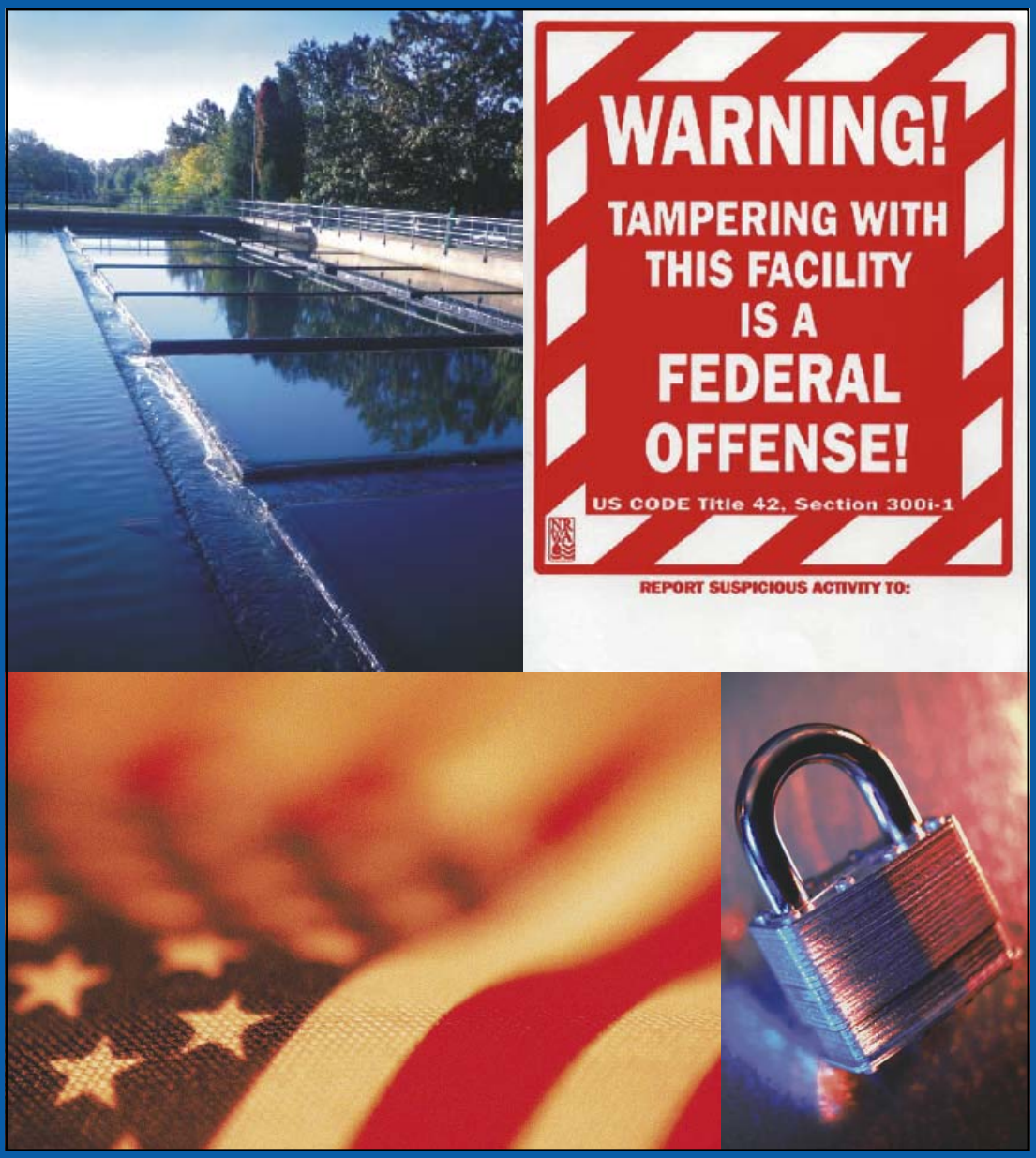
Learner's Guide to Security Considerations for Small Drinking Water Systems

Major Security Considerations When Performing a Sanitary Survey of a Small Water System



Office of Water (4606)
EPA 816-R-03-013
www.epa.gov
August 2003

This document is intended for:

- Use in conjunction with the sanitary survey training for those states that choose to incorporate security provisions into their sanitary survey activities.
- Use as a tool in a basic water security review for systems serving fewer than 10,000 persons.

This document was developed in collaboration with the Association of State Drinking Water Administrators (ASDWA)/EPA Drinking Water Academy (DWA) Sanitary Survey Workgroup.

A Note about this Guide

The primary purpose of this Guide is to identify and explain major security considerations applicable to small drinking water systems. The Guide can be used by state agency personnel in conjunction with a sanitary survey or as a preliminary security review of a small drinking water system.

This Guide is not for use by security specialists, nor does it serve as a vulnerability assessment. Instead, it will be used by personnel who typically visit small systems to evaluate sanitary deficiencies. This Guide will enable users to do a preliminary evaluation of security concerns. This preliminary evaluation should be followed up by a more detailed review by a security specialist using a methodology that conforms with EPA's Six Elements of a Vulnerability Assessment and meets the minimum criteria set forth in the Bioterrorism Act.

This Guide makes references to the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems*. That document is distributed during sanitary survey training courses.

Contents

Introduction

The primary purpose of this Guide is to identify and explain major security considerations applicable to small drinking water systems. The Guide can be used by state agency personnel in conjunction with a sanitary survey or as a preliminary security review of a small drinking water system.

This Guide **is not for use by security specialists, nor does it serve as a vulnerability assessment**. Instead, it will be used by personnel who typically visit small systems to evaluate sanitary deficiencies. This Guide will enable users to do a preliminary evaluation of security concerns. This preliminary evaluation should be followed up by a more detailed review by a security specialist using a methodology that conforms with EPA's Six Elements of a Vulnerability Assessment and meets the minimum criteria set forth in the Bioterrorism Act.

EPA's Six Elements of a Vulnerability Assessment are:

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

A "Multiple Barrier" Approach to Security

Most users of this Guide are familiar with the "multiple barrier" concept in drinking water. Simply stated, this approach builds in as much redundancy as possible to ensure an adequate quantity of safe drinking water. Start with the best possible source and protect that source. Treat the water in a manner consistent with the risks associated with the source. Store and deliver the water in a secure distribution and storage system, and monitor the quality of finished water to ensure that the entire treatment process is working effectively.

In a similar fashion, one might think of a "multiple barrier" approach to security in a water system. Effective security for drinking water systems consists of multiple layers of protection. Like the multiple barrier approach to water quality, the best security approach builds in redundancy, particularly to protect critical system functions or components. An approach to protecting finished water from accidental or intentional contamination might include some or all of the following elements:

- Physical security of the finished water storage facility through fencing, locks, lighting, video cameras, and both external barriers and equipment sensors. These may include redundant systems. For example, if a fence fails to deter an intruder, a sensor may still detect an intruder.

- Monitoring of pressure and selected water quality parameters, such as chlorine residuals, is also a means to help detect unauthorized access to finished water.

- If contamination is detected, some systems have valves that allow operators to isolate and contain the contamination while water is supplied from a redundant source or supply line. Therefore, the system can continue to function for most customers while the situation is remedied.

- Some small systems are interconnected with adjacent drinking water systems to provide alternate supply capacity during system failure, natural disasters, or purposeful system disruption. These interconnections are often established by formal contracts and provide another level of system redundancy.

- If all of these devices and procedures fail or are defeated during an attack by a determined adversary, the system should have an emergency response plan that will enable it to achieve its mission (provide safe water and/or fire flow) as soon as possible after a service interruption.

To enhance a water system's ability to address a wide array of threats, sanitary survey inspectors may want to use the security information provided in this document when inspecting drinking water systems in their state.

Single Point of Failure

Throughout the guide we will identify system components that represent a **single point of failure** (SPF), such as water source, pumps, and storage facilities. A **single point of failure** in the context of drinking water is a system component that, if compromised, would cause a significant undesirable consequence to occur.

An example of a single point of failure is a small system that has a single surface water source and only one transmission line from the source intake to the treatment plant. This one line crosses a highway bridge and is exposed at that point to potential attack. If this one

transmission line were destroyed, the system would be left with only post-treatment-plant storage. This single exposed supply line would be referred to as a "**single point of failure**."

Examples of consequences include the loss of water supply, disruption of supply in excess of system storage capacity, chemical or biological contamination, and, in extreme situations, illness and even death.

