A Water Security and Emergency Preparedness Training Workbook for Law Enforcement
A Water Security and Emergency Preparedness Training Workbook for Law Enforcement

EPA
United States Environmental Protection Agency

EPA 817-B-07-001
December 2007
Acknowledgment

The Water Security and Emergency Preparedness Training Workbook for Law Enforcement was prepared by Maureen McClelland of EPA Region I, with the assistance of Jane Downing, Lynn Gilleland, Justin Pimpare, Kevin Reilly, and Mark Sceery, also from EPA Region I. We gratefully acknowledge the insightful comments and assistance of reviewers from within EPA and other federal and state environmental agencies as well as law enforcement agencies.

Disclaimer: The U.S. Environmental Protection Agency (EPA) prepared this training workbook to help law enforcement work with water utilities to effectively plan for and respond to water-related emergencies. This document does not impose legally binding requirements on EPA, States, Tribes, or the regulated community, and it may or may not be applicable to a particular situation, depending on the circumstances. Federal and state decision makers retain the discretion to adopt approaches on a case-by-case basis that may differ from this guide where appropriate.

Notice: Limited Distribution. This document contains information that may not be appropriate for general public dissemination.
List of Contents

Acronyms

Overview

Part I: Drinking Water System Security

  Module 1 — Background
  Module 2 — Water Systems
  Module 3 — Threats
  Module 4 — Vulnerabilities
  Module 5 — Incident Management
  Module 6 — Response
  Summary

Part II: Wastewater System Security

  Module 1 — Background
  Module 2 — Wastewater Systems
  Module 3 — Threats
  Module 4 — Vulnerabilities
  Module 5 — Incident Management
  Module 6 — Response
  Summary

Resources

Appendix A — Forms
<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCSs</td>
<td>Distributed Control Systems</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>EPA</td>
<td>U.S. Environmental Protection Agency</td>
</tr>
<tr>
<td>EPA CID</td>
<td>Criminal Investigation Division</td>
</tr>
<tr>
<td>EPA HSD</td>
<td>Homeland Security Division</td>
</tr>
<tr>
<td>EPA OCEFT</td>
<td>Office of Criminal Enforcement Forensics and Training</td>
</tr>
<tr>
<td>ERPs</td>
<td>Emergency Response Plans</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>ICS</td>
<td>Incident Command System</td>
</tr>
<tr>
<td>JTTF</td>
<td>Joint Terrorism Task Forces</td>
</tr>
<tr>
<td>LEPCs</td>
<td>Local Emergency Planning Committees</td>
</tr>
<tr>
<td>NIMS</td>
<td>National Incident Management System</td>
</tr>
<tr>
<td>NIPP</td>
<td>National Infrastructure Protection Plan</td>
</tr>
<tr>
<td>NRP</td>
<td>National Response Plan</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition system</td>
</tr>
<tr>
<td>VAs</td>
<td>Vulnerability Assessments</td>
</tr>
<tr>
<td>WaterISAC</td>
<td>Water Information Sharing and Analysis Center</td>
</tr>
<tr>
<td>Water SSP</td>
<td>Water Sector-Specific Plan</td>
</tr>
<tr>
<td>WUERM</td>
<td>Water Utility Emergency Response Manager</td>
</tr>
</tbody>
</table>
What Is The Water Security Training Workbook?
The Water Sector, composed of 160,000 public drinking water supplies and 16,000 wastewater treatment facilities, is one of 17 critical infrastructures and key resources defined by various Presidential Decision Directives and the Department of Homeland Security (DHS). The protection of these facilities requires an integrated and coordinated approach among federal agencies, state and local governments, and the private sector. Law enforcement provides a critical role in threat identification, protection, and investigation and should be integrated into the overall protection framework at the local, state, and federal levels. This workbook on water-sector security was developed to increase the awareness of law enforcement personnel to some of the threats and other security issues surrounding public drinking water supplies and wastewater facilities and to help facilitate integration and coordination at the local level.

The workbook will help you understand the basics of how water and wastewater systems operate, as well as what utilities are doing to protect themselves and to respond to contamination threats and incidents.

The workbook is organized into two sections, each with six modules. The first section is dedicated to Drinking Water Security, and the second section deals with Wastewater Security.
Why Is This Workbook Needed?

Physical disruption or contamination of a drinking water system can cause illness, disease, or even death. A water system can be contaminated, damaged, or disrupted through intentional terrorist or criminal action, by an accident, or by a natural disaster. Intentional contamination poses one of the most serious threats to a drinking water system because of the intent to cause damage or to harm human health. When a contamination threat is received or a contamination incident happens, it is critical that a water utility act quickly and effectively to protect public health and the environment.

Wastewater systems provide essential services to residential customers and to commercial and industrial businesses by collecting and treating wastewater and then discharging it to receiving waters. Disruption in wastewater treatment can cause harm to the environment and contaminate waters used as drinking water sources. Components of the wastewater collection system can also provide a means to facilitate the physical harm or destruction of critical buildings and other infrastructure.

This workbook encourages law enforcement to get to know their local drinking water and wastewater systems and to work with them to develop plans for responding to contamination threats and incidents. Law enforcement should also become familiar with the Water Sector-Specific Plan (Water SSP) that was released in June 2007 under the guidance of DHS’s National Infrastructure Protection Plan (NIPP). The Water SSP was created by the U.S. Environmental Protection Agency (EPA) in coordination with Water Sector security partners including the Water Sector Coordinating Council and the Water Government Coordinating Council. It is a broad-based critical infrastructure protection and implementation strategy for drinking water and wastewater utilities, regulatory agencies, and Water Sector training and technical assistance partners.
How Can This Workbook Help Me?
This workbook will help you:

➢ Understand the basic components of a drinking water and wastewater system.
➢ Understand some of the vulnerabilities of these systems.
➢ Understand how a water-sector utility might respond to a contamination threat or incident and what role law enforcement might play.
➢ Understand some of the tools available to assist a utility in responding to an event.

Every drinking water and wastewater system is different, and we encourage law enforcement to get to know the systems in their jurisdiction and become familiar with their emergency response plans.

Who Should Read This Workbook?
This workbook is aimed at law enforcement, although anyone who may be involved in an emergency response concerning drinking water or wastewater systems, such as public health officials, emergency responders, environmental protection officials, and other government officials, may find this workbook useful since it describes the basics of a drinking water and wastewater system and a general process for threat and incident response.
Part 1:
Drinking Water Security
Module 1 — Background

Why Do You Need to Understand Your Drinking Water Systems?

Why should law enforcement be involved?
In today’s uncertain times, there are a growing number of threats that could undermine drinking water. The focus of this workbook is to increase the awareness of law enforcement personnel to some of those threats and other security issues surrounding public water supplies.

Actual events of serious drinking water contamination occur infrequently, and typically do not result in contaminant levels posing near-term health concerns. Nonetheless, with the threats of such events increasing, we cannot take drinking water safety for granted. Greater vigilance by law enforcement, water utilities, and government is vital to ensure that such events do not occur in the public water supplies of this country.

Utility operators want to ensure the safety and security of drinking water resources, but they cannot do the job alone. They are not experts in security; they know how to treat water. Law enforcement’s knowledge and expertise are needed for emergency response purposes and investigative purposes to ultimately bring those who intentionally tamper with a public water supply to justice, whether the act constitutes vandalism, an environmental crime, or an act of terrorism.

What do you need to know?
To assist drinking water utilities with the job of protecting our water supplies, law enforcement should understand the potential threats to water systems. You also need to understand how a water system operates, how each component functions, where systems are located, and what they look like.
Understanding local water system operations, critical resources, and vulnerabilities and knowing the utilities’ contacts will help law enforcement better protect and respond to potential threats and incidents.

**What has happened nationally?**

National alerts have provided the following information:

“[M]embers of Al Qaeda had discussed plans to attack the U.S. drinking water supply.”

“Al Qaeda views critical infrastructure targets in the U.S. as attractive attack options because of their potentially economic and psychological impacts. These targets include water reservoirs and systems, including dams.”

“We know from information . . . from detainees that visible presence of security has disrupted planning and surveillance activities by operatives.”
Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act):

Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) requires water utilities serving more than 3,300 people to:

- Develop vulnerability assessments (VAs).
- Develop emergency response plans (ERPs).
- Prioritize actions to enhance security inside and outside facilities.
- Coordinate with existing Local Emergency Planning Committees (LEPCs).

The Bioterrorism Act also:

- Expands EPA's emergency powers to include “a threatened or potential terrorist attack....”
- Increases penalties for persons who tamper or threaten to tamper with public water systems.

Under the Safe Drinking Water Act, “tampering” is broadly defined as either introducing a contaminant into a public water system with the intention of harming persons or otherwise interfering with the operation of a public water system with the intention of harming persons. This is a federal crime for which up to a 20 year prison term is authorized (for additional information see: http://www.epa.gov/safewater/sdwa/laws_statutes.html).

Tampering with either a drinking water system or a wastewater system is a federal crime enforced primarily by EPA’s Special Agents, fully-sworn Federal law enforcement officers, assigned to the Office of Criminal Enforcement, Forensics, and Training (OCEFT), which oversees both the EPA Criminal Investigation Division (CID) and the EPA Homeland Security Division (HSD). The CID Special Agents investigate allegations of violations of the nation’s Environmental statutes and the Special Agents of the Homeland Security Division assist CID and the FBI with specific technical investigations that may be related to terrorism-including tampering. FBI Special Agents may also investigate allegations of violations of the nation’s environmental laws through a memorandum of agreement (MOU) between the EPA and FBI. These investigations may be conducted in conjunction with state and local law enforcement officers (LEOs). If, during the discovery of a suspected tampering incident at a public water system there is a suspected nexus to terrorism, FBI Special Agents or other LEOs assigned to the local Joint Terrorism Task Force (JTTF) may
respond to the incident, in addition to EPA CID Special Agents, to conduct the investigation. During this initial phase of an incident, it will be determined if the incident is a result of intentional activity, negligence, or other events based on the evidence at hand. In addition, a determination will be made at the initial phases of the incident whether there is a nexus to terrorism. These determinations at the very early stages of an incident will define the scope of the response by LEOs and how soon the utilities themselves can restore service, if it has been affected by the incident. This will be further discussed in Module 6 – Response.

Note: Utilities consider their Vulnerability Assessment a “sensitive” document.

Utilities have several concerns regarding the information contained in their VAs. In response, EPA developed security protocols to protect sensitive information, as described in the Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA.

EPA has developed a number of other guidance materials relating to water security, including a Water Sector-Specific Plan, a Response Protocol Toolbox, a Security Product Guide, VA tools, and ERP guidances. See the Resources section of this handbook and visit http://www.epa.gov/safewater/watersecurity.html.
Module 2 — Water Systems

Are You Familiar with the Drinking Water Systems in Your Jurisdiction?

Learning objectives
After completing this module, participants will be able to:

- Identify water systems in their jurisdiction.
- List and describe critical components of a water system.
- Identify other water systems’ assets in their jurisdiction.

What is a drinking water system?
A drinking water system delivers water for various uses (e.g., domestic, fire protection, critical care facilities, industrial use, irrigation, and sanitation).

