don't be defensive

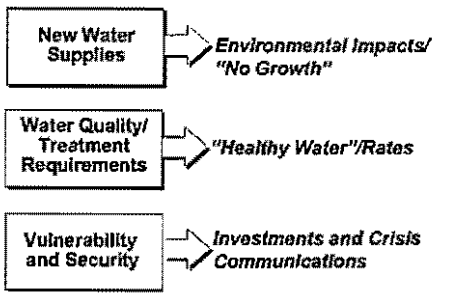
What to do when trust is low

- Maintain businesslike relationship and treat all participants with respect
- Summarize goals clearly and frequently
- Keep the public updated
- Train spokespersons to handle inquiries

Additional steps toward building trust and credibility

- Admit mistakes
- Remain impartial and hear all opinions
- Use recognized, credible experts to help communicate
- Make data available to interested parties

Strong credibility will help utilities with tough decisions



Developing a Concept of Emergency Operations

- Define emergency operations goals
- Create plans, policies and procedures
- Identify legal requirements
- Develop a strategy

Research

- Past Emergencies and Responses
- Current Planning Framework
- Analyze Risk Vulnerability Assessment
- Identify hazards
- Resources
- Characterization of Facilities

Review

- ✓ Legislation & Federal, State, and local mandates
- ✓ Existing Plans and Plans of Neighboring Water Utilities
- ✓ Outside Agencies Response Capability

Outside Agencies

- Community
- Government agencies
- State and local organizations
  - Health professionals
  - State Laboratories
  - Emergency Responders
  - Volunteers
  - 911 Operators

Resources

Resources should be:

- Applicable to your needs
- Available upon request
- Listed in order of relevance
- Quantified
- Identified before an incident

Plan Exercises

- Drills
- Functional exercises
- Tabletop exercises
- Full- scale exercises

Emergency Operations Plan Outline

Part 1: Introduction

- Purpose and Scope
- Policies
- Assumptions

Part 2: Water System Overview

- General description of entire water system
- System-wide overview
- Organization
- Location
- Facilities
- Security
- Interdependencies

Facility Annexes

- Organization
- Operations
- Maps
- Distribution diagrams
- Facility floor plans

Part 3: Risk Assessment

- Natural disasters
- Technological disasters
- Manmade disasters

Part 4: Organization & Coordination

- Organizational needs to respond to emergencies
- How coordination of resources enhances response
- The organization of the Incident Command System (ICS)
- Special considerations that need to be addressed

Overall Structure of the Organization

- Internal/external coordination requirements
- System-level
- Linkages to higher authorities
- Organizational chart
- Position responsibilities

Internal/External Organizations

- Utility organizational structure
- External contacts & organizations
- Checklists

Incident Command System

- Adopted external response system
- Critical decision-making involvement

Part 5: Activation, Notification, and Mobilization

- Activation
- Notification
- Mobilization

Activation

- Key personnel
- Organizational units
- Response levels

Notification

- Internal
  - Management
  - Safety Personnel
  - Laboratory personnel
  - Response personnel
- External
  - Law enforcement
  - State and Federal agencies
  - Customers
  - Other

Mobilization

- Individuals or groups
- Anticipated vs. surprise events
- Alert status
- Resource staging

Part 6: Communications

- Modes of communication
  - Internal
  - External
- Redundant communication capability
  - CB
  - Cell-phones
  - Landlines

Part 7: Incident Management

- Assessing the situation
- Operations
- Resource management
- Damage assessment
- Recovery/Restoration
- Deactivation
- Post-Incident Review

Part 8: Public Affairs and Communications

- Distribution of information to:
  - employees
  - public
  - media
- Customer action
- Community protection

Part 9: Plan Maintenance & Training

- Plan Reviews
  - Periodic
  - Post-incident
  - Post-exercise
- Training
- Exercises
  - Tabletops
  - Functional exercises
  - Full-scale exercises

Hazard-Specific Annexes

- Water Contamination
- Sewer Overflow
- Flooding
- Hazardous Material Release at a Facility
- Drought
- Wildfire
- Dam Failure
- Earthquake
- Landslides/Avalanche
- Severe Weather
- Criminal Activity
- Special Events
- WMD
- SCADA Intrusion
- Other

Appendices

- Contact Listings
- Team Rosters
- Emergency Shelters and Family Care Centers
- Checklists
- Resource Lists
- Forms
- Definitions/Glossary

Risk Communications

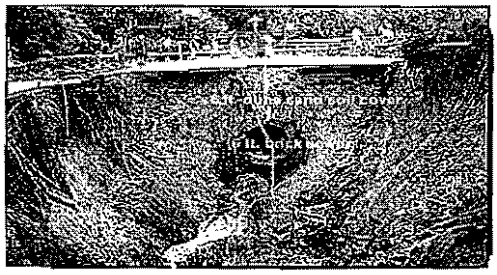
"If I had eight hours to chop down a tree, I'd spend six sharpening my axe."

