



Missouri Department of Natural Resources

Water Protection And Soil Conservation Division
Public Drinking Water Program

MODEL

Emergency Operating Plan
For Public Water Supplies

Security Threat

Mitigation

Preparedness

Response

Threat Evaluation Form

SECURITY THREAT

A security threat to a water system includes anyone or anything that may cause harm to a component or person that interrupts/interferes with the delivery of safe drinking water. Threats typically create panic in the community and create lack of confidence in water system operations. Perpetrators may be extremists, civil dissidents, employees on strike, disgruntled employees, released ex-employees or teenage pranksters. Threats range from trespassing, tampering, vandalism, sabotage, theft and terrorism.

With the terrorist attacks of September 11, 2001, the possibility of additional terrorist attacks against water systems in the United States has become evident. Terrorist threats have been made and are being addressed by all sizes of water systems. In most cases, where, when and how attacks will occur are unknown, and terrorist threats can be difficult to mitigate.

Hazards of these threats include loss of power and communications, SCADA cyber attack, explosions, intentional fires, chlorine release, broken mains, chemical or biological contamination, pump failure, dam failure or storage tower failure. Biological and chemical contamination of water supplies are addressed in a separate section. With terrorists and extremists, injury, death and economic damage may also be objectives of attacks against water systems.

Assessing system vulnerabilities can help facilities prioritize and determine which resources to protect and how much funding is desired. When identifying system vulnerabilities, the consequences of undesirable events should be taken into account. Assessing risk is a subjective process. One must consider the utility's ability to perform its mission, cost for repairs or replacement, and costs to mitigate hazardous consequences. General security improvements at water supply facilities can serve to deter and delay acts of tampering and terrorism.

The information in *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems* developed by the Association of State Drinking Water Administrators (ASDWA) and the National Rural Water Association (NRWA) in conjunction with the U.S. Environmental Protection Agency was incorporated in this section and the water system component sections of the PWS Model EOP. Although the self-assessment guide was designed for water systems serving populations between 3,300 and 10,000, it is also applicable to water systems serving less than 3,300. The document can be downloaded from the following website: www.epa.gov/safewater/security.

Mitigation

Mitigation as it relates to water system security generally means identifying and reducing access to "targets" or critical components in a system. An analysis of existing security equipment and procedures is the first step in determining system vulnerabilities. Physical and operational improvements should minimize risks posed by deliberate threats to a water utility. Some suggestions for improving water system security through operational and physical means follow:

A. Operational

Policies and procedures with respect to different types of security threats should be reviewed and their effectiveness evaluated. Identifying how personnel prepare for, and react to, threats and emergencies at water utilities is an important step in assessing vulnerability.

Personnel

- Establish a “culture of security”. Identify it as a key organizational value in placement interviews, employee meetings, and public communications.
- Consider appointing a security manager whose primary responsibility is addressing security needs at the utility.
- Contact your emergency service providers (fire, police, local/state/federal response) and familiarize them with your staff, your facility, and your unique circumstances.
- Review personnel hiring and firing policies. Conduct background checks on new employees and subject all employees with periodic background checks.
- Require photo identification of all employees.
- Collect keys and identification badges/cards from former personnel.
- Determine what information about the system should be protected.
- Review operational policies with contract employees. Consider limited access for contract employees or background screening such as the FBI most wanted list.

Policies and Procedures

- Make it policy that all doors and locked and alarms are set at the office, well houses, treatment plants, and vaults.
- Tell employees to question strangers in your facilities, and do not allow access to anyone who does not have a valid reason for being there.
- Coordinate with the public to report any suspicious activities at utility components to law enforcement.
- Indicate restricted areas by posting “Employees Only” or “Restricted Area” signs.
- Remove signs identifying wells, pumping stations and facilities.
- Do not leave keys in equipment or vehicles at any time.
- Terrorist threats to all critical water supply infrastructures should be taken seriously and considered a potential hazard.

Facility Operations

- Instruct employees to report unusual situations or attempts by third parties to obtain information about the utility.
- Cross train employees to provide backup capabilities during emergencies.
- Discuss detection, response, and notification issues with public health officials and establish a protocol.
- Vary the scheduling of operational procedures and employee security checks to avoid predictable patterns.
- Establish a protocol for determining, during an emergency, at what point you take specific actions.
- Reevaluate the utility’s policies addressing contractors, visitors, and scheduled tour groups to restrict site access.