Design Basis Threat

Design Basis Threat (DBT) is a common term used by security experts when evaluating threats to various infrastructure systems, including drinking water systems. A DBT is a specific threat scenario developed to use assessing a drinking water system's vulnerability to supply interruption, physical facility damage or destruction, or supply contamination by a determined adversary. The DBT may be developed for threats from inside or outside the system.

The basic approach taken in this Guide for small systems is not to use a formal methodology and develop a specific set of Design Basis Threats. Rather, it assumes that the primary threats to the small drinking water system are associated with inadequate operation. By reducing or eliminating problems identified in this Guide, water suppliers can better analyze the nature of a realistic set of problems facing the system (e.g., natural disaster, vandalism, and crime). Adopting recommendations made during a security review using this Guide will greatly aid implementation of a system's emergency response plan.

Statutory and Regulatory Background

In 1998, President Clinton issued Presidential Decision Directive NSC-63, which established an initiative to protect critical infrastructure, including drinking water systems. In 2002, Congress passed the Bioterrorism Act (Public Law 107-188). This law requires community water systems serving more than 3,300 persons to assess their vulnerability to an attack intended to disrupt the water supply.

Although new statutory requirements based on the threat of terrorist action are the impetus for many new security measures in water systems, good public health protection demands that all systems take the initiative to act responsibly before *an emergency of any nature* – regardless of its cause. This guide will help inspectors understand if systems are meeting this goal.

Before You Begin . . .

Understand the Mission of the Water System

To properly define the security considerations that are relevant for a small water system, the inspector must start with a definition of that system's mission. Only then can the inspector determine, for example, which system functions are critical to the mission. Thinking through the four questions below will help the inspector and the system articulate the system's mission.

A. Who does the system serve? What are the critical assets the system serves?

The inspector should ensure that the system is aware of the critical facilities (e.g., hospitals, government facilities, and emergency shelters) it serves. These critical facilities may be targeted by individuals or organizations intent on harming the populations these institutions serve. It is vital that the managers of these critical facilities be made aware of security concerns that could affect their access to safe drinking water and fire flow, and that the system and the facility plan for that contingency and enhance the security of the supply if necessary.

Questions that the inspector should ask to determine if the operator has focused on the possible security implications of critical facilities include:

i) Would loss of water quantity and quality affect the critical facilities?

It is important that a system understands the water supply requirements of the critical facilities it serves and establishes alternate plans to ensure a continued supply to those critical facilities in the case of an emergency. Failure to provide safe water to these facilities during an emergency could result in the most significant negative effects of that emergency.

ii) How quickly could an alternative source be secured?

Understanding the delays that may affect the supply of safe water will help the system and the critical facilities it serves adequately plan for an emergency.

iii Would the targeting of a critical facility impair the system's ability to provide safe drinking water or water for fire flow? Are there ways to protect against this?

A system may have security vulnerabilities that extend outside of the system if a problem with a critical facility could affect the system's ability to deliver safe water. For example, if a system relies on electricity from a nearby power plant to continue operating, any emergency that affects the power plant also will affect the water system. In this scenario, installing a back-up generator would be a way to safeguard against that vulnerability.

B. Are there any high-density population areas served by the system?

The inspector should also question operators concerning any high-density population areas served by the system (e.g., schools, industrial facilities, high-rise buildings, high-density commercial areas, and shopping districts). Industries that use large amounts of water may be particularly affected by supply interruptions, and it may be appropriate for the supplier to work with these industries to enhance the security of supply and/or help plan for alternative supplies in the event of an interruption.

C. What is the purpose of the service the system provides?

Is the system's main purpose to provide drinking water? Fire flow? Industrial water? All three?

D. What are the mission objectives most critical to the water system?

Consider the following mission objectives as they relate to the water system:

- Treat and supply potable water.
- Provide adequate water supply for fire protection and public safety.
- Maintain public confidence.

I. Utility Management

The operation, maintenance, and security of any water system ultimately depends on management. Management is the process that provides funding and support to ensure continued, reliable operation through adequate staffing, operating supplies, and equipment repair and replacement. Management also consists of policies and procedures that are vital to security (e.g., personnel, protection of system data, planning, and internal and external communication).

Inspectors need to make sure that managers operating in the post-September 11 environment elevate security considerations to a new and higher level. This guide will enable state personnel to review security considerations as part of a sanitary survey. The systems reviewed should seek to fund and implement appropriate remedies.

If there is a specific threat against a system, its operators and managers should be prepared to take rapid and coordinated action with emergency response personnel. Inspectors should also ensure that managers have set up specific procedures to communicate and coordinate quickly with **Local Emergency Planning Committees** (LEPCs) in an emergency.

> For additional detail, see "Chapter 10 - Utility Management" in the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems*.

1. Emergency Response Plan

The Bioterrorism Act requires that each community water system serving more than 3,300 persons certify to EPA that it has developed an emergency response plan that incorporates the results of the vulnerability assessments. The plan must be completed within 6 months of completion of the vulnerability assessment.

Although systems serving fewer than 3,300 persons are not required to conduct vulnerability self-assessments, they should be highly encouraged to do so and to develop emergency response plans.

A. Is an emergency response or contingency plan available and workable?

The water system should have an emergency response or contingency plan that outlines what actions will be taken and by whom. The emergency plan should meet the needs of the facility, the geographical area, and the nature of the emergency likely to occur. Storms, floods, and major mechanical failures should be considered, along with vandalism and other acts.

The inspector should ensure that the plan designates a manager and a secondary contact who will be available in case of emergency regardless of the day of the week or time of day. The plan should be reviewed annually (or more frequently, if necessary) to ensure it is up to date and addresses security emergencies. Larger facilities (i.e., serving more than 3,300 persons) should practice implementing the plan annually.

B. If the system has a plan, is it accessible to all system personnel and appropriate local officials?

The inspector should verify that the information in the plan is available to all water system personnel and local officials including police, emergency personnel, and the state drinking water primacy agency (if appropriate). The plan should not be posted where unauthorized personnel can see it, however, because this would constitute a security risk.

C. Is there an emergency contact list for the emergency response plan? Does the list include basic system information?

As a first step in developing an emergency response plan, the system should have prepared an emergency contact list. Inspectors should verify that it contains the names and telephone numbers of all of the people that the system might need to call in the event of an emergency.

Given the limited ability of most systems to deal with biological or chemical contamination, the emergency contact list should include the following groups:

- Appropriate personnel at the state public health agency.
- The state drinking water primacy agency, if different from the public health agency.
- The regional FBI field office.
- Local police.
- Any other key personnel.

Inspectors should ask if the system has contacted the people listed in the plan and discussed the steps to take in an emergency.

The inspector should ask if the emergency contact list contains basic system information that an operator may need to provide or have readily available during an emergency (e.g., system address, phone number, population served, and number of service connections).

D. Does the emergency plan include workable plans or sections that address the areas listed below?

- Source protection
- Sampling and monitoring
- Emergency or contingency
- Repair and/or replacement
- Contamination assessment

E. Does a representative of the system attend regular LEPC meetings to review the emergency plan?

The inspector should ask if a system representative regularly attends scheduled **LEPC** meetings and speaks with **LEPC** members. By attending meetings and speaking with **LEPC** members, the system forces the **LEPC** and itself to think of the water system as a critical facility and to develop and maintain an adequate emergency response plan.

F. Does the operating staff have the authority to make required emergency response decisions? Are there any policies that could prevent staff members from responding to emergencies effectively?

The inspector should determine if any restrictions limit the decision-making authority of the operations staff. Would this have a negative impact on the system's ability to respond to an emergency? Examples of limited decision-making authority include the lack of authority to adjust chemical feed, hire an electrician, or purchase a critical piece of equipment. Examples of limited administrative policies include lack of support for training and insufficient system funding.

G. Are administrators familiar with, and accountable for, security needs?

Key management personnel should be familiar with security requirements that apply to their system. They should have first-hand knowledge of system needs through security needs assessments, plant visits, and frequent discussions with operators. Lack of first-hand knowledge may result in poor performance, poor decisions, and inadequate response to emergencies.

H. Is there a formal and adequate planning process?

The lack of long-range plans for facility replacement, alternative sources of water, and emergency response can adversely affect a system's long-term and emergency operations performance. Proper emergency response requires careful planning and practice.

Planning should also include a priority ranking for funding for your security needs.

I. Is a hazard communication program in place?

The system should have an inventory of all hazardous chemicals, a Material Safety Data Sheet (MSDS) for each chemical in its inventory, and written procedures for using, transporting, and handling these chemicals.

J. Is there a procedure to receive notification of a suspected outbreak of a disease immediately after its discovery by local health agencies?