Water systems are not all the same. They may or may not be regulated by federal and state governments, depending on the number of people they serve. They may be very simple or very complicated in construction and operations. They may use a ground water source, a surface water source, or both. They may also be small or large, ranging from one that serves a small trailer park to one that serves a major metropolitan area.

Any group of 25 or more people being served by their own water source 60 days a year or more make up a public water system. Public water systems include places such as schools, gas stations, campgrounds, highway rest areas, restaurants, industries, neighborhood associations, and trailer parks.

We will focus on the larger residential and municipal systems. However, much of what is included in here applies to small systems as well.

Water systems may cross multiple geographical boundaries. Your town’s jurisdiction may include components of another town’s water system. Even if the majority of people in your town get water from their own private wells, you may still have assets to protect.
What are the components of a drinking water system?
The major components of most water systems are:

- Water source.
- Transmission.
- Raw water storage.
- Treatment.
- Finished water storage.
- Distribution system.
- Administration and operations.
- Supporting utilities.

All of these components can be vulnerable to attack from different types of adversaries and through different mechanisms.

What is your drinking water source?
Your community may rely on more than one source for its drinking water. The source may be surface water, ground water, or both. The source may lie in another jurisdiction. Area-wide coordination, cooperation, and communication are necessary.

Surface water
A reservoir is an artificial lake or specially built basin in which water is stored. A small reservoir may provide water for just one community. Large reservoirs may supply water for many communities. Underground pipes or aqueducts may transport water hundreds of miles. Lakes, rivers, and streams may also provide water to public drinking water systems.

Ground water
Ground water is accessed through wells drilled into aquifers. An aquifer is an underground rock formation through which water flows slowly. Springs, which begin underground as groundwater, are another source of water. A public well pumps water from underground aquifers and distributes water to the community.
What are source water protection areas?

Drinking water agencies across the country have identified the land areas that provide water to public supply wells and surface water supplies. In these areas, precipitation falling on the land can eventually make its way to a water supply well, reservoir, or river used to provide drinking water. As precipitation moves across the land or through the soil, it may pick up pollutants and carry them to nearby drinking water sources. Because activities on these lands can lead to drinking water contamination, these lands have been designated as drinking water protection areas.

Depending on which state you’re in, these areas may be called:

- Wellhead protection areas.
- Aquifer protection areas.
- Watershed protection areas.
- Source water protection areas.

It is important to keep pollutants off these lands whenever possible.

During heightened alerts, law enforcement might be asked to increase patrols of these areas.

How is drinking water treated?

Surface water typically is treated with chemicals that combine with naturally occurring particles. These particles can then settle and be filtered out to make the water clear. Filtration is important because, besides making the water clear, it removes some germs that are difficult to kill. The water is then disinfected to kill any remaining germs.

Ground water is pumped from aquifers, which can be shallow or deep. Ground water may or may not be disinfected or otherwise treated. Some groundwater systems treat the well water with chemicals to control taste and odor.
What are water treatment processes?
Water treatment can involve the following processes. It is important that you are aware of these processes so that you understand areas of vulnerability. Check with your water supplier to see which apply to your local water system.

- **Intake screening.** As water is drawn into the treatment plant from a surface water source, large items such as logs, sticks, fish, and plants are screened out. If the source is ground water, the screening is done by nature as the water travels through the soil or bedrock into the well, which typically also is screened.

- **Pretreatment.** Chlorine and chemicals, such as alum and lime, are added to the water to help remove impurities and destroy any bad taste or odor. Sometimes chemicals are added to remove excess minerals that make the water hard or cause rust to form.

- **Coagulation and flocculation.** The water is sent into a large basin, where the chemicals cling to the impurities in the water (coagulation) causing them to form larger, heavier particles called floc. These larger particles settle to the bottom of the basin so that the chemicals and the impurities can be removed from the water.

- **Filtration.** From the basin where the floc settles (sedimentation basin) the water travels through filters. Here layers of sand, gravel, and sometimes hard coal (anthracite) remove any other impurities left in the water. Another filter may be used to remove toxic organic substances.

- **Disinfection.** Once everything is removed from the water, a small amount of disinfectant is added to prevent bacteria from growing in the water as it travels through the distribution system. Chlorine and chloramines are used most often.
because they are very common and effective disinfectants, and residual concentrations of them can be maintained to guard against typical biological contamination in the water distribution system. In some places, fluoride is also added. Security concerns associated with chlorine will be discussed later in the text. Typically, disinfection is the last step in the treatment process and the water is referred to as finished water, water that is ready to drink.

**Taste and odor control.** Problems with taste and odors can originate in the source water, within the treatment plant, in distribution systems, and in consumers’ plumbing. There are a variety of chemicals (i.e., potassium permanganate) and treatment processes (i.e., granular activated carbon) used by water utilities to overcome these problems.

Law enforcement should do a walk through of their local water utility and learn the areas of a treatment facility that may store hazardous materials.

**How is finished water stored?**
Most water systems include facilities to store finished water. A clear well is a finished water storage facility (tank) adjacent to the treatment plant. Water can be stored in ground-level tanks, buried tanks, or elevated tanks out in the distribution system. Small water systems often use very small, pressurized tanks to maintain pressure in the distribution system.

Adequate storage capacity is important because it ensures the positive water pressure necessary to prevent contaminants from being drawn into the distribution system.

Storage tanks are a favorite target of vandals and are potentially vulnerable to contamination. Storage tanks have an entry hatch on the roof, just above the ladder, to allow entry into the tank for maintenance activities such as cleaning and inspection.

Many water systems now lock and alarm their storage tank hatches. They may use motion detectors or video cameras to maintain surveillance around water tanks.

On the next page are photos of two different storage tanks. Elevated tanks are used where the topography doesn’t allow placement of a ground-level tank at an elevation that will provide adequate pressure to the system.
These tanks usually have a single pipe from the distribution system. Thus, they “ride on the line” or float on the pressure of the system, and water can go into the tank or come out of the tank through the same pipe, depending on system demand (pressure). Elevated tanks can be entry points for contamination because they usually are not inspected as often as ground-level tanks.

Law enforcement can provide some assistance working with water systems in surveillance and in response to alarms at tanks. Working with water systems to reduce incidents or false alarms will help maintain everyone’s vigilance in securing these important drinking water assets.

How is finished water distributed?
Water is transported from treatment and storage facilities through:

**Water mains**
- Transmission lines (pipes), which carry raw water from its source to a water treatment plant. After treatment, water is usually pumped into pipelines (transmission lines) that are connected to a distribution grid.
- Distribution pipes, which deliver water to customers.

**Pumping facilities.** Some water systems also have booster pumps that help keep the distribution system pressurized. Structurally sound mains and pumping facilities are critical to guard against public health risks. If pressure is lost or if negative pressure is induced, contaminated water or sewage may be pulled back into the system through holes or cracks in the mains.
In a water system, many applications require a pump to move water from one point to another. In addition to transporting water through the system, pump applications include chemical feed systems, sludge removal, air compression, and sampling. It is important that water suppliers have more than one pump serving critical areas; otherwise it may be a vulnerability.

**Hydrants** are used for fire protection and by the water department for operational purposes, such as flushing the system. Any other user should have permission of the water department before hooking up to a hydrant. Depending on your locality, there may be a permit process for hydrant use, or designated hydrants for use by other entities.

Law enforcement may want to check whether their town has a hydrant-use policy that they can help enforce. Always check and see whether or not somebody hooked up to a hydrant should really be there.

Remember - Tampering with a fire hydrant is tampering with a public water system, a federal offense.

**Service connections** include meters and backflow preventers. These devices help reduce the risk of accidental contamination; however, they introduce significant headloss (loss of pressure in the system).

**Valves** are critical for isolating portions of a water system. Improper use of valves can cause severe damage to a water system.

**What are administration and operations functions?**

The operation and maintenance of any water system ultimately depends on management and management’s commitment to maintaining a structurally sound and safe system. The
proper administration and operation of a water system depend on two important assets: employees and computer systems.

**Employees**
A water utility’s employees generally are its most valuable asset. They have knowledge of the system and water quality, and they may also have experience dealing with previous contamination threats. The importance of knowledgeable and experienced personnel is highlighted by the complexity of most water treatment and distribution systems.

Do you know the people who operate your drinking water system? The importance of knowing who runs your water system is a key point that cannot be emphasized enough. The day-to-day experience of water system personnel is an invaluable tool to countering any attack.

Law enforcement should get to know personnel at their water treatment facility and become familiar with the operation:

- Meet your water supply personnel face-to-face.
- Know the key contacts and their telephone numbers.
- Know their official vehicles and any identifying logos or insignias.
- Know what type of identification card they have, if any.

**SCADA**
Supervisory Control and Data Acquisition (SCADA) systems typically are defined as computer-based monitoring and control systems that centrally collect, display, and store information from remotely located data collection transducers and sensors in order to support the supervised remote control of equipment, devices, and automated functions. More and more water systems today rely on SCADA for their routine operations. Unfortunately, these systems can be susceptible to hackers who can cause significant damage.

Essentially every component of the water supply system—pumping and storage, treatment operations, and distribution—depends on energy and could be highly automated. Although these operations are backed up by manual controls, damage could be done if power were disrupted or if the automated systems were temporarily lost due to cyber attack.
What dependencies and interdependencies exist with other sectors?

Water has a variety of uses and is connected to other infrastructures through dependencies and interdependencies. Water systems are dependent upon:

- **Electric power** to run pumps, wells, treatment, operations, repairs, security systems, computers, common rights-of-way.
- **Diesel or propane fuel** for back-up power generation, transportation, and utility vehicles.
- **Natural gas** for heating/cooling systems and for back-up power generation.
- **Telecommunications** for voice and data communications and for automated meter reading systems, general operations, remote monitoring, communications with emergency responders, common rights-of-way.
- **Transportation** for the delivery of chemicals and other materials, for operations and maintenance, repair, and to transport emergency responders and equipment, common rights-of-way.
- **Chemicals** such as chlorine and other treatment chemicals.
- **Banking and finance**, which are important to company operations.
- **Postal and shipping**, which are important to company operations.

A number of other infrastructures depend on water:

- **Agriculture**: irrigation, animal drinking, facility cleaning.
- **Food**: food processing and restaurant operations.
- **Public Health**: hospitals.
- **Emergency services**: fire fighting, emergency water supplies, equipment maintenance.
- **Government**: office operations.
- **IT and Telecomm**: equipment cooling.
- **Energy**: steam production, mining, refining, pollution control.
- **Transportation**: office operations, equipment maintenance, common rights-of-way.
- **Chemical**: manufacturing operations.

It is important to consider how an incident in one sector can adversely affect a water utility.

More information regarding interdependencies will be discussed in Module 3.
Questions

1. Are the source(s) of your drinking water within your jurisdiction? If so, where are they?

2. What types of treatment are used by your local water system and where are the critical facilities located?

3. What chemicals, if any, are stored on site?

4. Can you name one person at the water treatment plant that you might use as a contact?

5. Have you visited your water treatment plant, met personnel, and done a walk through?

6. What other water systems may have facilities or drinking water sources in your jurisdiction?

7. Does your water system have an emergency power source?

8. Do you have a copy of the water system’s emergency response plan?

9. Does your town have a hydrant use policy and, if so, do you have a copy?
Module 3 — Threats

What Are the Potential Threats to Your Drinking Water Systems?