- Test all chemicals delivered to the plant to verify authenticity.
- Consider eliminating or limiting public access to critical areas of the plant.
- Be sure that all visitors have proper identification and a staff escort when they visit.
- Ask law enforcement officials to provide extra surveillance of facilities.

Source Water and Treatment

- Identify alternative raw and finished water sources for use during emergencies. Consider power, operational, and equipment requirements to provide water supply.
- Consider activating unused or abandoned supply wells or abandoned or obsolete treatment facilities during emergencies. See Appendix H for other water treatment alternative options.
- Securely cap all abandoned supply wells and bore holes to prevent contamination.
- Establish interconnection supply agreements with neighboring water utilities to provide treated (or raw) water during emergencies.
- Water supply components such as plant, pump stations, wells and intake have in place priority service for electric power and/or install backup generators or batteries.
- Install shutoff valves capable of isolating portions of the system.
- Periodically monitor pH, turbidity, total and fecal coliform, total organic carbon, ultraviolet absorption, color and odor of source waters.
- Toxicity of source water can be measured with daphnia toximeter (expensive) or minnow aquariums. If either shows distress, conduct additional testing.
- Restrict access to dams and intake structures by installing barricades and locked gates.
- Properly seal wellheads, securely attach well vents and caps, and properly secure observation or test wells to prevent tampering.

B. Physical

A physical protection system must provide delay, detection, and response. Keep in mind that a determined adversary can gain access to or disrupt even the most secure systems. The goal in preparation is to lengthen the delay time, shorten detection and response times, and mitigate adverse consequences.

System Buildings

- Install hardened doors, locks, window security, and lighting.
- Locate parking for private vehicles a sufficient distance from utility and other buildings.
- Limit places of entry to facilities and control access with electronic keys or identification card checks.
- Install delay systems such as fencing, locked gates, guard stations, and other barriers. Berms and landscaping with steep grades are useful in preventing vehicle attacks.
- Consider interior and exterior detection sensor technology, including microwave, ultrasonic, active infrared, sonic, vibration, fiber optics, video motion detectors, and closed circuit television systems.
- Construct with fire-safe building material.
- Consider real-time monitors for contaminating agents.
- Install gas monitoring systems for chlorine and other hazardous gases.

- Ensure chlorine chemicals are secured in a well-ventilated, fire resistant, sheltered area away from other chemicals and inspect regularly.
- Creating redundancy in a system is one example of protecting critical assets. However, having three working pumps with one spare located unprotected right next to them is not redundancy. In this case, the spare could be disabled just as easily as the working pump. Placing spare equipment in a secure or removed location from the working equipment is acceptable redundancy.

Distribution

- Fit hydrants, manholes, meter boxes and valve boxes with tamperproof caps and lids.
- Know locations for valves and conduct periodic maintenance to easily access during emergency situations.
- Reservoir and tank access panels and vents should be tamperproof.
- Cover and lock finished water reservoirs.
- Fence and lock vulnerable areas such as pump stations, valve vaults, and meter pits to deter access.
- Install alarm systems on door hatches at remote facilities. Routinely test to ensure alarms operate properly with SCADA system. Educate employees and law enforcement on how to respond to alarms.
- Increase frequency and geographic distribution of chlorine residual monitoring to monitor possible contamination that decrease chlorine residual.
- Integrate early warning monitoring systems into water transport, treatment, and distribution systems that will notify an operator immediately of changes in chemical characteristics, flows, pressure, and temperature.
- Install valves at critical points in the distribution system to prevent backflow.
- Monitor customer complaints on color, taste and odor of the water.

Cyber, SCADA, and Communications

- Isolate the SCADA network from all other network connections, especially those connections to and from the Internet.
- Consider installing firewalls and setup to maximum security level.
- Install intrusion-detection software that alerts malicious network activity from internal and external sources.
- Do not rely on factory default configuration setting to protect your system.
- Upgrade password-protection protocol. Require regular password changes.
- Restrict employee access only to those resources needed to do their job functions.
- Limit control of remote terminals to on-site or main terminals only.
- Keep the networking and operating system current.
- Install a data log that can track all activity on a SCADA system.
- Subscribe to the Information Sharing and Analysis Center (ISAC) coordinated by the Associate of Metropolitan Water Agencies (AMWA) to learn about threats, warnings and prevent damage of water systems. ISAC also offers information about contaminants, weapons, security issue and other information not available to the public. www.WaterISAC.org
- See additional computer security measures at the end of this section.