Abraham Lincoln

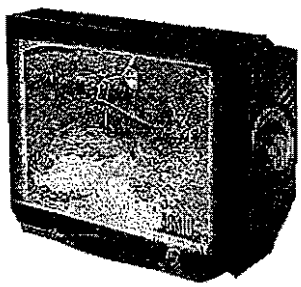
What is a Crisis?

- "Unexpected"
- Major incident with negative outcome
- Disrupts normal business, threatens credibility of organization
- More serious than a "problem"
- Every crisis is different, presenting different obstacles

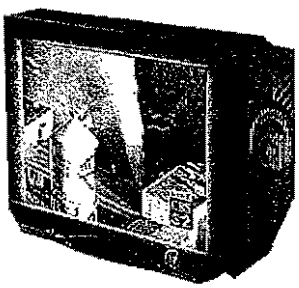
Collapse results in complete loss of natural creek bed and $1.875 million in mitigation costs



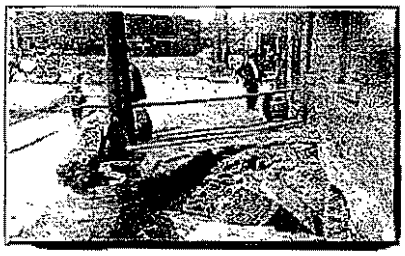
$700,000 enforcement action results from South Sacramento water main break



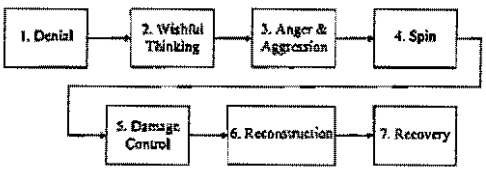
Warner Bros. lot soaked by broken main March 13, 2000



1899 sewer collapse requires $500 appropriation for property damage



The Seven Stages of Crisis Communication



1-4 Dysfunctional
5-7 Mature, highly evolved organizations

Bill Huey & John Knapp
Reputation Management, March/April 1997

Time Magazine - "Coping with Catastrophe"

"The worst part of a crisis is being unprepared. By removing the unexpected quality, you are removing that which is most unnerving."

Steven Fink, President
Lexicon Communications

Some Common Excuses...

- It's too soon to act
- It's just an isolated incident
- We need more time
- Let's not overreact
- We can't say anything; we'll be sued
- It will trigger copy cats
- If we say something, people will find out

Crisis Communications Approach

- Preparing for a crisis
- Implementing your Plan During a Crisis
- Assessment After a Crisis

Make as many decisions in advance as possible

Elements of a Crisis Communications Plan

- Introduction
- Mission/Vision Statement
- Background
- Objectives
- Key Messages
- Crisis Team
- Target Audiences
- Communication outlets/tools
- Communications protocol
- Drill Plan
- Evaluation

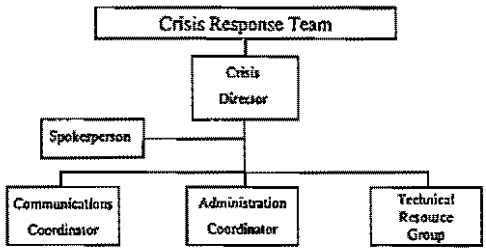
Prior to a Crisis

Develop and Test a Crisis Plan

- Create list of potential crises
- Assemble crisis response team
- Identify spokesperson(s)
- Develop key messages
- Determine key audiences
- Establish crisis communications center

Prior to a Crisis, *continued*

- Identify needed technical support
- Establish communications protocol
- Build relationships with agencies and organizations that you'll involve
- Develop media list and get to know reporters!
- Create fact sheets
- Test your plan



Crisis Tools

- Telephone log
- Media roster
- Communications calling tree
- Check list
- Situation analysis summary and update template
- List of caterers, A/V vendors

During a Crisis

Locate Spokesperson
-Involve in All Aspects of Situation

Step 1: Assess the situation
Step 2: Address concerns
Step 3: Activate crisis control center
Step 4: Assign responsibilities
Step 5: Establish On-site source