Learning Objectives
After completing this module, participants will be able to:

➤ Understand different threats to water systems.
➤ Be familiar with potential types of contaminants.
➤ Be familiar with different types of attackers.

What are the potential threats?
The Bioterrorism Act of 2002 requires every water utility serving a population of more than 3,300 to conduct a vulnerability assessment of its system to a “terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply.”

The Act requires water suppliers to look at the major components of their water systems, identify the threats to each component, estimate the potential effects of those threats on their systems and their operations, and develop prioritized plans for risk-reduction.

There are three general types of threats to water systems: physical, contamination, and cyber.

Physical threats can range from general vandalism to the use of explosives. Targeting specific facilities within a water system, a perpetrator may wish to vandalize, break in, destroy,
or disrupt that facility’s equipment and operations. There are a variety of ways to disrupt the many different functions of a drinking water system. Physical destruction can occur through the use of explosives, but is not limited to that. It could include the use of treatment chemicals such as chlorine gas. A physical attack that destroys water system components is generally considered more likely than an intentional contamination event. Explosive materials may also be more readily available than chemical/biological contaminants.

Some possible targets are:

- Intakes.
- Reservoirs.
- Wells.
- Dams.
- Pumping stations.
- Exposed mains.
- Treatment plants.
- Power supplies.

Physical interdependencies between the power and water sectors are one of the key infrastructure interdependencies. The effects of the August 14, 2003, power failure on drinking water and wastewater facilities varied from a momentary loss to days without power and water and wastewater service. The lesson learned by these facilities was the need to review their vulnerability assessments and emergency response plans to better address power outages in their plans.

 Interruption of transportation can also hinder the operations of a water treatment facility if it is unable to get the chemicals or the fuel deliveries it needs to continue operations.

Obvious signs of tampering should be reported immediately to law enforcement.
Incident – August 18, 2003
For the fifth day in a row, Detroit Water and Sewerage Department officials asked their 4.3 million customers to boil all tap water before drinking it. Detroit sells water to 126 southeastern Michigan communities. They also say residents should conserve water. Testing water in Michigan takes at least 48 hours and requires two clear indications in a row that water is clean. If both test results show bacteria-free water, the water is considered safe to drink. Thursday’s power outage stopped the pumps, dramatically lowering the pressure and the amount of water in the pipes. That meant bacteria were able to enter the water supply. Detroit’s water system has back-up generators at three of its five plants that should kick in when the main power fails. But the power wasn’t nearly enough to get the water running at high pressures. It was basically there for emergency reasons, such as fires. In 1995, it cost $2 million in equipment alone to provide backup power for a plant that pumps 30 million gallons a day. Some of Detroit’s plants pump 600 million gallons a day. Victor Mercado, director of the water department said his department will closely examine what the department could have done differently (http://www.freep.com).

Incident - Florida, January 2003
At a water treatment plant in Florida, an unknown person or persons crossed a barbed-wire fence, broke open an entry gate, and removed aerator screens. State officials reviewing the case described it as a “professional job” that could have affected the water in more than 4,000 homes. The utility was fined by the state for violating a new law requiring notification of the health department of such break-ins within 24 hours (http://www.heraldtribune.com).

Contamination threats are more difficult to discern than physical threats. The event does not have to actually result in contamination of the water to have an impact. Just the threat of the contamination will alter a system’s operation. Signs of a possible contamination incident include dead or dying animals, fish, or vegetation; empty containers or drums near a water system facility; discarded personal protection equipment such as gloves, goggles, or suits; odors; discolored water; or large numbers of individuals seeking medical help in hospital emergency rooms. Most of these signs can happen for other reasons, so it is important to use sound judgment and not cause undue panic when evaluating an incident.
Currently, there are several hundred contaminants that might be used to contaminate a water supply. A few contaminants have the potential to produce widespread death or illness; a larger group of contaminants could produce localized death or illness in a segment of the population; hundreds of contaminants could disrupt service and undermine consumer confidence.

**Incident – Cyanide- Illinois, 1998**
A white supremacist group calling itself “The New Order” proposed the use of a 50-gallon drum of cyanide to poison the water supplies of major cities. The plot was proposed to divert attention from the groups’ other planned attacks, including bank robberies, unspecified attacks on all capital buildings around the country, post offices, etc. Several members of the New Order were arrested in Illinois in 1998 (“Supremacists had hit list, FBI agent says,” the New York Times [7 March 1998]:A14 [http://www.nytimes.com]).

**Incident - Ricin – South Carolina, 2004**
A letter containing the poison ricin was found in an airport postal office in Greenville, SC. Law enforcement officials were said to view the incident as a case of criminal extortion with no threat to public health or suspicion of terrorism. Quoted officials also said that the enclosed note threatened that large quantities of ricin would be dumped into drinking water reservoirs unless the government conceded to demands regarding working conditions in the trucking industry (http://www.cdc.gov/nceh/hsb/chemicals/mmwr-ricin.pdf).

**Incident – Salmonella typhi – 1984**
In the summer of 1984, members of the Rajneeshee cult contaminated salad bars in The Dalles, Oregon, with the Salmonella bacterium. Cult members had discussed a plan to use sewage and rodents to contaminate the area’s water supply, but this idea was never carried out (http://www.cdc.gov/ncidod/EID/vol5no4/tucker.htm).

**Cyber threats** are a new category of concern. SCADA systems may be susceptible to hacking, which could result in disclosure, theft, or corruption of sensitive information. SCADA system hacking could affect the operation of the system, with potentially harmful effects.
The consequences of a cyber attack may require local law enforcement to assist a water system in notifying the public. And of course, any investigation following such an incident will include local law enforcement.

**Incident – March 2005**

A series of water main breaks occurred in Denver one night. Early indicators pointed to a computer problem that may have resulted in too much pressure in water lines, breaking a valve and causing subsequent water main failures around town. Three breaks reportedly occurred between the hours of midnight and 1 a.m.

Early indicators point to a possible computer problem, which may have sent too much pressure through water lines, breaking the valve and causing subsequent water main failures around town.

Meanwhile, cleanup and repair costs resulting from a massive water main break Friday at Denver Public Schools headquarters could reach $1 million and keep the building closed until at least Thursday. The break in a high-pressure water main filled the building’s sub-basement with four feet of mud in spots.

According to officials, shifting earth most likely caused the 6-inch underground steel water main to sever.

About 200 to 300 employees work in the seven-story building. Some were to report to work today in other locations, while others were getting an unplanned day off. School operations were not expected to be affected, a district spokesman said. (http://www.wwdmag.com/wwd/index.cfm/powergrid/rfah=|cfap=/CFID/1542911/CFTOKEN/34152703/fuseaction/showNewsItem/newsItemId/8780).

**What are the consequences of an attack?**

The consequences of one of the above attacks or threats on a water system are varied. We shall offer some general thoughts on the subject here, but to find out the specific consequences that would affect water systems in your jurisdiction, you need to meet with your water system personnel.

One of the factors that affect the severity of the consequences of an attack is the amount of redundancy built into a water system. A contaminated reservoir may not cause the shut
down of a system with multiple sources and adequate storage. But if that reservoir is the
system’s sole source of water, a “single point of failure,” then losing that reservoir is a
much larger problem.

Law enforcement should work closely with their water system to learn what the system’s
“single points of failure” are, and pay special attention to them, especially in times of
heightened threat levels.

The mission of a water system will also affect the consequences. If a water system puts a
high priority on providing fire protection, then a contaminated source may mean that a
water system does not shut down, but instead issues a “do not use order” or, that it
bypasses a damaged treatment plant or process in order to provide water for fire protection.
These issues are system specific, so again, you need to meet with the water systems in
your jurisdiction to discuss this with them.

**How can water supplies be protected?**
Water systems must identify their critical assets. They need to consider the following kinds
of questions:

- What are the easiest targets?
- What will affect the water system or its customers the most?
- What are the terrorists’ goals?
- What are the terrorists’ constraints?

Asking and answering the right questions will help water system personnel determine the
nature of an attack. Remember that many things must go as planned to result in casualties.
History says this isn’t that easy. However, it is relatively easy to disrupt service or destroy
public confidence.

Law enforcement may be able to assist a water utility in identifying local and regional
threats and in determining what assets are vulnerable. Law enforcement also may be able
to assist the utility in becoming a less attractive target.
Law enforcement’s role in assisting water utilities might focus on:

- Surveillance.
- Patrols.
- Communications/24 hr. contacts.
- Physical security.
- Site control.
- Public notification.
- Investigations.
- Threat warnings.
- Liaison with state and federal law enforcement and intelligence resources.

It is vitally important that law enforcement take any threat to a water system very seriously and notify water contacts. If notified, a water supplier can then take action to minimize risk to the public.

**How are threats delivered?**

Threats can come about through:

- Natural disasters.
- Vandals.
- Disgruntled employees.
- Terrorists.
- Computer hackers.

**Vandals**

**Incident – June 2002 – Wisconsin**

On June 11, during a routine facility check, utility staff discovered that one or more unknown persons had cut the barbed wire on a newly installed security fence and removed the padlock on a tank hatch on the city’s 5 million-gallon elevated water storage reservoir. Immediately acting to protect the city’s 60,000 residents from a possibly contaminated water supply, employees shut off water from the reservoir, isolating it from the distribution system, and began the 48-hour process of draining it. After a thorough investigation and water sampling analysis, the incident was believed to have been caused by local youths. The utility manager said, “Three strands of barb wire were cut at the corners and the padlock was cut off. We assume it was kids using a bolt cutter; it was an impressive feat.”
Incident - October 1999
It had a look that is common to weekend vandalism: the cut screen, the mess in the building, the spilled material. But the building was the control room of the water treatment plant, and the mysterious bright red substance was spilled into the town’s water supply over the weekend. The substance was identified as a vinyl patching compound. The problem was isolated and the residents were supplied with treated water from a neighboring district. Two 13-year-old boys were in custody and facing charges of contaminating a public water supply. (Cox J., Sacramento Bee, October 13, 1999.)

Incident - Plutonium Trichloride Hoax
A letter sent in 1985 contained a threat to poison water with plutonium trichloride (Pl-Cl₃) unless charges associated with a notorious criminal case in New York City were dropped. The letter was judged to be a hoax, despite sampling analyses indicating potentially elevated levels of plutonium. (Questions were raised regarding possible errors with the sampling and analysis protocol.) The incident was announced publicly (4 months later) after press inquiries.