The ability to receive information about suspected problems with the water at any time and respond to them appropriately and quickly is critical. Procedures should be developed in advance with the state drinking water primacy agency, local health agencies, and the **LEPC**.

K. Does the system have a communications procedure in place to use immediately after discovery of contamination?

The inspector should verify that the system has procedures in place to notify testing and laboratory personnel of an incident as soon as it detects a contamination problem. If a problem is caused by microbial contaminants, discovering the type of contaminant is critical.

Systems can consult the Public Notification Rule's Tier I Violation provisions for suggestions on how to quickly circulate to its customers information about a problem with the system's water. Example notification methods include radio, door-to-door notices, and television.

Advanced planning on how information can be provided to an alarmed public will be critical in an emergency. The inspector should verify that the system has a working plan to distribute information to customers as soon as possible after discovering a health hazard.

The system should also have contingency plans to telephone or visit facilities that have large populations of people who might be particularly threatened by an outbreak. Such facilities include hospitals, nursing homes, the school department, jails, large public buildings, and large companies. The system should enlist the support of local emergency response personnel to assist in this outreach effort.

2. Data Security

A. Are as-built drawings available?

The inspector should ask if as-built drawings of the system are available. The lack of as-built drawings makes it difficult for staff to perform repairs or shut off affected parts of the system in a timely manner. In the event of an emergency, the speed of repairs often is a critical determinant of the scope and severity of the emergency. Quick repairs may enable a system to limit damage.

B. Are maps, records, and other information stored in a secure location? How often are maps updated? How are maps stored and protected?

Records, maps, and other information should be stored in a secure location when not in use. The inspector should check that access is limited to authorized personnel. Although maps should be available to authorized users, maps should not be left unsupervised, unlocked, or unattended. The inspector should ensure that back-up copies of all data and sensitive documents exist and are stored securely off site and that drawings and as-builts are updated at least once each year.

C. Are copies of records, maps, and other sensitive information labeled confidential, and are all copies controlled and returned to the water system?

Sensitive documents (e.g., schematics, maps, and plans and specifications) distributed for construction projects or other uses should be recorded and recovered after use. The system should discuss with bidders for new projects measures to safeguard its documents.

D. Are vehicles locked and secured at all times?

Vehicles typically contain maps and other information about the operation of a water system. Water system personnel should exercise caution to ensure that this information is secure. Water system vehicles should be locked when not in use or left unattended. The inspector should verify that the system requires employees to remove any critical information about the system or potentially harmful tools (e.g., valve wrenches) before parking vehicles for the night.

E. Is there an overall operation and maintenance (O&M) manual for the facility?

In addition to the standard O&M manual, manufacturer's literature should be available for all pieces of equipment. All of this information, as well as as-built plans of the facility, should be on site or readily available.

F. Are there standard operating procedures (SOPs) at the facility?

SOPs are essential to provide consistent plant operations from one operator to the next. SOPs need to be secured and protected.

G. Does the system store its information on a computer? Is computer access "password protected?"

If the system has one available, a Y2K plan can provide information on the system's computer access policies and any other computer security measures that may be in place.

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 is not shared with others.

H. Is virus protection installed and software upgraded regularly, and are the virus definitions updated at least daily?

The inspector should ask the system if it works with a virus protection company and subscribes to a virus update program to protect records.

I. Does the system have a plan to back-up computers?

Regularly backing up computers to prevent the loss of critical system data stored on them is critical to a system's long-term operation if a computer is damaged or breaks. The inspector should verify that the water system backs up its computers and ask if the system has tested the back-up system to make sure it can recover its data.

J. Is there information on the World Wide Web that can be used to disrupt the system or contaminate its water?

Posting detailed information on a Web site may make a system more vulnerable to attack. The inspector should ask whether the system has examined its Web site and other content on the Web to determine whether any site contains critical information that should be removed.

K. If the system allows Internet bill paying or provides other services over the Internet, does it have a firewall?

Firewalls are computer programs that protect computers from unauthorized access and use over the Internet. A system that offers services over the Web is vulnerable to computer hacking. The inspector should verify that a firewall is in place and is operational.

3. Internal and External Communication

A. Is there effective communication between key management staff, operations staff, local and emergency responders, and state emergency personnel?

Difficulties here can account for problems with the emergency response plan between the organization, the state, and federal agencies. The operator should review previous correspondence to determine the responsiveness of the system to emergencies. Are local law enforcement personnel aware of their response responsibilities to the water system? Do they know where critical system components are located? Is there an agreement in place that specifies the responsibilities of all parties?

B. What is the level of cooperation between the system and the LEPC? Has the system contacted all individuals who may need to be reached during an emergency?

Does the system have an active relationship with the **LEPC**? Does the system know all relevant stakeholders who may need to be contacted in an emergency? This includes local and state elected officials, police, fire, civil defense, public health, environmental, hospital, and transportation officials. How does the system's emergency response plan provide for access by police and fire officials?

C. Does the system have a neighborhood watch for the water system?

It is important that neighbors know whom to call in the event of an emergency or suspicious activity. Have the system's managers met with neighbors to enlist their support? Have the neighbors been given security information and law enforcement contacts? Are the neighbors notified when work is to be undertaken by the system or its contractors to avoid false alarms?

D. Has the system communicated with local law enforcement officials?

Do local law enforcement officials know the system and its physical layout? Do they know the types of suspicious activity that should be monitored during routine patrol? Do they know whom to contact at the water system if they see suspicious activity? Do they have timely access to keys and codes for locked system components?

E. Does the system and specifically do the operators know whom to contact in an emergency?

Is the emergency contact list stored in a place where all authorized personnel can access it? Are all operators aware of its existence? Do operators know whom to contact depending on the nature of the emergency?

F. Do water system personnel have a checklist to use for threats or suspicious calls?

To properly document suspicious or threatening phone calls, a simple checklist can be used to record and report all pertinent information about the calls. Calls should be reported immediately to appropriate law enforcement officials. Are checklists available at every telephone? Does the system have caller ID?

4. Employees

The inspector should be aware that staffing requirements during an emergency may be very different from staffing requirements during normal operation. The inspector should ensure that the system not only has sufficient personnel to operate securely day to day, but that it can respond effectively to an emergency with its current emergency staffing plans.

A. Does the system have adequate staff to handle emergencies?

Emergencies may create the need for more personnel. For example, most states recommend that all systems, even small systems, be staffed **24-7** during an orange or red alert. (See Appendix A: Homeland Security Advisory System for more information on orange and red alerts). Has the system made provisions for staffing during these situations?

The staffing issue should be coordinated with other systems and with the **LEPC**. It is possible, for example, that adjacent or nearby systems can share staff through mutual aid procedures. It also may be possible for other emergency personnel (e.g., police or fire personnel) to provide **24-7** surveillance or protection for the water system. Does the system share staff? Can it increase its staff to necessary levels if an emergency occurs?

B. Are employees adequately trained in security policies and procedures?

There should be an adequate training program that ensures all operators understand security policy and procedures. To properly operate a system under all circumstances, personnel must be adequately trained. Training can be accomplished in a variety of ways, including in-house training conducted by more experienced personnel and state-sponsored training.

C. When hiring personnel, does the system request that local police perform a criminal background check, and does the system verify employment eligibility (as required by the Immigration and Naturalization Service, Form I-9)?

Inspectors should inquire about procedures followed when plant personnel are hired. It is good practice to have all job candidates fill out an employment application. All systems should verify professional references. Background checks conducted during the hiring process can prevent employee-related security concerns from becoming employer-related security problems. At a minimum, systems should check Social Security numbers for authenticity and eligibility status.

If the system uses consultants or contract personnel, the inspector should ask if the system checks on the personnel practices of all providers to ensure that their hiring practices are consistent with good security practices. The system should also conduct its own background checks on individual consultants and contractors.

D. Are system personnel issued photo-identification cards?

For positive identification, all personnel should be issued water system photo-identification cards and should be required to display them at all times. Photo identification will also facilitate identification of authorized water system personnel in an emergency.

E. When terminating employment, does the system require employees to turn in photo IDs, keys, access codes, and other security-related items?

Requiring departing employees, and consultants and other short-term contractors who will no longer work at the water system, to turn in their IDs, keys, and access codes helps limit security breaches that can occur if unauthorized personnel obtain these security-related items from former employees.

F. Does the system use uniforms and vehicles with the system name prominently displayed?

Requiring personnel to wear uniforms and requiring that all vehicles prominently display the water system name helps inform the public when water system staff members are working on the system. If all system personnel and vehicles display the system name, then unauthorized personnel and vehicles without the system name can be an easily identified sign of tampering.