Preparedness

Planning and preparation is necessary to respond quickly and protect the safety and health of utility personnel and the public. A preparedness plan should be developed and include measures for dealing with acts of terrorism and general security threats. This plan, along with adequate training and system redundancy, will ensure a faster response and recovery from an emergency/disaster.

Preparations include:

- Develop an Emergency Operations Plan that details emergency response capabilities and responsibilities. The plan should improve understanding and cooperation by utility staff, law enforcement officials and medical responders.
- Incorporate findings of vulnerability assessment into the EOP.
- Update the plan often to reflect changes in plant capabilities and system improvements, strive to reduce deficiencies in the plan, and to keep up to date the contact names and phone numbers.
- Include in the plan for terrorism and general security: mission, goals, and objectives of the plan, agreements with other agencies or organizations and scenario-specific plans.
- Preparation for a terrorist threat or breach of security includes knowing what type of attacker you are protecting against. An attacker may be an individual or organized groups. A vandal generally has a goal in mind, but not necessarily a target. A “lone wolf” works alone, and its target is clearly defined. Victims may be targeted based on ethnicity or beliefs. The insider is a dangerous threat due to their detailed knowledge of the system and may be motivated by revenge.
- Threats from terror groups may include domestic extremist groups or terrorist organizations. Domestic extremist groups often resort to break-ins, arson, and construction equipment sabotage and are motivated by political or social agendas. Terrorist organizations often have large numbers of followers and the greatest financial and technological resources. The use of chemical and biological weapons of mass destruction is likely limited to terrorist organizations because of the significant resources required for their development.
- Identifying the “design-basis threat” should be based on the threat potential in a specific area. Equally important as determining potential adversaries is identifying what types of weapons might be used, what or who might be the target of an attack, and understanding the motives and intentions of a utility’s adversaries.
- Preparing for the psychological threat brought on by real or perceived terrorist activities is important. Water utility staff will have concerns of their own or their family’s personal safety could affect decisions and performance during a crisis. Continued stress can lead to physical and mental ailments.
- Essential for an effective emergency response is the education of employees on hazards and their effect on the water system and practicing emergency response.
- Maintain listing of employee training and emergency capabilities in the emergency operations plan. Continue training for reinforcement and introducing new employees.
- Maintain adequate chemical supplies and repair parts on stock.

Response

Every water utility must be prepared to respond effectively to emergencies and disruptive events. Even the most prepared water system is not completely immune to deliberate acts of terrorism.

- Report any suspicious activity or threats by calling 911. Law enforcement will contact the FBI and EPA.
- The FBI is in charge of all terrorist attacks and threats.
- EPA is lead agency on all tampering threats or incidents.
- Utilities shall contact MDNR's Regional Office and inform them of the situation and obtain advice or assistance. The Regional Office will contact Central Office for further assistance.
- Activate use of an alternative water supply if necessary. (see Appendix H)
- Determine the severity of the threat and monitor the situation and change operations accordingly.
- If contamination is detected or a portion of the distribution is damaged, consider whether it is possible to isolate the water in the affected area.
- If water treatment is reduced or stopped, customers should be notified or issued alerts by the media (see Appendix M).
- Restore service to priority customers first.
- If the President declares an area a disaster, the federal government will issue funds for SEMA to disburse.
- Keep track of all emergency related labor hours and work repairs performed. It may be possible to obtain grants or loans from the state or federal government (see Appendix N) following an emergency or disaster.

Response to Threats

ALL BOMB THREATS SHOULD BE TAKEN SERIOUSLY AND NEVER IGNORED. Most bomb threats are delivered by telephone. Another method is through some extortion attempt involving a written letter or e-mail. Below are tips for dealing with bomb and mail threats.

A. Bomb Threats

- Keep the caller on the phone as long as possible and try to get answers to the Bomb Threat Evaluation Form at the end of this section.
- Ask the caller to repeat the message.
- Record every word spoken by the caller if possible.
- Listen carefully and record important information about the caller such as gender, age, language and voice descriptions.
- Pay particular attention to background noises that may give clues as to the location of the caller.
- Immediately call 911 to report the call to the local law enforcement agency. Local police will contact the Missouri State Highway patrol, fire department, ATF, FBI, or other appropriate agencies as necessary.