Computer Hackers
Incident - 2000
In Queensland, Australia, on April 23, 2000, police stopped a car on the road to Deception Bay and found a stolen computer and radio transmitter inside. Commercially available technology had been used to turn this vehicle into a pirate command center for sewage treatment along Australia’s Sunshine Coast. The perpetrator’s arrest solved a mystery that had troubled the Maroochy Shire Wastewater System for 2 months. Somehow the system was leaking hundreds of thousands of gallons of putrid sludge into parks and rivers and onto the manicured grounds of a Hyatt Regency hotel. Janelle Bryant of the Australian Environmental Protection Agency said, “Marine life died, the creek turned black, and the stench was unbearable for residents.” Until the suspect’s capture, during his 46th successful intrusion, the utility's managers did not know how the attacks were accomplished. To sabotage the system, the suspect set the software on his laptop to identify itself as “pumping station 4,” then suppressed all alarms. He was the “central control system” during his intrusions, with unlimited command of 300 SCADA nodes governing sewage and
drinking water alike. “He could have done anything he liked to the fresh water,” said Paul Chisholm, chief executive of Hunter Watertech.

Questions

1. What are the potential threats to drinking water?

2. Can you name a few contaminants that might be used in an attack against a water utility?

3. Can you think of a few places in your jurisdiction that might make an attractive place to add contaminants to the water system?

4. What can law enforcement do to assist a water utility in becoming a less attractive target?

5. What can law enforcement do to assist a water utility in understanding potential threats?
Module 4 — Vulnerabilities

Are You Aware of the Vulnerabilities and the Means of Protecting Key Components of a Water System?

Learning objectives
After completing this module, participants will be able to:

- Understand vulnerabilities of water systems.
- Understand some of the contaminant concerns at water systems.
- Understand ways of working with water system personnel to protect their water systems.

What are the potentially vulnerable components of a water system?
Under the Bioterrorism Act of 2002, water suppliers are required to look at the major components of their system, identify the threats to each component, and estimate the potential effects of those threats on their system and its operations.

The following is a brief discussion of some of the vulnerabilities of water systems. This is not intended to be a complete overview. Law enforcement should talk with the managers of the local water system to understand its particular vulnerabilities and how they plan on protecting them.

Potentially vulnerable components of the water system operation include:

- Source water (reservoirs, wells, intake structures, dams, raw water pumps).
- Treatment and chemical storage facilities (treatment plants, treatment processes, chemical storage, booster treatment, clear well).
- Transmission and distribution system (pump stations, valves, hydrants, service connections).
- Finished water storage (storage tanks).
Administration and operations (administration building, billing, maps and records, SCADA).

Supporting utilities (transportation, communication, electricity).

Source water
When looking at reservoirs or wells, water suppliers should ask themselves, “Is it possible for someone to dump or discharge a hazardous substance into the reservoir or well and go unnoticed?”

Reservoirs:
- **Vulnerabilities**: Natural and man-made contamination.
- **Means of protection**: Dilution, treatment, watershed patrols, local residents (water watchers).
- **What to look for**: Cars parked near reservoir access; discarded equipment around the reservoir; illegal entry onto water company lands; unknown persons taking photos or videos of reservoirs. Law enforcement should know any restrictions that are in place around the reservoir (is it closed to hiking? swimming? boating? fishing?) and enforce those restrictions.

Wells:
- **Vulnerabilities**: Natural and man-made contamination; physical damage to the well cap, pump, casing, or power supply.
- **Means of protection**: Fencing, redundancy, well construction, patrols.
- **What to look for**: Signs of intrusion or tampering with the well; illegally parked or abandoned cars in the area; people in the area when inappropriate; discarded equipment, containers or drums; and triggered alarms.

Law enforcement may be asked to increase patrols in the vicinity of reservoirs. Protecting so many assets is challenging and may at times cross lines of jurisdictions and require area-wide cooperation.

Intake Structures
The key question that must be answered is: “How possible is it for someone to intentionally contaminate a water source near the intake and go unseen?” The intake area is not
necessarily adjacent to the treatment plant and is therefore vulnerable to outside intruders who may go undetected by water system personnel. Intakes can be critical assets because contaminants may be introduced or delivered to the intake and pass into the system in a concentrated form, thus challenging the treatment system.

- **Vulnerabilities:** Natural and man-made contamination; physical damage to the pipe or the gate house structure or the valve mechanisms in the gate house.

- **Means of protection:** For the gate house: fencing, locks, alarms, redundancy, proper lighting, patrols. For the intake: multiple physical barriers, if there is a walkway – barbed wire around fence, lock entrance to walkway.

- **What to look for:** Signs of intrusion at the gatehouse such as cut fence, broken locks, doors, or windows; tampering with power or lighting; signs of contamination such as discarded equipment or containers; dead or dying fish; odors; discoloration of the water; boats or swimmers entering the restricted area around the intake; cars parked illegally or abandoned around the area.

**Dams**

- **Vulnerabilities:** Physical damage to the structure itself; damage to the gates, controls, or valves.

- **Means of protection:** Area around the facility should be fenced and locked with tamper-proof locks; adequate lighting; area patrolled periodically; access restrictions on dam and roadways.

- **What to look for:** Broken locks, cut fences, unknown vehicles parked in vicinity, unauthorized surveillance.
Treatment and Chemical Storage Facilities

When looking at the treatment facilities, the water supplier will be looking at the physical security of the facility and asking the following kinds of questions:

- Is the area around the facility fenced and locked?
- Are access roads gated and locked?
- Are the facilities staffed? For how long?
- Is there adequate lighting?
- Are there tamper-proof locks?
- Are there other types of access controls?
- What types of alarms are in place and how are they monitored?
- Are the buildings locked?
- Is the area patrolled periodically?
- Are the facilities inspected and, if so, how often?
- Is a log kept?
- What are the delivery procedures?

Treatment Plants:

- **Vulnerabilities:** Physical damage to the structure itself; damage to pumps, filters, chemicals, storage tanks.
- **Means of protection:** Adequate lighting, tamper-proof locks, alarm system, trimmed shrubbery, periodic patrol of area, limited access on roads into facility, appropriate warning signage in place (e.g., NO TRESPASSING, AUTHORIZED PERSONNEL ONLY).
- **What to look for:** Signs of break in such broken locks, doors, or windows; cut fence; unexplained changes in water quality.

Chemical Storage:

Chlorine is the most commonly used disinfectant in water treatment, but other chemicals are sometimes used which often have advantages over chlorine. The disinfection system can be tampered with to cause harm either by over- or under-
feeding chlorine or turning it off completely. Chlorine gas is very dangerous if accidentally or intentionally released. Liquid chlorine (sodium hypochlorite) is dangerous if mixed with the wrong chemical, which can form chlorine gas. Powdered chlorine (calcium hypochlorite) is dangerous if stored with combustible material (e.g., gasoline diesel, a dangerous fire hazard). Other commonly used disinfectants are chloramines, chlorine dioxide, and ozone.

- **Vulnerabilities:** Physical damage to the storage facility, tampering with the chemical feed system, tampering with the chemicals, intentional release of chlorine from gas cylinder.
- **Means of protection:** Tamper proof locks, delivery standard operating procedures, (e.g., require pre-notification from supplier for bulk deliveries, including driver identification and time of arrival); hazardous chemicals properly labeled and secured.
- **What to look for:** Broken locks, doors, window, discarded containers, deliveries at unusual times.

Law enforcement should be familiar with general chemical delivery procedures and schedules. For example:

- Does the water system in your jurisdiction accept deliveries 24 hours a day or only during business hours?
- Are there multiple delivery points or one central location?
- Do they receive large bulk deliveries from large tanker trucks or do they use smaller trucks with pallet deliveries?
- Where do tanker trucks wait if they cannot make delivery upon arrival?

Law enforcement should be familiar with the chemicals used at their local water utility and have personal protective equipment as needed. Law enforcement should know emergency response procedures established by the water supplier and their community. If a release is determined at the facility, work with your local HAZMAT team to determine the nature and volume of the release.
Transmission and Distribution System

Transmission lines are pipelines that transport raw water from its source to a water treatment plant. After treatment, water is usually pumped into pipelines (transmission lines) that are connected to a distribution grid. The distribution system is an underground network of large and small pipes that transport water. The distribution system grid comes above the ground through pipes and faucets in houses, hydrants on streets, and storage tanks throughout the system. The size of the pipes can vary from as little as 4 inches to 10 feet in diameter.

- **Vulnerabilities**: Various pumps, pump stations, valves, fire hydrants, service connections. These all make convenient entry ways into the distribution system. Abandoned buildings with water service connections may make especially easy targets.
- **Means of protection**: Redundancy in the system, tamper proof locks, caps and covers on valve boxes and fire hydrants.
- **What to look for**: Unauthorized or unmarked truck hooking up to a fire hydrant, unusual activity around abandoned buildings.

▸ **Finished Water Storage (storage tanks):**

- **Vulnerabilities**: Contamination, entry hatches, vents, area around tanks.
- **Means of protection**: Perimeter fences, access roads gated and locked, exterior lighting, vents adequately secured and/or filtered, tamper-proof locks on hatches, alarms monitored.
- **What to look for**: Cut fences, broken locks, unauthorized vehicles in area around tank, triggered alarms.

Law enforcement can provide assistance in working with the water suppliers in surveillance and in responding to alarms at tanks. Working with the water suppliers to limit incidents and reduce false alarms would help maintain everyone's vigilance in securing these important assets. Additionally, means of facility access for law enforcement should be discussed.

Remember: If tampering is suspected because the water supply was actually accessed, then the local JTTF should be notified as soon as possible. This will initiate a chain of events to provide the local LEO's with federal investigative and intelligence support.
Administration and Operations

The proper operation and maintenance of any water system ultimately depends on management.

The employees of a water utility are generally its most valuable asset. They have knowledge of the system and water quality, and may also have experience in dealing with previous contamination threats. The day-to-day experience of water system personnel is an invaluable tool to countering any attack.

- **Vulnerabilities**: Physical, biological, chemical, and psychological threats; theft of sensitive documents (e.g., VA, ERP, plans of distribution system, employee personal info); disgruntled employees or contractors.

- **Means of protection**: Security policy, background checks done on employees, access codes strictly controlled, ID badges required, restricted access to keys for equipment or vehicles.

The above descriptions are just some of the vulnerabilities associated with drinking water systems and are in no way a complete list. Law enforcement is strongly encouraged to contact the water suppliers in their jurisdiction and meet with them to discuss the specific vulnerabilities of those water systems.

Law enforcement might be called upon to help notify customers about water-related issues in the event of a total electrical failure. There is always a need to have reliable communications outside the utility with fire officials, emergency response teams, city command centers, and others.

Law enforcement should know emergency response procedures established by the water supplier and communities.
Questions

1. Have you done a walk through of the water utilities in your jurisdiction with water system personnel?

2. Are you familiar with the type of vulnerabilities particular to these systems?

3. Do you know the critical contacts at the water utility? Do they know yours?

4. Are there abandoned facilities in your community that someone could use to tap into the water system?

5. Are you aware of the emergency response procedures of the water supplier and your community.

6. Do you know who your local HAZMAT team is?

7. Do you have access to distribution maps of the water system?
Module 5 — Incident Management

How do you manage a threat or incident?

Learning objectives
After completing this module, participants will be able to:

➤ Understand the types of threat warnings.
➤ Understand procedures for evaluating threat credibility.
➤ Understand the Incident Command System.