G. Have water system personnel been advised to report security concerns and to report suspicious activity?

System personnel should be trained and knowledgeable about security issues at the 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.

5. Physical Security

A. 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 or water quality) restricted to authorized personnel?

The system should restrict or limit to authorized personnel access to its critical components. This is the first step in enhancing water system security. The inspector should ask if the system:

- Requires photo identification cards to be displayed within the restricted area at all times.
- Posts signs restricting entry to authorized personnel and ensures that assigned staff escort people without proper ID. (All signs should include a number to call to report suspicious activity.)
- Does not offer public tours of critical treatment system components.

B. Are facilities, including wellhouses and pump pits, fenced and are gates locked where appropriate?

Do all facilities have a security fence around the perimeter? Does the fence meet General Services Administration (GSA)[1] standards for fencing? The inspector should ask if the fence perimeter is patrolled periodically to check for breaches and maintenance needs. Does the system have sensors on exterior fences?
All gates should be locked with chains and tamper-proof padlocks that, at a minimum, protects the shank. Inspectors should urge the system to avoid combination locks.

C. Are doors, windows, and other points of entry such as tank and roof hatches and vents kept closed and locked?

The system should lock all building doors and windows, hatches and vents, gates, and other points of entry to prevent access by unauthorized personnel. Are locks checked regularly? A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place.

Are doors and hinges to critical facilities constructed of heavy-duty reinforced material? Hinges on all outside doors should be located on the inside. All windows should be locked and reinforced with wire mesh or iron bars, bolted on the inside.

D. Is there external lighting around the critical components of the water system?

Adequate lighting of the exterior of a water system's critical components is a good deterrent to unauthorized access and may result in the detection of trespassers. Motion detectors that activate switches which turn lights on or trigger alarms also enhance security.

[1] For more information, see http://www.gsa.gov.

E. Are warning signs (tampering, unauthorized access, etc.) posted on all critical components of the water system (e.g., well houses and storage tanks)?

Sample warning sign:

WARNING

Tampering with this facility is a federal offense.
Unauthorized access is strictly prohibited.

Report any suspicious activity to Water System Maintenance at 1-800-555-1234

Warning signs are an effective means of deterring unauthorized access. "Warning - Tampering with this facility is a federal offense" should be posted on all water facilities. "Authorized Personnel Only," "Unauthorized Access Prohibited," and "Employees Only" are examples of other signs that may be useful. Have signs like these been posted around the system? All signs should include a telephone number to call to report suspicious activity.

F. Does the system patrol and inspect source intakes, buildings, storage tanks, equipment, and other critical components?

Frequent and random patrolling of the water system by system staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol. Inspectors should ask systems to consider asking local law enforcement agencies to patrol the water system, advising them of critical components and explaining why they are important.

6. Repairs and Response

A. Does the system have adequate materials on hand to make repairs?

The lack of repair equipment such as a backhoe can prevent the staff from making repairs in a timely manner or digging a path to allow flow to occur on a short-term basis to at least provide for fire protection.

If repair materials are not available, how many hours would it take to obtain these materials at 2:00 a.m.? The inspector should ask if the system can at least obtain two full circle repair bands for each pipe size, two solid couplings for each pipe size, two bell-joint repair clamps, and one length of each type and size of pipe.

II. Source

Finding and protecting an adequate source of supply is essential to public health and to security. Indeed, the source of water supply may well be a "**single point of failure**" for many water systems. A **single point of failure** is a system component that, if compromised, would cause a significant and major undesirable consequence. Thus, a system that has only one source of supply would be vulnerable to a variety of threats. The source could be contaminated or its transmission line disrupted. The source could be compromised in a manner that forces the system to take it off-line for a substantial period of time. If any such threats materialized, the system would be left only with post-treatment plant storage. The source of supply, therefore, would be referred to as a "**single point of failure**."

The following section discusses a number of attributes of water supply sources. Many of these attributes are associated with redundancy—providing methods by which the loss of a single source of supply will not cause system failure.

> For additional detail, see "Chapter 3 - Water Sources" in the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems.*

1. Back-up Sources of Supply

A. Does the system have a back-up source of supply in the event that its primary source of water is contaminated or shut down?

This is the critical question. If there is no back-up source of supply, then the source is likely to become a **single point of failure**. Options for possible back-up sources of supply include the following:

i) Interconnection with a neighboring system.

This is an option for systems near another system with extra water supply available. Inspectors should ask if the system:

- Reviews the contract annually to ensure that the neighboring system still has sufficient extra supplies to meet emergency needs.
- Inspects the inter-connection line annually and flushes or operates valves at least annually.

ii) Back-up well.

Does the system routinely run the pump in the back-up well to ensure the source is still viable and employees can quickly get the well in service? The system should know whether the back-up well is in the same aquifer and ensure that the back-up well has a source of power separate from the primary well's power source.

iii) Tanker trucks or bottled water.

Systems with only one source or no back-up source should have contracts for tanker trucks or with bottled water companies stating the required time frame for delivery. This time frame should be reflected in the emergency plan.

iv) Back-up intake for surface water systems.

The system should have a back-up intake that can be used if the primary intake is damaged or destroyed, but the source quality is unchanged.

v) Back-up transmission line.

If there is a single transmission line from the source to the treatment plant, this transmission line is a **single point of failure**. Inspectors should make sure that the system is aware that some type of back-up or alternative to that transmission line is important.

vi) Minimum source to support fire flow.

The system should consider all uses of the water it supplies, including fire flow. Depending on the nature of the security breach, failure to support fire flow may be a **single point of failure**.

2. Protection of Sources

A. Does the system monitor raw water so that it has a baseline that will allow system operators to know if there has been a contamination incident?

Routine parameters for raw water include pH, turbidity, total and fecal coliform, total organic carbon, specific conductivity, ultraviolet adsorption, color, and odor. The inspector should verify that the system uses methods with adequate sensitivity to monitor these parameters.

B. Does the system provide adequate protection for its sources and related components?

Questions for the inspector to ask include the following:

Ground Water Supplies

1) Control of intake
- Is the intake protected by a fence?
- If yes, does it meet General Services Administration (GSA) standards for fencing?
- Is it of sufficient height?
- Is the bottom secured?
- Is the gate locked?

- Is the fence in good repair?
- Is there a sensor on the gate that will detect a breach of security?
- Is the fence line clear of vegetation?

Surface Water Supplies

In addition to the questions in item #1 above, inspectors visiting systems that have surface water supplies should consider the following questions:

2) Control of watershed
   - Depending on the size of the watershed and the extent of ownership by the system, how is the rest of the watershed protected?
   - Is the physical protection well-constructed, well-maintained, and in good repair?

3) Reservoirs and dams
   - How are these protected?
   - Is the physical protection well-constructed, well-maintained, and in good repair?
   - Are the dams regularly patrolled?
   - Are approaches to the dams and reservoirs locked, lighted, and alarmed?
   - Is recreational use banned or restricted?

C. Does the system adequately protect its transmission line?

If there is a single transmission line from the source to treatment, it could be a **single point of failure**. Therefore, the transmission line should be physically protected against any type of tampering or intrusion.

In addition to the questions in item #1 under Ground Water Supplies, inspectors should consider the following questions:

- Are there pump stations along the distribution route prior to treatment?
- If so, are these pump sites protected?
- Are there any vulnerable points along the transmission line?
- Does the system add disinfectants prior to the treatment plant to increase contact time? Does the system add an oxidant prior to the treatment plant for oxidation of organics that are causing taste and odor problems?
- If the system adds chemicals prior to the treatment plant, are the sites of application secure? If chemicals are stored at the sites of application, are they secure?

3. Protection of the Watershed or Wellhead

A. Is the watershed or aquifer recharge area protected?

Does the system have a wellhead protection program or a watershed protection program? The nature of activities in the recharge zone of the well or watershed and the degree to which they are controlled can influence the quality of the water source. This is especially the case if the aquifer is unconfined.

The SDWA Amendments of 1996 require states to develop Source Water Assessment Programs. On a system-specific basis, this involves determining the recharge area or "area of contribution" for each source, identifying all sources of man-made contamination within this area, and implementing measures necessary to protect the source from contamination. The inspector should verify that the system has made these determinations, which will aid its security planning.

B. What is the nature of the protection area? What is the size of the protected area, and who owns it? How is the area controlled?

Is the protected area industrial, agricultural, forested, residential, or commercial? What has the system done to reduce the threat of potential contamination of the watershed?