- Remain available so law enforcement can interview you.
- Educate personnel who answer incoming calls to the facility how to properly handle threats.
- Do not touch suspicious objects.
- Report any suspicious persons and evacuate all non-essential personnel from the building and prevent entry to all but police and essential building personnel.

B. Mail Threats

- Examples of indicators of suspicious mail or package:
 1. The mail contains other materials such as a powder, liquid, or anything unusual.
 2. Postmark showing mailed from a foreign country.
 3. No return address or return address is unusual.
 4. Poorly handwritten or typed address.
 5. Cancellation or postmark shows a different location than the return address.
 6. Excessive postage or excessive weight.
 7. Misspelled words, names or incorrect titles. Title present but no name.
 8. Restrictive markings such as “Personal” Or “Confidential”, particularly when the addressee does not usually receive personal mail at the office.
 9. Mail may be poorly wrapped with several combinations of tape and may be endorsed “Fragile–Handle With Care” or “Rush–Do Not Delay”.
 10. Rigid or bulky packages with excessive tape or string around them.
 11. Packages with protruding wires or aluminum foil.
 12. Ticking sound.
 13. Letter bombs may feel rigid or appear uneven or lopsided.
 14. Packages or envelopes may have and irregular shape, soft spots, bulges or make a sloshing sound.
 15. Oil stains, discolorations, or a strange odor.
 16. Packages with visual distractions.
- What to do if your facility receives suspicious mail:
 1. If you feel pressure or resistance when removing contents from a letter or package – STOP.
 2. Do not shake or empty the envelope or package.
 3. Do not panic or merely discard the envelope or package.
 4. Do not try to clean up powders or fluids.
 5. Place envelope or package in plastic bag or other container to prevent leakage.
 6. If no container is available, cover the mail with clothing, paper, a trashcan, and do not remove the cover.
 7. Isolate the specific area of the workplace so that no one disturbs the item.
 8. Wash hands with warm soap and water for one minute to prevent spreading to face or skin.
 9. Have someone call 911 and tell them what you received, and what you have done with it.
 10. Inform plant superintendent or supervisor.
 11. List all people in the area or room when the suspicious mail was recognized or anyone that may have been in contact with the mail.

12. Give the list to law officials and public health authorities for follow-up, investigations and advice.
13. Remove all contaminated clothing and give to law officials
14. Shower with soap and water as soon as possible.
15. Local law enforcement may contact the local hazmat team, FBI and the local health department.
16. Do not allow anyone to leave the office.

General Computer Security Measures

Data system security is a complex subject and a detailed discussion of the topic is not within the scope of this document. This section provides basic information for securing a location with a broadband direct connection to the Internet.

- Types of Service: High-Speed Internet Access versus a “dial-up connection”.
 1. Broadband access (higher cost but always on and faster access) – There are several different types of broadband access. The most common are digital subscriber link (DSL), fractional T-1 and cable modem.
 2. Dial-up connection – modem to call into a server or a regular telephone.
- What are the risks of a broadband service?
 1. The circuit remains connected, unless you turn off your computer – vulnerable.
 2. Hacker - plants virus software or take remote control of your computer to disrupt your system.
 3. Connection to Internet – identified by Internet Protocol (IP) – with dial-up your IP address changes every time, with DSL your address is fixed, making it easier for “hacker” access.
- Consult Your Service Provider: The service that provides the connection to the site should be consulted regarding security for the connection. Frequently the basic consultation is free and they can also tell you what security will be provided as part of the service and what other security services they provide that you may wish to consider.
- Firewall Protection of the Circuit: As a minimum, all sites should have a hardware firewall securing the connection to the Internet. Software firewalls, installed on each computer at the site, may be used to augment the hardware firewall if desired.
- Internet Browser Security Settings:
 1. The general security of the browser should be set as high as possible, but allow reasonable flexibility when using the Internet.
 2. Downloading and use of plugins should be limited to those required to perform necessary business functions.
 3. Cookies should be disabled.
- File and Print Sharing:
 1. File sharing should be disabled on all computers unless necessary for business purposes. If sharing is enabled, username and password protection should be turned on.
 2. Print sharing should be turned off on all machines unless absolutely needed for business purposes.
- Security Patches.
 1. A procedure should be initiated to periodically check for and install operating system and browser security patches.