During a Crisis, *continued*

- Step 6: Determine key audiences
- Step 7: Determine information to be communicated
- Step 8: Notify key audiences
- Step 9: Establish system for continual updates
- Step 10: Record and Track Inquiries

Employing Key Principles Improves Success

- Principles
  - Accurate
  - Consistent
  - Timely
  - Clear
  - Complete
  - Responsive
- Outcomes
  - Reduced tension by stating the facts and the actions being taken to correct it
  - Demonstrated commitment
  - Control the information
  - Secure credibility

Effective Media Relations are Key to Telling "Your" Story

- Be prepared
  - Define (and communicate!) organizational standards
  - Proving training
- Develop a media relations plan
  - Key messages
  - Use appropriate tools and formats
  - Outlets

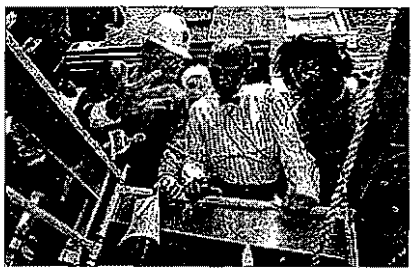
Credibility can be Built or Lost

- Building Credibility
  - Proactive open communications
  - Know who needs to hear what, when
  - Seek external expertise; create advisory board
  - Reveal what information is needed BEFORE being asked
  - Cooperate with the media

Credibility can be Built or Lost, cont.

- Losing Credibility
  - Blaming
  - No/little follow-up with victims or impacted parties
  - Technical justification for failure, rather than owning it
  - Hiding from the truth

"No secrets in a crisis. Everything comes out eventually."



Tips for Spokesperson

- Be warm and sympathetic - sincerity is important
- APOLOGIZE!
- Make statements that are worth being heard and repeated
- Never get mad or defensive
- Don't stray- stick to the situation at hand
- Don't give personal opinion or speculate

After the Crisis

Provide Closure and Revisit Your Plan

- Final update to key audiences
- Recognize participants
- Recover and rebuild
- Evaluate actions
- Update Crisis Communications Plan

Thoroughly Evaluate the Crisis and Response

- Establish timeline of events
- Identify any issues or gaps related to implementation - strategy or tactics
- Assess historical patterns for similar events
- Identify surprises - positive or negative

"Companies that behave appropriately and solve problems promptly are neither newsworthy or sueable"

James Lukaszewski
Seven Dimensions of Crisis Communications Management, 1998

CRISIS COMMUNICATIONS PLAN TEMPLATE

PRIOR TO A CRISIS

Create List of Potential Crises

Determine what crises could strike your utility, and gather or create simple background information for those that would be more likely or more complex to address. Information to gather could include experts within your utility, similar incidents at other utilities, and regulations. Example crises include:

- Contamination
- Major main break
- Chlorine spills
- Boil water notices
- Fuel/Oil spills
- Construction accident
- Violence in the workplace
- Natural disasters (flooding, hurricane, tornado, fire)

Select candidates to serve as spokesperson during a crisis

The public information officer is a natural, if you have one; if you do not, consider who has the best skills for the task, whether it be the general manager or public relations specialist. Assure that you have a backup individual, in the event that your top choice is unavailable or involved in remedying the crisis event. At the onset of a crisis situation, ensure this individual is *immediately* involved and informed. Remember that communication is a full-time job during a crisis and a dedicated spokesperson is usually necessary.

Name	Title	Phone number work/home

American Water Works Association
Dedicated to Safe Drinking Water

Determine the key audiences you will need to communicate with in a crisis

Create a roster that includes contact names, telephone numbers, fax numbers, and email addresses.
Some possible audiences might include:

Board Members
City Officials (mayor, city council, city manager)
County Officials
Employee Families
Fire Department
General Public
Groceries
Health Officials
Legal representations
Local Businesses
Medical Facilities/Doctors
Media (television, print, radio)
Police
Regional Utilities
Regulatory Authorities
Schools
Utility customers
Utility employees

Determine your available communication channels

Create contact rosters that include contact names for each applicable item, as well as telephone numbers, fax numbers, and email addresses. The best tool to apply will depend on the nature of your community, audience, time available, and the crisis at hand.