Inspectors should note what steps the system has taken to limit access to the protection area. One option is to purchase all or a portion of the area. Ownership with restricted access is the most stringent measure. Another method of limiting access is to restrict activities through zoning restrictions and ordinances. If ordinances are used, how they are enforced? Are there physical restrictions such as full or partial fencing that meets GSA standards? Are access roads gated and locked?

C. Are the entry points to the water system easily seen?

Fence lines should be cleared of all vegetation. Overhanging or nearby trees may provide easy access. The system should avoid landscaping that enables trespassers to hide or conduct unnoticed suspicious activities. It should also trim trees and shrubs to enhance the visibility of its water system's critical components. If possible, it should park vehicles and equipment where they do not block the view of the water system's critical components. The inspector should conduct a visual check to determine if the system implements these measures.

D. Is there an emergency response plan for spills in the water protection area?

Some industries (e.g., petroleum) are required to have emergency spill plans. Potential spill sites should be identified by the system and contingency plans developed in case of a spill. However, because a plan is only paper, the necessary equipment and personnel must be identified and coordination among all relevant agencies that are part of the **LEPC** (fire, police, water system) must be worked out and rehearsed prior to any emergency.

The plan should also include identified upstream dischargers. The inspector should ask if communication channels should be established to alert the system in the event of a contamination problem caused by an upstream discharger.

4. Proper Sealing of Wells

A. Is the well properly sealed?

Many of the components of a well cannot be observed. It is important that the well be properly constructed to prevent contamination of source water through the well casing or sanitary seal.

Wellhead covers or sanitary seals are used at the top of the casing or pipe sleeve connections to prevent contaminated water or other material from entering the well. The inspector should ensure that well covers and pump platforms are elevated above the adjacent finished ground level, which should be sloped to drain away from the well casing.

B. Does the well air vent terminate 18 inches above the ground or floor, or 3 feet above maximum flood level with return bend facing downward and screened? Are well vents and caps screened and securely attached?

Properly installed vents and caps can prevent the introduction of contaminants into the water supply. Ensure that vents and caps serve their purpose and cannot be easily breached or removed. Are the vents and caps checked regularly for signs of tampering or unusual entry?

C. Is the upper termination of the well protected?

The upper termination of the well should be either housed or fenced to protect it from vandalism and vehicle damage. Is the well cover locked? Are the wells inspected frequently for signs of tampering? Are the well houses kept clean?

D. Are observation, test, and abandoned wells properly secured to prevent tampering?

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, cement, grout, or clay slurry. Are there abandoned wells that have not been properly filled?

III. Pumps

Pumping facilities should be protected against all security threats. The perimeter of the property should be fenced, and doors and windows to the building should be locked. Doors should be strengthened with interior steel plates and windows screened with wire mesh. If illegal entry has occurred, then a change in appearance of the inside and outside of the perimeter (e.g., damaged screens) can be helpful to the operator in making that determination quickly. Check around the outside of the building for electrical panels, switches, and valves. Make sure that these cannot be accessed by the public. Pumps are often located in remote areas, so they are more vulnerable to vandalism and intrusion than other parts of the system. Routine monitoring of those areas is essential. Loss of a pump without an adequate back-up is a **single point of failure**.

> For additional detail, see "Chapter 4 – Water Supply Pumps and Pumping" in the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems.*

1. Pumps, Motors, and Appurtenances

A. Does the system have an emergency plan if its pumps fail?

Systems need to have back-up capability to provide water for the system. To ensure adequate pressure and adequate water supplies, the system must look at all potential areas where pumps could fail; these include failure of the pump or power source for the pump and contamination of the well. Questions the inspector should ask the system include:

i) Where is the back-up pump kept?

If the back-up pump is kept in the same place as the primary pump, both may be subject to the same threat.

ii) What are the number (including reserves), location, and type of pumps?

At least two equal pumping units should be provided for each application, except in the case of well pumps where another complete well system provides suitable back-up. A serious deficiency exists, for example, if only one of two raw water pumps is functional. This is a **single point of failure**.

iii) How are operators notified if a pump stops working? Are the pumps equipped with an adequate failure alarm system?

The pump control system should be equipped with failure alarms. If a pump fails to start or stops for any reason other than normal shut-down on the automatic cycle, an alarm system should activate to notify the operator that the system has failed. The type of alarm should also be considered. Many pumping stations are equipped with a flashing light or a horn situated outside the building and activated in the event of a system failure. This type of system depends on someone actually seeing or hearing the alarm and calling the water system operator. This system, of course, is not fool proof. A more dependable system consists of an alarm connected to a telephone line or remote telemetry unit (RTU) and programmed to automatically notify operations personnel until the problem at the pumping facility is corrected.

B. Does the system control pumps through a Supervisory Control And Data Acquisition (SCADA) system?

i) If so, if the SCADA system is down, can personnel operate the system manually?

It is possible that some system operators are entirely dependent today on SCADA systems. This constitutes a **single point of failure**. It is imperative that operators be able to manage the system manually if SCADA systems are not functioning.

ii) Is the SCADA system located with the pumps?

In a small system, the likelihood of co-location of these two types of equipment is high. This increases the likelihood of a significant system failure if both the pumps and SCADA are compromised. Co-location of the SCADA system and pumps could constitute a **single point of failure**.

2. Auxiliary Power Unit

A. Does the system have auxiliary power?

Auxiliary power may be necessary for the continuous operation of a water system. It is especially critical in areas where power outages are frequent and in systems that have limited water storage as part of the distribution system. The auxiliary power unit should not be accessible to the public. The lack of an adequate power supply constitutes a **single point of failure**.

Is the auxiliary power unit (APU) exercised and tested regularly and properly?

The inspector should verify that the APU system is exercised at least once a week with an operator in attendance. Furthermore, the APU system should be exercised under a load. The APU should be used as the source of power for the pumping facility during the exercise period. This procedure ensures that all functions of the APU are tested and working properly. Does the system keep records of APU exercising? Do these records include engine and generator gauge readings?

IV. Water Treatment Process

The water treatment process presents two different security concerns. The system must ensure that its water is protected from microbial contamination through treatment and that chemicals used in the treatment process are properly protected and stored and cannot cause harm to the system.

If the water treatment processes are compromised, the system will fail in its mission to supply safe drinking water to its customers. It still may be able to provide pressurized water for fire flow, but it would not be able to meet its primary mission.

In addition, the chemicals used in the treatment process pose a hazard to the delivery of safe drinking water that could be exploited. Chemicals added at the wrong time in the treatment train or in large amounts could compromise system security. The inspector should ensure that systems have safe delivery, storage, and treatment practices for all chemicals used in the treatment process.

> For additional detail, see "Chapter 6 – Water Treatment Processes" in the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems.*

1. Delivery of Chemicals

A. Are deliveries of chemicals and other supplies made in the presence of water system personnel?

The inspector should verify that the system has established a policy that an authorized person, designated by the water system, must accompany all deliveries. The authorized person should verify the credentials of all drivers. This prevents unauthorized personnel from having access to the water system. It also prevents delivery drivers from unloading chemicals into the wrong tank. Inspectors should ask whether the system has specific procedures in place to handle chlorine gas, which is extremely poisonous. For more information on, see section IV-3.

B. Has the system discussed with its suppliers procedures to ensure the security of their products?

The inspector should ask if the system verifies that suppliers take precautions to ensure that their products are not contaminated. Chain of custody procedures for delivery of chemicals should be reviewed. A designated system employee should inspect chemicals and other supplies at the time of delivery to verify they are sealed and in unopened containers. The employee should match all delivered goods with purchase orders to ensure that they were, in fact, ordered by the water system. The system should keep a log or journal of deliveries. It should include the driver's name (taken from the driver's photo ID), date, time, material delivered, and the supplier's name.

2. Chemical Treatment

A. What chemicals are used?

The system operator should know what chemicals are used, if they are approved for water treatment, and if they are applied properly. The operator *should be aware of possible adverse effects of chemical overfeed addition* to be able to respond to emergency chemical addition situations more effectively.

B. Do daily operating records reflect chemical dosages and total quantities used?

It is extremely critical for the operator to monitor daily chemical use, dose rates, and remaining chemicals in stock. A significant drop in chemicals in stock could indicate a theft and an impending threat to the system.

C. Where are the application points of all the chemicals used?

The system operator should know where all of the application points are and which points are being used. In addition to recording the amount of chemical fed, daily O&M inspections should include checking the valve position for each chemical application point to ensure that chemicals are being injected at appropriate locations.

Does the system add chemicals beyond the treatment plant to maintain adequate levels of residuals in the distribution system? If so, the points of application and the chemicals at those sites should be locked or otherwise secured. The inspector should verify that this is the case.