EPA has developed a “Response Protocol Toolbox” that provides information on how to work through the process of determining whether a threat is real or a hoax. This Toolbox will help everyone investigate these incidents thoroughly, safely, and methodically so that the health of the water system personnel, the first responders, and the general public will be protected, and panic will be avoided.

The goal of terrorism is to instill fear in the population, not necessarily to cause damage or casualties. This fear can be caused by the mere threat of contamination—if the threat is not properly managed. For this reason, both threatened and actual contamination incidents are a concern faced by the public at large and, in particular, drinking water professionals.

An important distinction is the difference between a contamination threat and a contamination incident.

What are Types of Threat Warnings?
A threat is an indication that something may have been done to the water system, and may or may not prove to be true. (Maybe a hatch door is found open.)
An incident is a confirmed contamination event or attack on a water system that requires a response.

Water contamination threats and incidents may be of particular concern due to the range of potential consequences:

- Creating an adverse impact on public health within a population.
- Disrupting system operations and interrupting the supply of safe water.
- Causing physical damage to system infrastructure.
- Reducing public confidence in the water supply.
- Long-term denial of water and the cost of remediation and replacement.

The threat management process involves two parallel and interrelated activities:

- Evaluating the threat.
- Making decisions regarding appropriate actions to take in response to the threat.

Historical evidence suggests that the probability of intentional contamination of the drinking water supply is low; however, experts agree that it is possible to contaminate a drinking water system, resulting in adverse public health consequences. The probability of a contamination threat is relatively high.

The first critical step in evaluating a contamination threat is recognition of a threat warning (i.e., an unusual situation that may have presented the opportunity for contamination of the drinking water). The utility will likely be in the best position to observe a threat warning and evaluate whether or not the activity is possible (i.e., first decision point in the “Threat Evaluation” process).

Types of threat warnings include:

- Security breaches.
- Witness account.
- Direct notification by perpetrator.
- Public health notification.
- Notification by law enforcement.
- Notification by news media.
Unusual water quality parameters.

Consumer complaint.

The following is a brief description of several types of threat warnings. To learn more, see Module 1 of the EPA “Response Protocol Toolbox.”

**Security breaches.** This may be the most common type of threat warning encountered by a utility. In most cases, the security breach is most likely related to lax operations or typical criminal activity such as trespassing, vandalism, and theft rather than intentional contamination of the water. However, it may be prudent to assess any security breach with respect to the possibility of contamination.

**Witness account.** Awareness of an incident may be triggered by a witness account of suspicious activity such as trespassing, breaking and entering, and other types of tampering. Utilities should be aware that individuals observing suspicious behavior near drinking water facilities will likely call 911 and not the water utility. In this case, the incident warning technically might come from law enforcement, as described below.

**Direct notification by perpetrator.** A threat may be made directly to the water utility, either verbally or in writing. Historical incidents would indicate that verbal threats made over the phone occur more frequently than written threats. While the notification may be a hoax, threatening a drinking water system is a federal crime.
under the Safe Drinking Water Act as amended by the Bioterrorism Act and should be taken seriously.

- **Notification by public health agency.** Notification from a public health agency or health care providers regarding increased incidence of disease.

- **Notification by law enforcement.** A utility may receive notification about a contamination threat direct from law enforcement, including local, county, state, or federal agencies. As discussed previously, such a threat could be a result of suspicious activity reported to law enforcement, either by a perpetrator, a witness, or the news media. Other information, gathered through intelligence or informants, could also lead law enforcement to conclude that there may be a threat to the water supply. While law enforcement will have the lead in the criminal investigation, the utility has primary responsibility for the safety of the water supply and public health. Thus the utility’s role will likely be to help law enforcement understand the public health implications of a particular threat, as well as the technical feasibility of carrying out a particular threat.

- **Notification by news media.** A threat to contaminate the water supply might be delivered to the news media, or the media may discover a threat. A conscientious reporter would immediately report such a threat to the police, and either the reporter or the police would immediately contact the water utility. This level of professionalism would provide an opportunity for the utility to work with the media and law enforcement to assess the credibility of the threat before any broader notification is made.

*Law enforcement will have the lead in any criminal investigation.*
What is the threat management process?
The goals of threat response and management for a water utility are to evaluate the threat, take necessary steps to protect public health while the threat is being evaluated, confirm the threat, remediate the water system, if necessary, and return the system to safe normal operation as soon as possible.

The threat management process is considered in three successive stages: “possible,” “credible,” and “confirmed.” It is important to stress that the response to an incident will be based on incomplete information. Not everything about the incident can be known in the timeframe in which response decisions must be made.

For example, decisions to isolate a portion of a water system, issue a boil order, or issue a do-not-drink order may have to be made before water quality test results are provided by a laboratory to confirm a contamination incident.

Continued emergency response training allows water suppliers, state officials, and law enforcement to gain an understanding of how to best make decisions without complete information.

Possible
A threat is deemed “possible” if the circumstances indicate the opportunity for contamination.

Example of a possible threat:

- Opened fence to a water tank with the lock cut and lying on the ground, or a phone call to the utility telling the utility that the system has been harmed.

The evaluation to determine if a threat is “possible” should be conducted quickly, with a 1-hour goal to determine if additional actions are needed.

Credible
Once a threat is considered possible, additional information will be necessary to determine if the threat is “credible.” The threshold at the “credible” stage is higher than that at the possible stage, and in general there must be information to corroborate the threat in order for it to be considered “credible.” Often this information is circumstantial but, if enough
indicators suggest something has taken place, then additional response decisions need to be made. Steps should be initiated to confirm the incident and positively identify the contaminant.

The actions to decide if a threat is “credible” should proceed quickly, with a goal of making this determination within 2 to 8 hours.

Preliminary site characterization information will help determine whether a threat is credible. In addition, water suppliers and state drinking water officials should be in contact with other supporting agencies, including law enforcement, to gather information to guide the assessment.

Law enforcement and water utilities need to work together to preserve crime scenes while at the same time allowing water personnel access to facilities as necessary. The expertise of law enforcement agencies (local, state, and federal) will be critical in evaluating the credibility of a contamination threat. They may have knowledge of recent criminal activity in the area that might help establish credibility or support advanced stages of the investigation. The Water Utility Emergency Response Manager (WUERM) should be available to provide expertise on the drinking water system to law enforcement during the threat evaluation.

**Confirmed**

A contamination incident is “confirmed” once conclusive evidence is obtained. Confirmation implies that definitive evidence and information have been collected to establish the presence of a harmful contaminant in the drinking water. Definitive evidence that a system has been contaminated is sought to “confirm” a threat and classify it as an “incident.” The best information is reliable water quality testing data from a laboratory using known analytical methods. This information may not be available right away, especially for biological testing data, because it can take 24 to 48 hours to receive results. Other sources of evidence such as eye witness reports, physical evidence from a location in the water system, or reports by the perpetrators themselves may be adequate to confirm an incident.

**What is the Incident Command System?**

While many entities are involved in a threat evaluation, the Incident Command System (ICS) is the accepted model for managing emergencies. This model allows its users to adopt an organizational structure to fit any situation regardless of jurisdictional boundaries.
The ICS is extremely flexible and can grow or shrink to meet the changing needs of an incident. The organization that assumes responsibility for incident command will vary with the nature and severity of the incident. During the course of managing a contamination threat, the individual designated as incident commander may change as different organizations assume responsibility for managing the situation.

Among the various organizations that may assume incident command responsibility during an intentional contamination situation are:

- **Water Utility** will likely be responsible for incident command during the initial stages of a situation. The utility will retain this responsibility by default unless or until another organization (with proper authority) assumes command. The Water Utility Emergency Response Manager (WUERM) would probably serve as incident commander while the utility maintains overall responsibility for managing the crisis.

- **Drinking Water Primacy Agency** may assume incident command when the utility lacks the resources to manage the threat.

- **Public Health Agency (state or local)** may assume incident command if the situation is a public health crisis (without links to terrorism).

- **Local Law Enforcement** may assume incident command when criminal activity (excluding federal crimes such as terrorism) is suspected. Law enforcement will have the lead in the criminal investigation and will determine whether or not a crime has been committed. EPA CID may assume incident command when the federal crime of tampering with a public water supply is suspected. EPA CID will have the lead in the criminal investigation and will determine whether or not an environmental crime has been committed.

- **FBI** will assume incident command when a crime is suspected to have a nexus to terrorism.

If an organization other than the utility assumes incident command, the utility will play a supporting role during the threat management process. Regardless of which organization is in charge of managing the overall situation, the water utility will maintain responsibility for the water system.
The National Response Plan (NRP) establishes a comprehensive all-hazards approach to manage domestic incidents. The NRP includes the best practices and procedures from several incident management disciplines (e.g., homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector) and combines them into one. It outlines how federal departments and agencies will work together and how the federal government will coordinate with state, local, and tribal governments and the private sector during incidents. For additional information on the National Response Plan (NRP) go to http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml.

For more information on the threat management process, please see Module 2 of the Response Protocol Toolbox, which can be obtained at EPA’s Water Security Web site (http://www.epa.gov/watersecurity).

Law enforcement will have the lead in the criminal investigation and will determine whether or not a crime has been committed.

Law enforcement will assist in the evaluation of any possible threats posed by secondary devices if a confirmed event has occurred.

Law enforcement and water utilities need to work together to preserve crime scenes, while at the same time allowing water utility personnel access to facilities as necessary.

Local law enforcement may assume responsibility for incident command in situations in which criminal activity is suspected. EPA CID may assume incident command when the federal crime of tampering with a public water supply is suspected. EPA CID will have the lead in the criminal investigation and will determine whether or not an environmental crime has been committed.
Questions

1. What is the difference between a contamination threat and a contamination incident?

2. What are some of the threat warnings you might encounter from a water utility?

3. Is there a special notification form?

4. Do you have a diagram of the building facilities of the water utility?

5. Would you be able to access the water utility to respond if there was an incident?

6. Do you have keys to any locks or access codes?

7. Do you know the water utilities emergency response plan and have you practiced with them?
Module 6 — Response

What Do You Need to Know to Respond to a Water Threat or Incident?

Learning objectives
After completing this module, participants will be able to:

- Recognize the framework for evaluating a water contamination threat.
- Describe some of the actions that might be implemented in response to a contamination threat.

What do you need to know about your water systems?
Each water system is unique with respect to age, operation, and complexity. Distribution systems are particularly unique in that many are complex and often an undocumented mix of new and old components.

There are many ways to gain a better understanding of a particular water system, one of which is through its vulnerability assessment.

Meet with your water utility managers and ask them to share what areas they identified as key locations that are vulnerable to intentional contamination.

Law enforcement can assist a water utility in improving physical security around its plant.

What do you need to know about your water system personnel?
The employees of your water utility are generally its most valuable asset in preparing for and responding to water contamination threats and incidents. They have knowledge of the system and water quality, and may also have experience in dealing with previous contamination threats. The day-to-day experience of water system personnel is an invaluable tool to counter any attacks.
What do you need to know about your water system’s emergency response plan?