College Stations*
Door Hangers
Emergency Flyers
Emergency Phone Bank (automated phone message to specific area)
Government Access Cable*
Ham Radio Groups*
Homeowner Associations*
Hotline
Internet Sites*
Newspapers*
On-hold Messages
Personal Phone Calls
Press Conferences
Press Releases
Property Management Groups*
Radio (particularly talk format)*
Schools*
Telephone Trees*
Television Stations*
Volunteer Emergency Management Groups*
Your Own Web Site

*warrants roster

Determine possible locations for a crisis communications center

Consider locations within your utility, as well as off-site possibilities, where media, officials and residents can assemble to gather information, obtain updates, and take care of their own work needs. Possibilities include churches, civic centers and community centers. Keep in mind that your crisis communications center may not be in the vicinity of the actual crisis, and will depend on the specifics of the situation.

Determine necessary technological support needed for crisis communications and store or ensure you'll have ready access to it

Consider that the crisis communications center could be anywhere, and power may not be available depending on the specific crisis.

Battery-powered televisions, radios
Cellular phones
Contact rosters
Copiers
Crisis Plan
Easels/markers/newsprint
Extension cords
Fax machines
Flashlights
Hard hats
Internet connection
Lap-top computers/printer
Maps (service area, etc)
Paper/office supplies
Specific phones/phone lines
Two-way radios*
VCR

*Keep in mind that often times the media will intercept radio communications.

Establish a protocol for handling inquiries

Create a utility policy on how media calls and other inquiries will be addressed and how information will be transmitted, both internally and externally. Determine who will be responsible for responding to a significant increase in telephone calls and other inquiries, and how the calls and inquiries will be logged. Also, make sure your phone system and internet are capable of handling the increased amount of calls and e-mails that coincide with a crisis, and that a "hold" system is available to avoid having callers receive a busy signal.

Create Key Messages

Prepare key messages to be the foundation for communication during a crisis. It's important to have key messages in writing, so they are easily accessible at the onset of a crisis. Ideas to include:

- Dedication to providing safe water
- Commitment to public health
- Safety record (both in terms of service to the public and operations)

Create fact sheets

If not already in existence, create fact sheets that include information on:

- Source of water supply
- Water treatment methods employed at utility
- General information about the utility (number of treatment plants, number of employees, years in operation, etc)

*AWWA's web site provides fact sheets on most water-related issues, such as arsenic and *cryptosporidium*. Information can be found at http://www.awwa.org/pressroom

Train Spokesperson on how to address the public and media

Once you have identified the spokesperson that will handle media inquiries, review the basics of public and media interviews and conduct practice interviews. Tips to keep in mind:

- There is no "off the record"
- Statements should be succinct
- Speak visually; offer analogies
- Avoid technical jargon; translate to "lay language" (8th grade level)
- Show compassion
- Show confidence
- Do not comment on personal opinions or provide your own
- Never say "no comment"
- It's okay to say "I don't know" but be willing to find the information
- Be honest

Test Your Plan

Many organizations conduct 'crisis drills' to ensure the crisis communications plan addresses relevant issues, such as distributing information internally.

DURING A CRISIS

At the onset of a crisis, ensure your spokesperson is immediately briefed on the situation.

As you proceed through these steps, keep in mind that you need to move to Step 8, "Notify Key Audiences," as soon as possible. It's better to start getting some information out rather than waiting until all of the facts are in.

Step 1: Assess the Situation

Ensure that you are informed of the basic elements of the situation:

- What happened?
- Where did it happen?
- How did this happen?
- Who is involved?
- Who is affected?
- When did it happen?

Step 2: Once You Get the Facts, Address the Following Issues

- What are the specific elements of the situation that make it a "crisis?"
- Are immediate needs being handled?
- How serious is the situation?
- What measures are being taken to correct the situation?
- Is the situation under control?
- Are emergency provisions being made?
- When will the situation be corrected?
- Have all of the facts been gathered?
- What is the position of the utility?

Step 3: Determine Location of Crisis Control Center

Depending on the nature of the crisis, select a location that is convenient for your audiences and the media. The specific situation and magnitude of the crisis may lend itself to creating a separate crisis control center, as well as a crisis communications center. The command center may serve as the central location for residents, customers, and those directly affected by the crisis, while the communications center may be where the media gathers for updates.

Step 4: Assign Responsibilities

Determine available personnel and assign responsibilities, such as answering phones, responding to the media, monitoring media coverage, updating information to phone responders, etc. Be open to involving utility personnel in numerous roles during a crisis situation, whatever their usual responsibilities may be.