D. Does the system monitor treated water beyond the chemical addition point so that it has a baseline which will allow system operators to know if there has been a contamination incident?

This is especially important if the system uses chemicals that can pose an immediate threat to public health, even in small quantities (e.g., chlorine dioxide). Routine parameters for raw water include pH, turbidity, total and fecal coliform, total organic carbon, specific conductivity, ultraviolet adsorption, color, odor, and disinfectant levels. The inspector should verify that the system uses appropriately sensitive methods to monitor these parameters.

E. Is chemical storage secure and safe?

Inspectors should pay particular attention to the chemical storage areas because they contain hazardous materials and, therefore, must have adequate security measures in place. Incompatible chemicals (i.e., chemicals that can react and cause harmful effects) should not be stored in the same area. A table of incompatible chemicals is provided in Appendix B.

3. Security Considerations for Gas Chlorination Systems

Facilities that use chlorine gas should have a sign posted (such as the one displayed below) to indicate this. However, inspectors should ensure that the system has used common sense in placing the sign and that it is not easily visible from outside the system.

Chlorine gas is extremely dangerous. It is classified as a poisonous gas and an inhalation hazard by OSHA, EPA, and DOT. Inspectors should consider the special dangers and related security concerns of systems using gas chlorination, including the difficulties of containing a highly corrosive and potentially explosive gas. Exposure to large quantities of chlorine gas (100-150 ppm) can be fatal in 5 to 10 minutes.

A. Physical Security

i) Has the system considered alternatives to chlorine gas?

If a system is located in a densely populated area, a leak could cause severe negative effects. The inspector should determine if the system has considered switching to alternative means of disinfection such as sodium hypochlorite or calcium hypochlorite.

ii) Is the chlorine gas kept in a locked area? Is access to the chlorine gas supply restricted?

Inspectors should ensure that access to the chlorine gas supply is limited and tightly controlled.

B. Delivery

i) Has the system discussed security considerations with its supplier of chlorine gas?

The inspector should ensure that the system has spoken to the manufacturer about the supply and delivery of chlorine gas. What kinds of security procedures does the manufacturer follow? How does the manufacturer ensure the safety and integrity of its chlorine gas shipments?

ii) Have the system and the manufacturer established procedures to ensure the security of their products?

Does the manufacturer tell the system what kind of vehicle will deliver the shipment? Does the system verify that the driver is the same driver that the manufacturer dispatched by checking the driver's license?

iii) Does the system have special measures in place for the delivery of chlorine gas?

The inspector should ask if the system follows any chemical delivery procedures in addition to the system's standard procedures due to the dangers associated with chlorine gas. At a minimum, the shipment should never be left alone during delivery. Other questions to ask include:

- Are containers checked to verify they are all sealed?
- Are all deliveries matched to a purchase order to ensure that they are, in fact, what the system ordered?
- Does the system keep a log of all deliveries?

C. Safety Concerns

i) Does the system have procedures in place to account for the particularly hazardous nature of chlorine gas?

The inspector should ensure that the system has the ability to detect, respond to, and immediately control a gas leak.

ii) How are leaks detected? At what detection concentration are automatic detectors set? Have they been tested recently?

Automatic detectors should be tested at least monthly. The detection level should be set on the low range (1 ppm). Operators need to be alerted as soon as possible if tampering or malfunction occurs.

iii) Are there adequate leak containment provisions? Is the chlorination equipment properly contained?

The Uniform Building Code requires the air treatment system and fire sprinkler water to be totally contained. In the event of tampering, the system must have adequate provisions to contain the gas.

iv) Is there an alarm tied to interruptions in the chlorine feed?

Low system vacuum and low cylinder pressure are the two most common alarm systems. If there is an alarm system, does it work? Does the alarm shut down the flow of water or just initiate an alarm? Inspectors should ensure that system personnel are alerted if the chlorine feed is interrupted because this interruption could indicate a potential tampering problem.

v) Is there a Risk Management Plan, and when was it last practiced? Is there a Process Hazard Analysis?

The Risk Management Plan and the Process Hazard Analysis contain information crucial to a system's ability to respond effectively to an emergency. The risk management plan is an EPA requirement under the Clean Air Act that applies to facilities that store regulated toxic and flammable substances in amounts that exceed threshold levels specified in 40 CFR 68.130. The facility must have a written emergency evacuation plan. The inspector should ask if the system has practiced implementing the plan. OSHA requires that a Process Hazard Analysis be conducted to identify, evaluate, and control hazards involved in any facility with more than 1,000 lbs. of chlorine on hand. Identification and evaluation of the potential hazards and a plan for their control are essential security practices.

V. Storage Facilities

Storage facilities serve two purposes: to maintain an adequate supply of treated water and to pressurize the system. The storage of treated water is an important back-up capability in the event that a system's source is compromised. Pressure is essential not only for adequate fire flow, but to prevent backsiphonage, which would create the threat of contaminants being drawn into the distribution system. Storage facilities are, therefore, very important for system security, but are often located in remote areas and so are more vulnerable to vandalism and intrusion than other areas of the system. Loss of storage facilities could be a **single point of failure** if the system cannot maintain an adequate supply of treated water or sufficient pressure to maintain fire flow.

> For additional detail, see "Chapter 5 – Storage Facilities" in the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems.*

1. Emergency Procedures

A. Are emergency procedures established?

There should be a procedure for detecting and responding to tank contamination. The inspector should determine if the program is adequate. A resource list should be available that contains information on where to obtain essential storage repair materials and services in an emergency. An alternative source of water should be available.

2. Ensuring Adequate Storage Capacity

A. Is the storage capacity sufficient to maintain adequate supply and pressure in the distribution system if the source of supply to the tanks is temporarily interrupted?

Systems that lack adequate storage run the risk of losing pressure. If the source of supply is interrupted, the system should have enough storage to provide water to its critical facilities and sufficient pressure to maintain fire flow until an alternative source can be arranged. Insufficient storage capacity is a **single point of failure**.

B. Can the tank be isolated from the system?

If there is a contamination problem or a structural problem, the system should be able to take its tanks out of operation without having to shut down entirely. This can usually be accomplished if gate valves and a drain pipe have been provided. The inspector should determine if the operator has regularly exercised the valves to ensure their integrity. Has the system installed a sampling tap on the storage tank outlet to test water in the tank for possible contamination?

C. Are procedures established to sustain the water supply when the storage tank is out of service?

Prior to removing the tank from service due to disruption or maintenance, the water system staff should coordinate and practice procedures for sustaining the distribution system pressure. This could be relatively simple in systems that are equipped with adequate back-up storage facilities. A small system that has only one storage tank or limited reserve storage would require a more complex means of maintaining the water supply. This could include operating high service pumps manually and positioning fire hydrant relief valves at various locations within the distribution system.

Are temporary measures established, tested, and practiced thoroughly? Are all water system customers and the fire department notified of the testing well in advance so that conservation and alternative plans can be made to decrease stress on the water system?

3. Physical Security

A. Is the site protected against unauthorized entry?

The storage site should be fenced, lighted, and alarmed to prevent unauthorized entry. Ladders to tops of storage tanks should terminate at least 10 feet above the ground to deter unauthorized climbing.

Inspectors should ask the system if access to the storage tank by non-employees is prohibited and controlled. In situations where there is joint use of a storage tank (e.g., with a private or municipal communications system), the water system should allow only restricted access to personnel who are not its employees.

B. Is all treated water storage covered?

Finished water storage tanks should be covered to prevent contamination. The inspector should ensure that the system owner/operator knows that covered tanks are important not only for protection of public health (e.g., keeping birds and rodents out of the finished water), but also for security. An uncovered tank is a soft target for anyone who wants to introduce contaminants into the finished water (by climbing the tank, by air from crop-dusting planes, etc.).

Covers must be watertight, made of permanent, long lasting material, and constructed to drain freely and prevent contamination from entering the stored water. The surface of a storage tank cover should not be used for any purpose that may result in contamination of the stored water. The roof-to-sidewall joint must be sealed.

C. Is the top access hatch designed correctly and does it close tightly? Are the hatches locked?

Improperly fitted hatch covers are a common problem. Access hatches should be closed with a solid watertight cover and a sturdy locking device. It is not unusual for the wind to lift open an unlocked cover. Padlocks are often cut off, and individuals can then introduce contaminants into the storage facilities.

Inspectors should see if systems have an electronic tampering system on the hatch. This will alert system personnel to potential intrusion.

D. Are control systems reliable and properly protected?

Inspectors should determine if the controls are suitable for the application and are functioning properly. Each storage facility should be equipped with a manual override and a pump failure and low-water-level alarm system. Are they adequately protected from unauthorized visitors and other outside elements?