Water systems were required to revise their emergency response plans to reflect the findings of their vulnerability assessments and to address terrorist threats.

Law enforcement should have a copy of the utility’s emergency response plan and should practice with the utility. How can you practice with a water utility? EPA has developed a Tabletop Exercise CD with several different scenarios involving a water utility. This is a great training tool to bring together all the essential response personnel involved in a water incident, allowing them to practice their roles and to revise any parts of their plan as necessary. (http://cfpub.epa.gov/safewater/watersecurity/tools.cfm#cd).

Law enforcement should also coordinate with their local EPA CID office.

What response actions should be considered at the “possible” stage?

Once a contamination threat has been deemed “possible,” relatively low-level response actions are appropriate. Two response actions that a water utility might consider at this stage are:

- Site characterization.
- Immediate operational response.

Site characterization is one of the critical activities intended to gather information to support the “credible” stage. Site characterization is defined as the process of collecting information from an investigation site in order to support the evaluation of a drinking water contamination threat. This process will normally take place within 2-8 hours of the initial event. Site characterization activities include the site evaluation, field safety screening, rapid field testing of the water, and sample collection. The investigation site is the focus of site characterization activities, and if a suspected contamination site has been identified, it will likely be designated as the primary investigation site. The results of site characterization are of critical importance to the threat evaluation process. Law enforcement serves an integral role in the site characterization process. Certain elements of the site characterization process are to be considered law enforcement investigative functions. These include the supervision of the preservation of the crime scene and the evaluation of information and physical evidence that may be present at the investigation site. The law
enforcement evaluation of any existing physical evidence, including forensic evidence, may aid in the determination of the threats credibility.

Immediate operational response actions are primarily intended to limit the potential for exposure of the public to the suspect water while site characterization activities are implemented. An example of an operational response is isolation of a tank by pumping water into the tank or valving out a tank. These actions generally would not affect consumers and thus generally would not require public notification.

Law enforcement can help by working with the water supplier on any threat or incident that may occur. What you think is inconsequential may have an impact on the water system, its operation, and public health.

What response actions should be considered at the “credible” stage?
The response actions considered at the “credible” stage may involve more effort and have a greater impact than those considered at the “possible” stage. Three response actions that a water utility might consider at this stage are:

- Sample analysis.
- Continuation of site characterization activities.
- Public health response.

Sample analysis and continuation of site characterization are part of the ongoing threat evaluation and are intended to gather information to “confirm” whether a contamination incident did or did not occur. Public health response actions are intended to prevent or limit exposure of the public to the suspect water and are more protective and have a greater impact on the public than the operational response action considered at the possible stage. An example of a public health response action is issuance of a “Do Not Drink” notice.

Know the clearly established communications responsibilities. In an emergency, a water supplier may need to notify large numbers of residents quickly. In the past, local law enforcement has been essential in assisting water supply personnel in notifying the public of emergencies (e.g., “DO NOT DRINK” orders).
Local law enforcement may be asked to participate in public notification strategies. Know the clearly established communications responsibilities. In the past, local law enforcement has been essential in assisting water utility personnel in notifying the public of emergencies.

**What response actions should be considered at the “confirmatory” stage?**

Once a contamination incident has been confirmed, it will be necessary to move into full response mode. Organizations that may be actively engaged in the response include the drinking water primacy agency, the public health agency, emergency response agencies, and law enforcement. All of these participating organizations will likely be coordinated under

<table>
<thead>
<tr>
<th>Threat Evaluation Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Possible</strong></td>
</tr>
<tr>
<td>· Location of security breach.</td>
</tr>
<tr>
<td>· Time of security breach.</td>
</tr>
<tr>
<td>· Information from alarms.</td>
</tr>
<tr>
<td>· Observations when security breach was discovered.</td>
</tr>
<tr>
<td>· Additional details from the threat warning.</td>
</tr>
<tr>
<td><strong>Credible</strong></td>
</tr>
<tr>
<td>· Results of site characterization at location of security breach.</td>
</tr>
<tr>
<td>· Previous security incidents.</td>
</tr>
<tr>
<td>· Real time water quality data from the location of security breach.</td>
</tr>
<tr>
<td>· Input from local law enforcement.</td>
</tr>
<tr>
<td><strong>Confirmatory</strong></td>
</tr>
<tr>
<td>· Results of sample analysis.</td>
</tr>
<tr>
<td>· Contaminant information.</td>
</tr>
<tr>
<td>· Results of site characterization at other investigation sites.</td>
</tr>
<tr>
<td>· Input from primacy agency and public health agency.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Was there an opportunity for contamination?</td>
</tr>
<tr>
<td>· Has normal operational activity been ruled out?</td>
</tr>
<tr>
<td>· Have other “harmless” causes been ruled out?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Do site characterization results reveal signs of contamination?</td>
</tr>
<tr>
<td>· Is this security breach similar to previous security incidents?</td>
</tr>
<tr>
<td>· Does other information (e.g., water quality) corroborate threat?</td>
</tr>
<tr>
<td>· Does law enforcement consider this a credible threat? EPA CID, FBI, JTTF</td>
</tr>
<tr>
<td>· Were unusual contaminants detected during analysis? Do they pose a risk to the public?</td>
</tr>
<tr>
<td>· Do site characterization results reveal signs of contamination?</td>
</tr>
<tr>
<td>· Is contamination indicated by a “preponderance of evidence?”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Notifications within utility.</td>
</tr>
<tr>
<td>· Local law enforcement agencies.</td>
</tr>
<tr>
<td>· EPA CID</td>
</tr>
<tr>
<td>· Drinking water primacy agency.</td>
</tr>
<tr>
<td>· State/local public health agency.</td>
</tr>
<tr>
<td>· EPA CID, FBI</td>
</tr>
<tr>
<td>· Emergency response agencies.</td>
</tr>
<tr>
<td>· National Response Center.</td>
</tr>
<tr>
<td>· Other state and federal assistance providers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Isolate affected area.</td>
</tr>
<tr>
<td>· Initiate site characterization.</td>
</tr>
<tr>
<td>· Estimate spread of suspected contaminant.</td>
</tr>
<tr>
<td>· Consult external information sources.</td>
</tr>
<tr>
<td>· Implement appropriate public health protection measures.</td>
</tr>
<tr>
<td>· Plan for alternate water supply.</td>
</tr>
<tr>
<td>· Analyze samples.</td>
</tr>
<tr>
<td>· Perform site characterization at additional investigation sites.</td>
</tr>
<tr>
<td>· Characterize affected area.</td>
</tr>
<tr>
<td>· Revise public health protection measures as necessary.</td>
</tr>
<tr>
<td>· Provide alternate water supply.</td>
</tr>
<tr>
<td>· Plan remediation activities.</td>
</tr>
</tbody>
</table>
existing incident command structures designed to manage emergencies at the state or local level. States and local entities likely have established their own response plans, which would be in effect if the incident were managed at this level. In any case, the utility will still have a role in the implementation of full response actions; however, it will generally act in a technical support role.

The following is an example of a threat warning with a contamination management threat matrix presented. This is a tabular summary that lists the following at each stage of the threat evaluation:

- Information considered during the threat evaluation.
- Factors considered during the threat evaluation.
- Potential notifications unique to a specific stage of a particular threat warning.
- Potential response actions.

**Security Breach**

**How should law enforcement and water utilities work together to address threats or respond to incidents?**

Law enforcement should meet water supply personnel face-to-face and should know officials’ vehicles and identification badges or card type.

Water suppliers and law enforcement should share critical contact lists.

Law enforcement can share information with police dispatchers on drinking water sources and critical facilities as well as the water utility’s critical contact list.

Before an incident, law enforcement should work with the water utility on how to protect the crime scene.

Law enforcement can work with the water utility and Neighborhood Watch groups to build awareness around suspicious activities near critical water sources and structures.
How do utilities use the Homeland Security Advisory System?
EPA provides guidance to water utilities at each threat alert level of the Homeland Security Advisory System. Work with your water supplier to see what assistance law enforcement can offer at various threat levels. Also know what operational changes may take place at different threat levels. The following is a brief review of the Homeland Security Advisory System and examples of suggested preventative measures. For more detailed information see the EPA document *Guarding Against Terrorist and Security Threats: Suggested Measures for Drinking Water Utilities* (August 2004).

**Homeland Security Advisory System**

**Green**

**Low Risk of Terrorist Attack**

Water utilities focus on the continuing assessment of their facilities and developing, testing, and implementing their emergency response plans. Water utilities should post emergency evacuation plans in an accessible, secure location near the entrance for immediate access by law enforcement.

Intruders, trespassers, and those detained for tampering should be prosecuted to the fullest extent possible.

**Blue**

**General Risk of Terrorist Attacks**

Protective measures by the water utility focus on activating employee and public information plans, exercising communication channels with response teams and local agencies, and reviewing and exercising emergency plans.

The water utility will reaffirm communication and coordination protocols (embedded in the utility’s emergency response plan) with local authorities such as police and fire departments, HAZMAT teams, hospitals, and other first responders.

Access to mission-critical facilities should be controlled.

The water utility is also encouraged to develop intelligence contacts with state and local law enforcement, EPA CID field offices, FBI field offices, and the Water Information Sharing and Analysis Center (WaterISAC).
**Yellow**

*Significant Risk of Terrorist Attack*

Protective measures should focus on increasing surveillance of critical facilities; coordinating response plans with allied utilities, response teams, and local agencies; and implementing emergency plans, as appropriate.

The water utility may ask law enforcement to increase surveillance activities in source water and finished water areas.

Law enforcement should also have the critical contact lists available for all water utility personnel.

**Orange**

*High Risk of Terrorist Attack*

Protective measures by the water utility should focus on limiting facility access to essential staff and contractors, and coordinating security efforts with local law enforcement officials and the armed forces, as appropriate.

**Red**

*Severe Risk of Terrorist Attack*

Protective measures should focus on the decision to close specific facilities and the redirection of staff resources to critical operations. As appropriate, water utilities will request increased law enforcement and/or security agency surveillance, particularly of critical assets and otherwise unprotected areas.
Questions

1. Do you know what threats are of concern to the water systems in your jurisdiction?

2. Do you know the key utility personnel contacts for the water systems in your jurisdiction?

3. Do you have a copy of the water utility emergency response plans for the utilities in your jurisdiction, and have you conducted any exercises with the utilities to test the plan?

4. Are you familiar with the response actions your utilities might take to possible, credible, or confirmed incidences?

5. Have you worked with the water utility personnel to explain how they should protect a potential crime scene?

6. Do you work with the utilities in your jurisdiction to provide appropriate assistance for changing National and local threat levels?
Summary

The following law enforcement actions are suggested throughout Part 1: Drinking Water Security.

Note: Utilities consider their Vulnerability Assessment a “sensitive” document.

During heightened alerts, law enforcement might be asked to increase patrols of these areas.

Law enforcement can provide some assistance working with water systems in surveillance and in response to alarms at tanks. Working with water systems to reduce incidents or false alarms will help maintain everyone’s vigilance in securing these important drinking water assets.

Law enforcement should learn the areas of a treatment facility that may store hazardous materials.