Step 5: Establish an On-site Source

Ensure that a utility communications representative is continuously on-site at the crisis location to monitor the situation and provide continuous updates of the most recent developments and information. The on-site representative can also provide any needed assistance to the media and other audiences.

Step 6: Determine Key Audiences

Given the specific crisis at hand, determine your key audiences. Review the list of possible audiences you developed during the planning phase and identify those who are directly impacted by the crisis, as well as those who will have questions and/or should be kept in the loop.

Step 7: Determine Information to be Communicated

Based on the specific situation and applicable key audiences, determine what information should be communicated, and make sure to continually include your key messages. Keep in mind that even though you want to provide as much information as possible, not all information needs to be communicated. If facts are missing, it may not be a good idea to relay that information.

Step 8: Notify Key Audiences

Determine which communication channels are appropriate to notify your key audiences. Consider what information these separate audiences most need and want. In communicating with key audiences, it is important to be able to offer them information in writing, as well. Be sure to continually update your different audiences as new information becomes available.

Step 9: Establish System for Continual Updates

As the situation progresses, determine the best method for providing continuous updates to your different audiences. Periodically review and reprioritize your audiences, information and communication channels as the situation changes. If you are working with the media, help them to get the story right. Continue to work with your different audiences throughout the crisis situation- from the moment the story breaks, until the situation is over.

Some tips include:

- Use one spokesperson, to be consistent
- Be accessible and ready to be available at all times (24/7)
- Back-up verbal information with written information
- Use written information, where possible (copies of spokesperson comments; data; etc.)

- Use graphics
- Explain technical issues; translate to lay terms
- Provide continuous updates, even if there is no new information
- Get back in touch, in anticipation of key news times/broadcasts
- Separate media from central command station
- Provide access to subject matter experts, both within your utility and in the water profession. However, ensure that they are capable of explaining the situation in non-technical terms.
- Facilitate media interviews and photographs

Step 10: Record and Track All Inquiries

Continually track interactions with your different audiences, including:

- Who you've spoken with
- Generally, what information you provided
- What is their particular interest (if media)
- When do they need to be called back
- Media interviews given and by whom

Establish a file to accumulate all communications, both internally and outgoing. Include information used by phone responders, news releases, internal memos, key messages, talking points. For each communication, note the date and time it was issued. Create a 'clip notebook' with all coverage, rosters of interviews and media coverage, and keep letters and comments received from customers/general public.

American Water Works Association
Dedicated to Safe Drinking Water

AFTER THE CRISIS

Final Update to Key Audiences

Provide a closing update and cover what happened, why, how, when, where, what was done to remedy the situation, and if available, what measures have been taken to avoid future difficulties.

Recognize Participants

Thank and recognize individuals and organizations that provided assistance during the crisis, particularly employees who rallied for the effort. As appropriate, apologize for the difficulties for those affected and thank them for their patience.

Re-establish Credibility

Communicate to your different audiences the preventative steps that are being taken to ensure another crisis does not arise. Also, explain exactly what happened and why it happened.

Evaluate Actions

Conduct a team meeting to de-brief, once the crisis is completely over. Determine your effectiveness in terms of:

- Response time
- Media portrayal- how did your utility look to the public?
- Accuracy- what did varied communications outlets get right and wrong?
- Consistent Key Messages
- Communication Tools- how did each tool work; what else could you have used?
- Prompt notification of key audiences
- Sufficient equipment
- Communications control center
- Communication to key audiences
- Internal communication – did employees and responders know what they needed to, and promptly?

Update Crisis Communications Plan

Add any lists or audiences that you deemed necessary during the crisis, and make any necessary improvements.

—Compiled by the AWWA Public Affairs Committee

American Water Works Association
Dedicated to Safe Drinking Water

(303) 794-7711
Fax (303) 794-7310
www.awwa.org

6666 W. Quincy Avenue
Denver, CO 80235

MEDIA INTERVIEW TIPS

Preparing for an interview

1. Gather all the information about the situation: Who, What, Where, When, Why, How

2. Write a summary statement to describe the incident, then rewrite it using half the words.

3. Write a sentence or two to describe how it affects the community and what you're doing to inform, protect, correct, and repair the situation. Describe the record of your utility in serving the public responsibly and safely (including statistics, if appropriate).

Rewrite this in the form of two to five main CONCISE points you can emphasize. These are your "Key Messages." Memorize them and practice speaking them, so you can feed them back easily during the interview. Rework the language, if need be, to fit your speaking style.