- Additional Tips to Reduce Computer Security Risks with Use of High-Speed Connections.
1. Use anti-virus software: scans computer and incoming email for viruses and deletes them (get anti-virus software from web sites of software companies, or buy at retail stores). Regularly update virus software: update routinely w/ “antidotes” to the latest “bugs”- most have a feature that download automatically when on the Internet.
 2. Don’t fall for a “fibbing” email: email attachments may have viruses – links to websites – “don’t forward emails warning of a new virus” – could be a hoax.
 3. If computer is infected, take immediate action. Unplug phone or cable line to your machine – scan computer with anti-virus software and update firewall – make adjustments before reconnection to Internet.
 4. Use strong passwords: at least 8 characters with inclusion of numerals or characters.
 5. Turn off software features you don’t use: i.e. instant messaging, printer sharing, file sharing.
 6. Backup important files: copy onto a removable disc and store.
 7. Report serious incidents: to Internet provider at abuse@yourISPname.com or postmaster@ISPname.com (where ISP is the name of your Internet service provider). Explain the problem and include information from firewall’s log file. May also contact FBI at www.ifccfbi.gov (the FTC) 1-877-FTC-HELP. FTC enters the data into consumer sentinel, a secure online database.

Information Sources:

FTC Publication, “Safe at Any Speed, Security Guidance for Consumers”.

NIST Publications on Computer Security Guidance – available at <http://csrc.nist.gov/publications/index.html>

Additional Sources:

USEPA, Water Infrastructure Security. <http://www.epa.gov/safewater/security/index.html>

Water and Wastewater System Security Self-Analysis: Preconference Seminar Springfield, Missouri. Missouri Rural Water Association. March 2002.

Counter Terrorism and Security in the Water Industry: A Manager’s Guide to Keeping Your Utility Safe (Participant Manual). Les Lampe et al. 2001. AWWA.

Security Analysis & Response for Water Utilities. Nicolas L. Burns, et al of Black & Veatch. 2001 AWWA

Water System Security: A Field Guide. 2002. AWWA.

21 Steps to Improve Cyber Security of SCADA Networks. United States Department of Energy. www.oea.dis.anl.gov. Patrick Burns (202) 287-1703

Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems. Association of State Drinking Water Administrators and National Rural Water Association. May 30, 2002. www.epa.gov/safewater/security

Notification Plan for Tampering Incidents or Threats for Tampering with Public Water Systems. USEPA, Region 7. October 2001.

THREAT EVALUATION FORM

Time _____ am / pm Date: _____ Caller ID# (____) _____ - _____

___ BOMB/EXPLOSIVE ___ SUSPICIOUS MAIL ___ CONTAMINATION

Questions:

1. When is package or device going to explode or release? When did contamination occur?

2. Where is it located? _____
3. What does it look like? _____
4. What is it (chemicals, germs, bomb)? _____
5. What will cause it to explode or release the contents? _____
6. Did you place the bomb, package, device or contaminant? _____
7. Why is the equipment or building being bombed or supply contaminated?

8. What is your name? _____ Address? _____ Phone? _____
9. Who are you affiliated with? _____

Exact Words of Threat:

Caller Information:

Gender: male female unknown (circle one)
 Age: adult _____ teen _____ child _____ unknown _____
 Language (circle one): educated foul irrational incoherent taped

Voice (circle all that apply):

accent ¹	altered	angry	calm	clear	crying
deep	disgusted	excited	familiar ²	high	laughing
lisp	loud	muffled	nasal	nervous	normal
ragged	rapid	raspy	slow	slurred	soft
stutter	whispered	clearing throat	cracked voice	deep breathing	

1. Type of accent? _____
2. Who did it sound like? _____

Background Information (circle all that apply):

animal noise	children noise	clear	computer/keyboard
factory noise	house noise	local	long distance
motor noise	office machines	music	pa system
phone booth	restaurant noise	static	street noise voices

remarks: _____

Contact your Supervisor

Call 911 immediately

Your Name: _____
Your Phone Number: (____) _____ - _____

Water System ID# _____
Water System Name: _____
Address: _____