Law enforcement may want to check whether their town has a hydrant-use policy that they can help enforce. Always check and see whether or not somebody hooked up to a hydrant should really be there. Remember: Tampering with a fire hydrant is tampering with a public water system – a federal offense.

Law enforcement should get to know personnel at their water treatment facility and become familiar with the operation:

- Meet your water supply personnel face-to-face.
- Know the key contacts and their telephone numbers.
- Know their official vehicles and any identifying logos or insignias.
- Know what type of identification card they have, if any.

Law enforcement should be aware of a water system’s “single points of failure” and pay special attention to them, especially in times of heightened threat levels.
Law enforcement may be able to assist a water utility in identifying local and regional threats and in determining what assets are vulnerable. Law enforcement also may be able to assist the utility in becoming a less attractive target.

Law enforcement’s role in assisting water utilities might focus on:

- Surveillance.
- Patrols.
- Communications/24 hr. contacts.
- Physical security.
- Site control.
- Public notification.
- Investigations.
- Threat warnings.
- Liaison with state and federal law enforcement and intelligence resources.

Law enforcement may be asked to increase patrols in the vicinity of reservoirs. Protecting so many assets is challenging and may at times cross lines of jurisdictions and require area-wide cooperation.

Law enforcement should be familiar with general chemical delivery procedures and schedules. For example:

- Does the water system in your jurisdiction accept deliveries 24 hours a day or only during business hours?
- Are there multiple delivery points or one central location?
- Do they receive large bulk deliveries from large tanker trucks or do they use smaller trucks with pallet deliveries?
- Where do tanker trucks wait if they cannot make delivery upon arrival?

Law enforcement should be familiar with the chemicals used at their local water utility and have personal protective equipment as needed. If a release is determined at the facility, work with a local HAZMAT team to determine the nature and volume of the release.
Law enforcement can provide assistance in working with the water suppliers in surveillance and in responding to alarms at tanks. Working with the water suppliers to limit incidents and reduce false alarms would help maintain everyone’s vigilance in securing these important assets. Additionally, means of facility access for law enforcement should be discussed. Should an alarm sound, local law enforcement are encouraged to coordinate with their local EPA CID office or their local FBI office.

Law enforcement might be called upon to help notify customers about water-related issues in the event of a total electrical failure. There is always a need to have reliable communications outside the utility with fire officials, emergency response teams, city command centers, and others.

Law enforcement should know emergency response procedures established by the water supplier and communities.

Law enforcement and water utilities need to work together to preserve crime scenes while at the same time allowing water personnel access to facilities as necessary. The expertise of law enforcement agencies (local and state) might be particularly helpful in evaluating the credibility of a contamination threat. They may have knowledge of recent criminal activity in the area that might help establish credibility or support advanced stages of the investigation. The Water Utility Emergency Response Manager (WUERM) should be available to provide expertise on the drinking water system to law enforcement during the threat evaluation.

Law enforcement can assist a water utility in improving physical security around its plant.

Law enforcement should have a copy of the utility’s emergency response plan and should practice with the utility. How can you practice with a water utility? EPA has developed a Tabletop Exercise CD with several different scenarios involving a water utility. This is a great training tool to bring together all the essential response personnel involved in a water incident, allowing them to practice their roles and to revise any parts of their plan as necessary. (http://cfpub.epa.gov/safewater/watersecurity/tools.cfm#cd). Law enforcement should also coordinate with their local EPA CID office.
Law enforcement can help by working with the water supplier on any threat or incident that may occur. What you think is inconsequential may have an impact on the water system, its operation, and public health.

Local law enforcement may be asked to participate in public notification strategies.

Law enforcement should meet water supply personnel face-to-face and should know officials’ vehicles and identification badges or card type.

Water suppliers and law enforcement should share critical contact lists.

Law enforcement can share information with police dispatchers on drinking water sources and critical facilities as well as the water utility’s critical contact list.

Before an incident, law enforcement should work with the water utility on how to protect the crime scene.

Law enforcement can work with the water utility and Neighborhood Watch groups to build awareness around suspicious activities near critical water sources and structures.

Law enforcement should also have the critical contact lists available for all water utility personnel.
Part 2: Wastewater Treatment System Security

Module 1 — Background

Why Do You Need To Understand Your Wastewater Treatment System?

Why should law enforcement be involved?
Like safe drinking water, properly treated wastewater is critical to public health. While the public is much less sensitive to wastewater than it is to drinking water, wastewater treatment systems are important to every day life.

Wastewater systems provide essential services to residential, commercial, and industrial customers by collecting and treating wastewater and discharging it into receiving waters. We don’t realize that the quality of the water in our nation’s lakes, rivers, and streams depend on properly treated wastewater. We also take for granted the proper functioning of the collection system. For example, what would happen if we weren’t able to flush our toilets due to a disturbance in the sewer line?
In today’s uncertain times, there are a growing number of threats that could undermine a wastewater system. The focus of this training workbook is to increase the awareness of local law enforcement personnel to some of those threats and other security issues surrounding wastewater treatment facilities and the collection system.

Wastewater treatment is the “last line of defense” against water pollution. Our community’s wastewater treatment plant is a vital part of the nation’s effort to protect water resources.

Actual disruptions of collection systems and wastewater treatments occur infrequently, and typically not at levels posing near-term health concerns. Nonetheless, with the threats of such events increasing, greater vigilance by law enforcement, wastewater facilities, and government is vital to ensure that such events do not occur in the wastewater systems of this country.

What do you need to know?

To assist wastewater utilities with the job of protecting our wastewater systems, law enforcement should understand the potential threats to a wastewater system. You also need to understand how a wastewater system operates, how each component functions, where they are located, and what they look like.

Understanding your local wastewater system operations, critical resources, and vulnerabilities, and knowing the utilities’ contacts will help law enforcement better respond to potential threats and incidents.

Sabotaging a publicly owned treatment works by introducing a hazardous substance is covered by a number of federal Clean Water Act (CWA) criminal provisions.

In general, a knowing violation of a regulatory requirement of the CWA by a person who knows at the time that another person was thereby placed in imminent danger of death or serious bodily injury is a federal environmental crime for which up to a 15-year prison term is authorized. (33 U.S.C. § 1319 (c) (3).

More specifically, the knowing introduction of any pollutant or hazardous substance into a sewer system or publicly owned treatment works which a person knew or reasonably should have known could cause personal injury or property damage is a federal
environmental crime for which up to a 3-year prison term is authorized. (33 U.S.C. § 1319 (c) (2) (b).

And, the knowing tampering with or rendering inaccurate any monitoring device or method used pursuant to the CWA is a federal environmental crime for which up to a 2-year prison term is authorized. (33 U.S.C. § 1319 (c) (4). (For more information: http://www.epa.gov/r5water/cwa.htm).

**What has happened nationally?**

Although the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) was directed specifically at public drinking water facilities, EPA strongly encourages wastewater facilities to look at their facilities in the same way. Below is a brief description of the requirements of the Act.
Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act)

Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) requires drinking water utilities serving more than 3,300 people to:

- Develop vulnerability assessments (VAs).
- Develop emergency response plans (ERPs).
- Enhance security inside and outside facilities.
- Coordinate with existing Local Emergency Planning Committees (LEPCs).

The Bioterrorism Act also:

- Expands EPA emergency powers to include “a threatened or potential terrorist attack....”
- Increases penalties for persons who tamper or threaten to tamper with public water systems.

EPA has developed a number of guidance materials relating to wastewater security. See the Resources section of this workbook and visit http://www.epa.gov/safewater/water security.
Module 2 — Wastewater Treatment Systems

Are You Familiar With The Wastewater Treatment Facilities In Your Jurisdiction?

Learning Objectives
After completing this module, participants will be able to:

- Identify the wastewater treatment facilities in their community.
- List and describe critical components of a wastewater system.
- Identify other wastewater systems’ assets in their jurisdiction.

What is a wastewater system?
Wastewater is any source of water that enters the sewer system. It includes substances such as human waste, food scraps, oils, soaps, and chemicals. Wastewater is derived from residential, commercial, and industrial activities. Commercial and industrial activities (such as acid cleaning from plating shops) also produce wastewater that must be treated prior to release to the environment. Industrial activities are more prone to discharge toxic pollutants. In addition to home and business production, wastewater can also be generated by storm runoff (referred to as inflow) and interception of ground water (infiltration). Because of potentially harmful substances that wash off roads, parking lots, and rooftops, this water also must be treated.

Wastewater treatment removes organic matter and other pollutants to improve the quality of wastewater so it can be discharged to a stream, river, lake, or coastal waters.
Wastewater is treated in a wastewater treatment facility prior to being discharged to a receiving water (i.e., river, lake, stream, or ocean). In 2002, the nation’s wastewater infrastructure consisted of approximately 16,000 publicly owned wastewater treatment plants; 100,000 major pumping stations; 600,000 miles of sanitary sewers; and 200,000 miles of storm sewers. The per capita volume of wastewater produced by a community ranges from about 50 to 250 gallons per day, depending on sewer uses.

What are the components of a wastewater system?
All wastewater treatment systems consist of two basic components: a collection system (which includes sanitary sewer, pump station, and collection basin) and a treatment facility.

How is wastewater collected?
Sewers are underground, watertight conduits that convey wastewater from its source of generation to a treatment facility. Flow through the system can be driven by gravity or it can be pumped. A main sewer line carries the liquid from large areas to the treatment plant. Manholes are located at regular intervals (about every 300 feet) to allow access to the pipes for inspection and cleaning. Every manhole is a point of entry into the collection system. The sewer/stormwater collection lines may be running along or directly under critical/sensitive buildings and structures. Lift stations are included in the collection system when gravity flow is not possible. A pumping station can be installed to lift the wastewater to an intercepting sewer at a higher level, or it can discharge to a force main that conveys the wastewater to the treatment plant. Unlike drinking water distribution systems, a wastewater collection system does not act under pressure. Therefore, access to the system through manholes and catch basins is not only a possibility, it is a serious concern. In the event of a hazardous material entering the system, the potential for a disaster (e.g., an explosion) and disruption to basic services is immense.

How does a wastewater treatment plant work?
Wastewater treatment combines chemical and biological processes that are designed to remove organic matter and other pollutants from solution. The processes are usually
arranged in a “treatment train” to improve the quality of the wastewater to a degree to which it can be discharged to the environment.

A wastewater treatment plant is typically composed of primary and secondary treatment processes, as described below.

**Primary treatment** removes 40–50 percent of the solids.

- **Sanitary sewers.** Carry wastewater from homes and businesses to the treatment plant.

- **Bar screens.** Let water pass, but not trash (such as rags or sticks). The trash is collected and properly disposed of, usually in a landfill.

- **Grit chamber.** A large tank that slows down the flow of water. This allows sand, grit, and other heavy solids to settle at the bottom. Later, they are removed and disposed of, usually in a landfill.

- **Primary sedimentation tank.** Lets smaller particles settle. Scrapers or other devices collect the solid matter that remains (called “primary sludge”) plus scum or grease floating on top of the tank.