E. Are overflow pipes and air vents screened?

A mesh screen covering vents and overflows could constitute vulnerable access points to the tank. Inspectors should ensure that screens are kept in good repair and that perimeter security is maintained. Inspectors should verify that regular patrols check that all screens are in good repair and report any damaged screens, which may indicate tampering.

VI. Distribution Systems

Distribution systems contain a large number of access points (e.g., customer connections, fire hydrants, and valve pits). Many of these access points are out of public sight and thus are potential points to introduce biological or chemical contaminants with little probability of detection.

To better protect public health, the water utility must do everything reasonable to prevent and quickly respond to contamination. Prevention can be strengthened significantly by maintaining adequate system pressure, maintaining a chlorine residual throughout the system, and implementing and enforcing a cross-connection-control program (see Section VII).

To properly respond to a contamination incident, the water system should include threats of contamination to the distribution system as part of its emergency response plan (ERP). Emergency communication channels and personnel should be in place. The system should also have a water quality monitoring program, accurate plans of the distribution system (preferably supplemented by a hydraulic model), adequate and functioning isolation valves, and organized water main flushing and disinfection programs.

> For additional detail on distribution systems, see "Chapter 7 – Distribution Systems" in the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems.*

1. Water Quality

A. Is there any point in the system where pressure drops below 20 psi during peak demand or fire response?

Pressures below 20 psi represent a security deficiency and a sanitary deficiency. At this low pressure, a backflow condition could occur which would allow the introduction of contaminants into the system. The system must be designed to supply adequate quantities of water under ample pressure and must be operated to prevent, as far as possible, conditions leading to the occurrence of negative pressure. Continuity of service and maintenance of adequate pressure throughout a public water supply system are essential to prevent backsiphonage. Is there a program to periodically monitor pressures throughout the system?

B. If there is a hydraulic model? Has it been compared to actual conditions? When was it last updated? Does it show any low-pressure conditions?

The inspector should ask if the model accurately represents actual system data. An updated and calibrated model can be used to detect tampering with the system.

2. Repair and Response

A. Is there a line flushing program? Is a systematic unidirectional process used? Are records maintained of frequency, location, and amount of time required?

Inspectors should verify that a distribution line flushing schedule exists and that it is followed. The ability to quickly and systematically flush distribution lines is an important element of responses to accidental or deliberate contamination. Depending on the type of contaminant, a system may have to disinfect the distribution lines.

B. Does the system have an adequate number of valves? Are the valves regularly inspected and exercised, and are records maintained?

The system should have enough isolation valves and blow off valves to effectively shut off and contain affected sections of the distribution system in the case of contamination.

Exercising the valves regularly helps ensure that operators know the location of all valves and are better prepared to rapidly shut off portions of the distribution system if necessary.

All valves in a system should be inspected and exercised annually to ensure they will function properly in an emergency. The inspection should include completely closing, opening, and reclosing each valve until it seats properly. Leaking or damaged valves should be scheduled for repair. A record of valve maintenance and operation, including the number and direction of turns to closure, should be kept.

C. Are there written procedures for isolating portions of the system and repairing water mains?

Written emergency response procedures improve the reliability of the water system. In a small system, this provides a means of handling unexpected problems when the regular operator is not available. In addition, it provides the operator with a means of dealing more effectively with non-routine tasks.

3. Distribution System Monitoring

A. Is at least a trace residual maintained at all sampling points throughout the entire system?

Maintaining a measurable residual throughout the distribution system is a minimal good operational practice. It is important in case microbial contaminants are introduced beyond the treatment facility. The inspector should ask the operator if there are any points in the system that do not have a chlorine residual. If this is the case, then the water quality at those points is suspect and more susceptible to microbial contamination.

B. Is there a plan to increase chlorine residual in the system in the event of an emergency?

The system should have a plan in place to respond to microbial contamination. The plan should include the temporary increase of chlorine residual in the distribution system if necessary to combat the contaminant.

C. Does the system monitor water in the distribution system so that it has a baseline that will allow system operators to know if there has been a contamination incident?

Routine parameters for water in the distribution system include pH, turbidity, total and fecal coliform, total organic carbon, specific conductivity, ultraviolet adsorption, color, and odor. The inspector should verify that the system uses methods with adequate sensitivity to monitor these parameters.

D. Are there an adequate number of residual sampling sites, and do they provide a representative sample of system conditions?

Sampling points should be established so the system can monitor disinfectant residuals in the entire distribution system. Small systems may be able to rotate through a number of sample sites to get an overall picture of disinfectant residuals.

From a security perspective, the objective is not simply to meet the requirements of the Total Coliform Rule. Rather, it is to ensure that the sampling points provide a comprehensive picture of disinfection residuals throughout the system.

E. Are customer water quality complaints aggressively investigated? Is there 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)?

It is critical for the system to be able to respond to and quickly identify potential water quality problems reported by customers. Inspectors should verify that procedures have been developed in advance to investigate and identify the cause of the problem, as well as to alert local health agencies, the state drinking water primacy agency, and the **LEPC** if a problem is discovered. By investigating customer complaints, a system manager may identify water quality problems that can be minimized before they become threats to public health.

Many customers are very sensitive to a change in water quality, taste, or odor, and a customer complaint is often a first line of defense in monitoring finished water quality.

VII. Cross Connections

Every water system should have an established and effective cross connection control program to prevent contaminants from entering the distribution system by way of backflow or backsiphonage. Unfortunately, this is not always the case, particularly in small systems. Sanitary inspectors occasionally find cross connections in facilities that are owned and operated by the water system itself (e.g., the water treatment plant). Evaluating how a system controls cross connections has always been an integral part of a sanitary survey. However, after the events of September 11, 2001, cross connection control is now of much greater importance. The risk of someone intentionally introducing a chemical or biological contaminant through an access point in the distribution system (customer connection, fire hydrant, or valve pit) is now a very real concern; the inspector must ensure that the water utility is taking the appropriate steps to minimize the possibility of such an incident.

For additional detail, see "Chapter 8 – Cross Connections" in the *Learner's Guide: How to Conduct a Sanitary Survey of Small Water Systems.*

A. Does the water system have a written cross connection control program?

The inspector should review the program to determine if the system has the ability to prevent and control cross connections before they become security vulnerabilities. An effective program should have these basic components:

- Authority to establish a program.
- Technical provisions.
- Right of entry and inspections.
- Device testing and repair.
- Certified testers.
- Plan review and inspection of new construction.

B. Is the program active in controlling cross connections?

The best way to see whether the program is active is to assess whether it covers all of the components listed above. If the inspector finds cross-connections in facilities that are owned by the water utility, then it can be assumed that the utility does not adequately understand the issue of cross connections, and more than likely is not controlling them elsewhere in the system, creating a security vulnerability.

C. Are backflow prevention devices installed and tested at each commercial site where backflow could cause a reduction in water quality?

These devices are necessary to prevent deliberate and accidental contamination of the system. They are a critical first line of defense that will deter or delay anyone attempting to contaminate the system.

D. Does the water system have a program to control the use of fire hydrants?

The use of fire hydrants by non-water system personnel has the potential to create serious cross-connection hazards. The inspector should determine if the water system has a program to ensure that if fire hydrants are used by non-water system personnel, appropriate procedures are followed so that no backflow can occur. Inspectors should also ensure that procedures exist to report unauthorized use of fire hydrants. These procedures can alert the system to potential tampering.

E. Does the system have a program to spot facilities in the community such as warehouses or abandoned buildings?

An abandoned building or a warehouse could be a potential location for the deliberate creation of a cross connection. The water system should be aware of these locations and conduct routine patrols of them.

Appendix A: Homeland Security Advisory System

The Department of Homeland Security has developed a strategy to help communicate the current risk of terrorist attacks to federal and state officials, disaster response groups, and the public. The Homeland Security and Advisory System is intended to convey the nature and degree of terrorist threats on a national, regional, or more specific level. One function of the system is to allow the Department to assign threat conditions based on a determination by the Attorney General, in consultation with the Department of Homeland Security. In assigning a threat condition, four factors are considered:

1. Is the threat credible?
2. Is the threat corroborated?
3. Is the threat imminent?
4. How grave is the threat?

The following threat conditions, as they pertain to drinking water systems, have been established:

Low Condition – Green

Low risk of terrorist attacks. Protective measures should focus on:

- Ongoing facility assessments.
- Development, testing, and implementation of emergency plans.