4. Think of some questions you may be asked about the situation. What sorts of things have you heard the media ask in similar situations? As a viewer or consumer, what would you want to know? Practice answering these until you are comfortable with your answer.

5. Ask a couple of coworkers to listen to you and help you practice responding to questions.

American Water Works Association
Dedicated to Safe Drinking Water

(303) 794-7711
Fax (303) 794-7310
www.awwa.org

6666 W. Quincy Avenue
Denver, CO 80235

During an interview

- **There is no "off the record"** – Anything you say is fair game.
- **Statements should be brief, and to the point** – Your interview will likely end up being only 10 to 30 seconds of air time. Make yourself the "editor" of your comments, rather than leaving it in the hands of the news director.
- **Show compassion** – Articulate your concern for the impacts on those affected by the crisis. Ensure you do not appear cold, uncaring or bureaucratic in your attitude. Meter your level of concern and empathy to the particular situation.
- **Show confidence** – Do not appear nervous or unsure of what you are saying. Reflect certainty and commitment that your utility will resolve the issue.
- **Do not provide personal opinions, conjecture, or respond to hypotheticals**– If a reporter asks what you think of the situation or proposes a hypothetical, bring the point back to the situation at hand.
- **Never say "no comment"** – This often leads to speculation that you know information you do not want to reveal or are trying to hide something.
- **It's okay to say "I don't know"** – Do not try to provide information you are not certain about or guess at a response. Inform the reporter that you will find that information and get back to them.
- **Be honest** – Do not lie to the media.
- **Act naturally**- Sincerity is important. You don't want to seem tense or in any way out of control.
- **Appearance is important**- Consider what you are wearing. Do you look like the person you would want to be relying on in an emergency?
- **Beware of becoming, or even seeming, defensive**- Your best response to an apparent negative or "goading" question is to reiterate the positives, as you prepared in your talking points.

—Compiled by the AWWA Public Affairs Committee

American Water Works Association
Dedicated to Safe Drinking Water

(303) 794-7711
Fax (303) 794-7310
www.awwa.org

6666 W. Quincy Avenue
Denver, CO 80235

MEDIA RELATIONS CHECKLIST

- ☐ **Understand How the Media Works** – In order to do their jobs, media representatives must gather as much information about a given topic as possible in a short amount of time, and then craft a story on that topic that is interesting, informative, and accurate. It is their JOB to be objective and report all sides of the story.

- ☐ **Respect the Media as Professionals** – From time to time your professional perspective and obligations will not coincide with those of the media; they understand this, and so should you. Don't overreact if they challenge you or the information you have presented. Interviews are opportunities to tell your story and get the correct information out there.

- ☐ **Develop Credibility; Be Open and Honest** – Credibility is built on trust and may take awhile to develop. Be open and honest with the media. Don't leave out important facts and DON'T misrepresent what is true, even if this may force you to provide less favorable explanations for your organization.

- ☐ **Be Prepared** – Communicate with employees throughout your organization and encourage them to call and inform you of any crisis or unusual, potentially newsworthy occurrence – positive or negative. If you know ahead of time that a main line has ruptured and water is rushing down the street, you have time to find out the facts and what's being done to repair it BEFORE the media contacts you. Similarly, establish a protocol within your utility regarding the appropriate people or persons to speak with the media.

- ☐ **Be Proactive** – If you know something newsworthy is occurring, tell the media before they need to call you. Bring them "into the loop" from the start. Develop a relationship with local reporters. Reporters are always looking for good stories – offer them ideas of ongoing and emerging occurrences and initiatives in your organization.

- ☐ **Return Media Calls and Be Responsive** – Reporters work under tight deadlines. If someone calls to ask a question or get "your side of the story," get back to them promptly. If they are seeking a subject matter expert or need to speak with someone else within the utility, be certain that person responds promptly. If you don't, the reporter will likely find someone else and it may not work to your benefit.

- ☐ **Be Fair**– When a reporter writes a good, well-balanced story, call or e-mail them to say you liked it and express your appreciation. If there is an error, consider the magnitude and the potential impact before reacting. Some mistakes can simply be let go. If one is particularly damaging, respectfully point out the error and offer the correct information. Being accusatory to the media – particularly in a public forum –is rarely beneficial in the long term.

- ☐ **Read the Paper, Listen to the Radio, Watch Television News** – Become familiar with the media representatives in your area. The more you know about the person you're talking with, the easier it will be to tailor your message so it will be received effectively.