Guarded Condition – Blue

General risk of terrorist attack. Protective measures should focus on:

- Activating employee and public information plans.
- Exercising communication channels with response teams and local agencies.
- Reviewing and exercising emergency plans.

Elevated Condition – Yellow

Significant risk of terrorist attacks. Protective measures should focus on:

- Increasing the surveillance of critical facilities.
- Coordinating response plans with allied utilities, response teams, and local agencies.
- Implementing emergency plans as appropriate.

High Condition – Orange

High risk of terrorist attacks. Protective measures should focus on:

- Limiting facility access to essential staff and contractors.
- Coordinating security efforts with local law enforcement officials and the armed forces as appropriate.

Severe Condition – Red

Severe risk of terrorist attacks. Protective measures should focus on:

- Decision to close specific facilities.
- Redirection of staff resources to critical operations.

Appendix B: Incompatible Chemicals

Purpose: The purpose of this appendix is to assist with the identification of chemicals in use at water treatment plants that should be stored separately. Several chemicals commonly used in water treatment are considered "incompatible" with one another. **The term "incompatible" applies to chemicals that could create a hazardous reaction (such as production of toxic gas, accelerated corrosion, or generation of excessive heat through an exothermic reaction, which could result in an explosion and fire) if mixed together in their concentrated form.** Depending on the type, form, concentration, and amount of chemical, this reaction could be catastrophic, resulting in a loss of life and rendering the water plant inoperable. It is therefore important to store chemicals in a manner that will prevent incompatible substances from coming into contact with one another.

Chemicals commonly used at water treatment plants can be divided into six broad groups of "incompatible" chemicals. These groups are listed in the table below:

Group 1:	Acids
Group 2:	Bases
Group 3:	Salts & Polymers
Group 4:	Adsorption Powders
Group 5:	Oxidizing Powders
Group 6:	Compressed Gasses

To ensure the safety of system personnel and the system itself, each of these groups of chemicals is considered incompatible with the other and therefore should be stored separately.

Examples of chemicals that should not be stored near each other, and the resulting consequence of improper storage include the following:

Examples of Incompatible Chemicals	Hazardous Reactions
Powdered Activated Carbon (PAC), an adsorption powder, mixed with Potassium Permanganate, an oxidizing powder.	Excessive heat generation, with the possibility of explosion and fire. Note: PAC alone is extremely combustible.
Calcium Hypochlorite, a combination base/oxidizer, exposed to moisture or mixed with a viscous fluid such as oil	Excessive heat, fire, or explosion possible. Can provide an ignition source for combustible materials.
Concentrated Sulfuric Acid, a strong acid, mixed with Concentrated Sodium Hydroxide, a strong base.	Excessive heat and liquid explosion. Note: Highly concentrated acids and bases, when mixed together, will have a much more hazardous reaction than weak acids and bases.
Calcium Oxide, a strong base available only as a powder, exposed to moisture.	Excessive heat, fire. Can provide an ignition source for combustible materials.

Liquid chemicals should be stored separately from dry chemicals, regardless of which compatibility group they fall into. Certain concentrated dry chemicals will produce an exothermic reaction when exposed to liquid or even small amounts of moisture. All chemicals should be stored in secure, well-ventilated areas that are free of moisture (especially dry chemicals), freezing conditions (especially liquid chemicals), excessive heat, ignition sources, and flammable/combustible materials. Products such as paint, antifreeze, detergent, oil, grease, fuel, solvent, and beverages should never be stored in the same area as water treatment chemicals.

Following is a list of a number of chemicals commonly used in water treatment, listed by their compatibility group. Because there is a wide range of chemicals available and in use today, inspectors may encounter chemicals not included in the tables below. OSHA Regulation 29.CFR.1910.1200 (Hazard Communication) requires that all organizations that handle hazardous chemicals, including water systems, maintain a Material Safety Data Sheet (MSDS) in their files for each chemical stored on-site. If there is a question regarding the properties or incompatibility of any chemical encountered at a plant, the appropriate MSDS should be reviewed.

Common Water Treatment Chemicals – Compatibility Groups**

Group I: Acids

Name	Common Name	Available Forms[1]
Acetic Acid	Ethanoic Acid	Liquid
Hydrofluosilicic Acid	Fluosilic Acid	Liquid
Hydrogen Fluoride Acid	Hydrofluoric Acid	Liquid
Hydrochloric Acid	Muratic Acid	Liquid
Nitric Acid	Nitric Acid	Liquid
Sulfuric Acid	Sulfuric Acid	Liquid

[1] Liquid and dry chemicals should be stored separately, even if they are in the same compatibility group. Certain concentrated dry chemicals, like calcium hypochlorite and calcium oxide (quickline) will produce an exothermic reaction when exposed to liquid or even small amounts of moisture.

Group II: Bases

Name	Common Name	Available Forms[1]
Calcium Hydroxide	Hydrated Lime	Dry
Calcium Oxide	Quicklime	Dry
Calcium Hypochlorite	HTH	Dry
Sodium Bicarbonate	Sodium Bicarbonate	Dry
Sodium Carbonate	Soda Ash	Dry
Sodium Hydroxide	Caustic Soda, Lye	Liquid, Dry
Sodium Hypochorite	Bleach	Liquid
Sodium Silicate	Water Glass	Liquid

[1] Liquid and dry chemicals should be stored separately, even if they are in the same compatibility group. Certain concentrated dry chemicals, like calcium hypochlorite and calcium oxide (quickline) will produce an exothermic reaction when exposed to liquid or even small amounts of moisture.

Group III: Salts & Polymers

Name	Common Name	Available Forms[1]
Aluminum Sulfate	Alum	Liquid, Dry
Copper Sulfate	Blue Stone	Liquid, Dry
Ferric Chloride	Ferrichlor	Liquid, Dry
Ferric Sulfate	Ferrifloc	Dry
Ferrous Sulfate	Coppras	Liquid, Dry
Polyaluminum Chloride	PACL	Liquid
Polyelectrolytes (Cationic, Anionic, Non-ionic)	Polymer	Liquid, Dry
Sodium Aluminate	Soda Alum	Liquid, Dry
Sodium Fluoride	Sodium Fluoride	Liquid, Dry
Sodium Hexametaphosphate	Glassy Phosphate	Dry
Sodium Phosphate	Sodium Phosphate	Liquid, Dry
Zinc Orthophosphate	Zinc Ortho	Liquid

[1] Liquid and dry chemicals should be stored separately, even if they are in the same compatibility group. Certain concentrated dry chemicals, like calcium hypochlorite and calcium oxide (quickline) will produce an exothermic reaction when exposed to liquid or even small amounts of moisture.

Group IV: Adsorption Powders

Name	Common Name	Available Forms
Powdered Activated Carbon	PAC	Dry
Granular Activated Carbon	GAC	Dry

Group V: Oxidizing Powders

Name	Common Name	Available Forms
Potassium Permanganate	Permanganate	Dry

Group VI: Compressed Gases[2]

Name	Common Name	Available Forms	Incompatible Chemicals Within this Category[3]
Amonia	Amonia	Liquid, Gas	Chlorine
Chlorine	Gas Chlorine	Liquid, Gas	Ammonia
Carbon Dioxide	Dry Ice	Liquid, Gas	-
Sulfur Dioxide	SO_2	Liquid, Gas	-

[2] Each compressed gas should have its own separate storage/feed area.

[3] Chlorine and ammonia are incompatible. They should be stored separately from each other, as well as from all other chemical groups.

**** Each Group of Chemicals must Be Stored Separately – the Groups Are Not Compatible – Operator Safety And/or Operation of the Plant Could Be Compromised.**

Appendix C: Additional Information

Links for additional water system security resources are listed below. Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) addresses the safety and security of drinking water. Presidential Decision Directive 63 establishes an initiative to protect critical infrastructure, including water systems. EPA's Ground Water and Drinking Water Infrastructure Security Homepage offers a number of resources, including training, tools and technical assistance. ASDWA's Critical Infrastructure Protection site contains publications, guidances, and other security-related documents.

Regulatory Background

A. Bioterrorism Act

HTML Version: www.fda.gov/oc/bioterrorism/PL107-188.html
PDF Version: www.epa.gov/gwdw000/security_act.pdf

B. Presidential Decision Directive 63

www.ciao.gov/related/#Policy

Critical Infrastructure Protection

A. EPA Ground Water and Drinking Water Infrastructure Security Homepage

www.epa.gov/safewater/security/

B. ASDWA Critical Infrastructure Protection Site

www.asdwa.org/criticinfpublic.htm

Office of Water (4606)
EPA 816-R-03-013
www.epa.gov
August 2003