—Compiled by the AWWA Public Affairs Committee

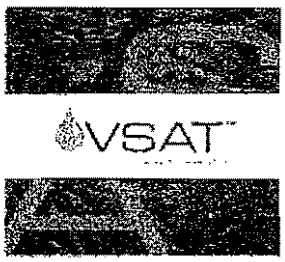
TRAINING and OTHER RESOURCES

AWWA Seminars
www.awwa.org
Vulnerability Assessments for Water Utilities
Course material is licensed from **AwwaRF** and **Sandia National Laboratories**

US Environmental Protection Agency
USEPA WATER PROTECTION TASK FORCE
http://www.epa.gov/safewater/security/

EPA's Water Protection Task Force with assistance from EPA Regions and external partners are taking many actions to improve the security of the nation's drinking water and wastewater infrastructure. The actions fall in six major categories. Tools, Training, Information Sharing, Research, and Networking.

New Vulnerability Assessment Tool for Wastewater Utilities
Introducing VSAT™wastewater
http://www.vsatusers.net/



The *Vulnerability Self Assessment Software Tool* (*VSAT™*) provides a comprehensive, intuitive system for wastewater utilities seeking to analyze their vulnerability to both intentional threats and natural disasters. *VSAT™* organizes data, supports vulnerability analyses, documents the analyses, and presents complex information in an easy-to-understand format for the full suite of potential utility assets including physical plant, employees, knowledge base, information technology, and customers. This invaluable software tool includes reference libraries of both potential threats and countermeasures, and provides an enduring method for managing the information generated by security vulnerability assessments.

amwa Association of Metropolitan Water Agencies

http://www.amwa.net/

Water Information Sharing and Analysis Center (Water ISAC)
Voluntary reporting by water sector utilities will contribute to the security of the nation's water infrastructure by enabling an early alert system. Water and wastewater utilities are encouraged to report malicious incident information so that data may be analyzed to establish trends and identify imminent or ongoing threats for the purpose of issuing timely and actionable warnings.

The Water Sector and the National Infrastructure Protection Center (NIPC) have developed criteria and thresholds for reporting incidents of malicious or unknown origin. When the Water Information Sharing and Analysis Center (Water ISAC) is fully functional, incidents will be reported through the Water ISAC web site. Until that time, water and wastewater utilities can voluntarily send incident information electronically from this site by completing the online form.

FBI/NIPC Offices and Contacts

- FBI Field Offices. http://www.fbi.gov/contact/fo/info.htm Go here to find the agency field office closest to you. The site has contact names and phone numbers listed by city.

- National Infrastructure Protection Center (NIPC). http://www.nipc.gov/ The NIPC is the national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response.

International Association of Emergency Managers
http://www.iaem.com/index.html

For AWWA Use Only.

AMERICAN WATER WORKS ASSOCIATION
INDIVIDUAL MEMBERSHIP APPLICATION

FAX (303) 347-0804 Phone 1-800-926-7337/303-794-7711
6666 W. Quincy Avenue/Denver, CO 80235
www.awwa.org

Dedicated to Safe Drinking Water

Have you ever been a member of AWWA?_____
When?_____
Member No._____

Please furnish your preferred mailing address below (indicate whether business or home): ☐ Business ☐ Home

☐ Mr.
☐ Mrs.
☐ Ms.
☐ Dr.

First Name | Middle Initial | Last Name | Suffix

Exact Street Address | (P.O. Box or Mail Stop)

City | State or Province | Zip or Postal Code

Title

Company Name | E-mail Address

Home Phone | Business Phone | Business Fax

Applicant's Signature | Date

Signature of AWWA Member Endorsing Application (Optional) | Endorsing Member Number

Is your company a current member of AWWA?_____ If not, please provide your company's main address if different from above:

Company Name | Main Business Address

City | State/Province | Zip or Postal Code

ANNUAL DUES:

	$99-Active Grade Code 02	$50-Operations/Administrative Grade Code 06 (For operator or administrative level personnel or employees of small utilities. Will not receive *Journal AWWA*.)	$32-Student Grade Code 14	$145-International Grade Code 03
ANNUAL DUES	$ _____			
Section Assessment*	_____			
Multi-Section Option†	_____			
TOTAL DUE	$ _____			

Make check payable to AWWA (U.S. funds only).
☐ MasterCard ☐ VISA ☐ Send Invoice
☐ American Express

PREPAYMENT OF ONE YEAR'S DUES REQUIRED
No action can be taken on this application until payment is received.

Dues amount guaranteed through December 31, 2002

Card No. _____ Exp. Date _____

*Section Assessment - AWWA has 43 local sections. Your section is determined by your address. However, some sections require additional annual fees to better serve their local members. Section assessments are mandatory for applicants with addresses as shown:

Please find your Section Assessment fee in the table at right and enter the total on the line reading "Section Assessment."

ADDRESS	ACTIVE (02)	OPERATIONS (06)	STUDENT (14)
Alabama, Mississippi	$20	$20	-
Alberta, Manitoba, N.W. Territories, Saskatchewan	$10	$10	-
California, Nevada	$15	-	-
Connecticut, New Jersey	$10	-	-
Florida, Minnesota, South Carolina, Texas	$10	$10	-
Georgia	$28	$28	$5
Idaho (western), Oregon, Washington	$10	-	-
Illinois	$8	$4	-
Maine, Massachusetts, New Hampshire, Rhode Island, Vermont	$50	$20	-
Missouri	$6	$3	-
New York	$15	$8	-
Pennsylvania	$15	$5	-

ALL APPLICANTS SHOULD COMPLETE THIS SECTION:

Circle the descriptions below that best describe you. The information is used in audits of AWWA readership. Circle only ONE in each group.

BUSINESS AND INDUSTRY
A. Public Water Supply Utility—Municipally Owned
B. Public Water Supply Utility—Investor Owned
C. Governmental—Federal, State, Local
D. Consultant
E. Contractor
F. Private Industrial Systems or Water Wholesaler
G. Manufacturer of Equipment & Supplies Including Representatives
H. Distributors of Equipment & Supplies including Representatives
I. Educational Institutions, Faculty and Students, Libraries, and Other Related Organizations
J. Fully Retired
K. Research Labs
L. Unreported

CHECK FIELD(S) SERVED:
5 ☐ Water Supply Only 7 ☐ Wastewater Only
9 ☐ Both 3 ☐ Other

JOB TITLE
A. Executive-Gen'l Mgr., Commissioner, Board Member, City Mgr., Mayor, President, Vice-President, Owner, Partner, Director, etc.
B. Management-Division Head, Section Head, Mgr., Chief Engineer, Comptroller, etc.
C. Engineering/non-managerial-Civil Engr., Mech. Engr. Envir. Engr., Planning Mgr., Field Engr., Systems Designer, etc.
D. Scientific/non-managerial-Chemist, Biologist, Biophysicist, Researcher, Analyst, etc.
E. Purchasing-Purchasing Agent, Procurement Specialist, Buyer, etc.
F. Operations-Foreman, Operator, Maintenance, Crewman, Service Rep., etc.
G. Marketing & Sales/non-managerial-Mkt. Analyst, Mkt. Rep., Salesman, Sales Rep., etc.
H. Other (describe) _____
I. Professorial - Teacher, Educator, etc.

Completion of this information is optional.

AWWA maintains profile data for use in developing additional programs and services to meet the diverse needs of our members.

Birth Date
_____/_____/_____

Race/Ethnic Identification: (check one)
☐ 1 American Indian/Alaskan Native
☐ 2 Asian/Pacific-Islander
☐ 3 African American
☐ 4 Hispanic
☐ 5 White (Non-Hispanic)
☐ 6 Other

Gender: (check one)
☐ F Female ☐ M Male

† MULTI-SECTION MEMBERSHIP OPTION In addition to your own section membership, you may also join other AWWA section(s). This allows you to receive information on events and activities from other local sections. If this is of interest to you, call 1-800-926-7337 for multi-section information and fees.

The following information is for USPS Standard class mailing requirements ONLY: In some AWWA sections, a portion of the section allotment equal to 50 percent or more of the domestic subscription rate charged for the section periodical will be allocated toward a subscription of that periodical. Dues allocated for each publication members receive: *Journal* $30 *MainStream* $6 *Opflow* $5

CERTIFICATE OF COMPLETION

ISSUED TO

IN RECOGNITION OF SATISFACTORY COMPLETION OF THE

August 6, 2002 Satellite Teleconference:

"Hardening Targets: Assessing Your Vulnerability "

SPONSORED BY THE

TEXAS SECTION OF THE

AMERICAN WATER WORKS ASSOCIATION

Approved for ____ Professional Development Hours

OR __4__ Contact Hours Credit

OR ____ Continuing Education Units

Mike Howe Executive Director