**Secondary treatment** completes the process, so that 85–90 percent of the pollutants are removed.

- **Aeration tank.** Supplies large amounts of air to a mixture of wastewater, bacteria, and other microorganisms. Oxygen in the air speeds the growth of helpful microorganisms, which consume harmful organic matter in the wastewater.

- **Secondary sedimentation tank.** Allows the microorganisms and solid wastes to form clumps and settle. Some of this mixture, called “activated sludge,” can be mixed with air again and reused in the aeration tank.

- **Disinfectant.** Chlorine or another disinfectant is usually added to the wastewater before it leaves the treatment plant. The disinfectant kills disease-causing organisms in the water.
The treated water is usually discharged to a nearby waterway such as a stream, lake, river, or coastal water source. It can also be used on land for agriculture and other purposes and may undergo further tertiary treatment depending on the use.

Electricity is used to operate pumps in the collection system and process the wastewater within the treatment facility. This is important when considering how an impact to one sector, such as energy, can adversely impact the water sector, including wastewater collection and treatment.

In recent years, wastewater treatment systems have increased their reliance on supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs) for remote command and control of system components. Use of SCADA/DCS technologies allows tighter control of the treatment process, improved system efficiency, and decreased costs.

**What are administration and operations functions?**

The operation and maintenance of any wastewater system ultimately depends on management and its commitment to maintaining a structurally sound and safe system. The proper administration and operation of a wastewater system depend on two important assets: employees and computer systems.

**Employees**

The employees of a wastewater facility are generally its most valuable asset. They have knowledge of the system, and may also have experience in dealing with previous contamination threats or incidents. The importance of knowledgeable and experienced personnel is highlighted by the complexity of most wastewater treatment systems.

Do you know the people who operate your wastewater system? This is a key point that cannot be emphasized enough.
Law enforcement should get to know personnel at their wastewater treatment facility and become familiar with the operation:

- Meet your wastewater personnel face-to-face.
- Know the key contacts and their telephone numbers.
- Know their official vehicles and any identifying logos or insignias.
- Know what type of identification card they have, if any.

The day-to-day experience of wastewater system personnel is an invaluable tool to countering any attacks.

**Supervisory Control and Data Acquisition (SCADA)**

A SCADA system is typically defined as a computer-based monitoring and control system that centrally collects, displays, and stores information from remotely located data collection transducers and sensors in order to support the supervised remote control of equipment, devices, and automated functions.

Every component of the wastewater system pumping and treatment operation depends on energy and is highly automated. Although these operations are backed up by manual controls, damage could be done if power was disrupted or if the automated systems were temporarily lost due to cyber attack.

**What dependencies and interdependencies exist with other sectors?**

Wastewater utilities operate interdependently with other utilities.

Wastewater systems are connected to other infrastructures through dependencies and interdependencies. They may depend upon:

- **Electric power** for pumps, treatment, operations, repairs, security systems, computers, common rights-of-way.
Diesel or propane fuel for backup power generation, transportation and utility vehicles.

Natural gas for heating and cooling systems and for back-up power generation.

Telecommunications for voice and data communications and automated meter reading systems, general operations, remote monitoring, communications with emergency responders, common rights-of-way.

Transportation for delivery of chemicals and materials, for operations, maintenance, and repair, for transport of emergency responders and equipment, and for common rights-of-way.

Chemicals such as chlorine and other treatment chemicals.

Banking and finance, which are important for company operations.

Postal and shipping, which are important to company operations.

It is important to consider how an incident in one sector can adversely affect the wastewater utility.
Questions

1. Where are the wastewater treatment systems in your jurisdiction?

2. Have you visited your wastewater treatment facilities, met personnel, and done walk throughs?

3. Where does the treated wastewater go after it leaves the facilities?

4. Where are key manholes or access points in the collection systems?

5. Does the wastewater system have chlorine gas on site?

6. What are the chemicals at the treatment facility?

7. Are you aware of the chemical delivery procedures?

8. Where are the pump stations?

9. Does the wastewater utility have an emergency power source?

10. Do you have copies of the wastewater facility’s emergency response plans?
Module 3 — Threats

What Are the Potential Threats to Your Wastewater System?

Learning objectives
After completing this module, participants will be able to:

- Understand different threats to wastewater systems.
- Be familiar with potential types of contamination.

What are potential threats?

Contamination threats. Threats may come from chemicals stored or used on site for treatment, or they may come from flammable and explosive substances introduced into the collection system. Threats against chemicals stored and used on site for treatment are intended to create acute releases and expose large populations. Top targets at wastewater treatment plants are likely to be chlorine and sulfur dioxide.

Damage or destruction to the physical infrastructure. Physical threats can range from general vandalism to the use of explosives. Targeting specific facilities within a wastewater system, a perpetrator may wish to vandalize, break in, destroy, or disrupt that facility’s equipment and operations. There are many ways to disrupt the different functions of a wastewater treatment facility. They include threats to destroy or disable collection or treatment processes. Tactics may include destruction with hand tools, explosive devices, or weapons fired from a distance. A trained and determined adversary can be expected to lodge an attack against the asset most
likely to maximize damage or mission failure, often referred to as a “single point of failure.” Included in this category are main lift pumps, large-diameter conveyances, unique pieces of equipment, electrical switchgear, and process controls.

**Disruption to computer systems.** Wastewater systems increasingly depend on electronic controls for operation. Cyber threats are intended to disrupt or disable operations or result in data or identity theft. In addition, a cyber threat applied to a customer information management system could be a very damaging event requiring a great deal of time and effort to rectify.

**Disruption to other utilities (e.g., electricity, transportation).** The tie between the power and the water sectors is one of the key infrastructure interdependencies. The power failure of August 14, 2003, and its effects on drinking water and wastewater facilities varied from a momentary loss of power to days without power and water services. The lesson learned by these facilities was the need to review their vulnerability assessments and emergency response plans in order to address power outages in their plans. They also recognized the need to review and update their plans on how to notify or recall needed employees in emergencies.

**What are the consequences of an attack?**
The consequences of one of the above threats on a wastewater system are varied. We shall offer some general thoughts on the subject here, but to find out the specific consequences that would affect the wastewater system in your jurisdiction, you need to meet with your wastewater system personnel.

One factor that affects the severity of the consequences of an attack is the amount of redundancy built into a wastewater system. If the wastewater’s main lift pump is the only pump it has for the conveyance of wastewater to the treatment plant and that pump is lost, “a single point of failure,” then losing that pump is a much larger problem.
Law enforcement should work closely with their wastewater system to learn what the system’s “single points of failure” are and pay special attention to them, especially in times of heightened threat levels.

**How can wastewater systems be protected?**

Wastewater systems must identify their critical assets and consider questions such as:

- What is the easiest target?
- What will affect the system or its customers the most?
- What are the terrorists’ goals?
- What are the terrorists’ constraints?

Asking and answering the right questions will help wastewater system personnel determine the nature of an attack. Remember that many things must go as planned to result in casualties. History says this isn’t that easy; however, it is relatively easy to disrupt service or destroy public confidence.

Law enforcement may be able to assist a wastewater utility in determining what assets are vulnerable, and law enforcement may be able to assist the utility in becoming a less attractive target.

Law enforcement can provide some assistance in working with wastewater personnel in surveillance and in responding to alarms. Working with wastewater personnel to reduce incidents or false alarms will help maintain everyone’s vigilance in securing these important assets.

Law enforcement’s role in assisting wastewater utilities might focus on:

- Surveillance.
- Patrols.
- Communications/24hr. contacts.
- Physical security.
- Site control.
- Public Notification.
- Investigations.
- Threat warnings.
- Liaison with state and federal law enforcement and intelligence resources.
It is vitally important that law enforcement take very seriously any threat to a wastewater system and notify wastewater contacts. If notified, wastewater treatment personnel can then take action to minimize risk to the public.

**Questions**

1. What are the potential threats to wastewater?

2. Can you name a few contaminants that might be used in an attack against a wastewater utility?

3. Can you think of a few places in your jurisdiction that might make an attractive place to add contaminants to the wastewater system?

4. What can law enforcement do to assist a wastewater utility in becoming a less attractive target?
Module 4 — Vulnerabilities

Are You Aware of the Vulnerabilities and the Means of Protecting Key Components of a Wastewater System?

Learning objectives
After completing this module, participants will be able to:

- Understand vulnerable areas of wastewater systems.
- Understand some of the chemical concerns at wastewater systems.
- Understand ways of working with wastewater system personnel to protect their wastewater systems.

Wastewater treatment personnel are encouraged to look at their system, identify the threats to each component, and estimate the potential effects of those threats on their system and its operations. The following is a brief description of some of the vulnerabilities of wastewater systems. This is not intended to be a complete overview. Law enforcement should talk with wastewater personnel to understand their system’s specific vulnerabilities and how they plan on protecting them.

What are the potentially vulnerable components of a wastewater system?

Physical structures
Physical damage to or the destruction of key components of the wastewater treatment system is considered to be the most likely threat against a wastewater treatment
system. Because of the large size of most wastewater collection systems, security is an issue. Access to trunk lines is readily available through regularly spaced manholes that are mostly unprotected. Similarly, lift stations and pumps are readily accessible to the terrorist. Physical damage to a treatment plant could potentially disrupt operations for several days to months, depending on the type and amount of damage done. For example, a flammable substance could be placed into the collection system to use the collection system as a pipe bomb to damage or destroy targets in and around the system, recognizing that the sewer system may provide access to targets (such as government buildings, military installations, stadiums, or convention centers where publicized events are occurring).

**Incident - Louisville, Kentucky, 1981**

Shortly after 5:15 a.m. on Friday, February 13, 1981, two women going to work drove under a railroad overpass. There was a gigantic blast, and their car was hurled into the air and landed on its side. More than 2 miles of 12-foot diameter sewer line had been destroyed. No one was seriously hurt. Thousands of gallons of hexane had spilled into the sewer lines. A spark from the women’s car apparently ignited the hexane.

The two miles of sewer was turned into an open trench and remained that way until the end of the summer. It took 20 months to repair the sewer lines and several more months to complete work on the street.

**Incident - Guadalajaro, Mexico**

In 1992 there were at least 9 separate explosions in the sanitary sewage system. The cause of the explosions was gasoline leaking from the state run pipeline into a sanitary sewer collection line. The explosions killed at least 215 people and caused 15 blasts that created a 20-foot-deep trench along sewer mains in a 20-block area.

**Process chemicals**

Most wastewater systems are located close to major economic activity, including high-risk government facilities. Chlorine storage and its distribution system, located outside, can make them a visible and vulnerable target. Chemical deliveries can create access issues and potential for “contamination” of wastewater treatment and the surrounding neighborhood if not properly delivered.
**Incident – December 2003.**
An ammonia leak at an East Baton Rouge, Louisiana, wastewater treatment facility was determined to be caused by criminals who sought to steal the plant’s process ammonia, which is also a key ingredient in the manufacture of illegal drugs such as methamphetamine.

**Incident – June 2005.**
A corrosive gas that formed in the sewage treatment plant when a chemical was delivered through the wrong pipe forced the evacuation of homes and businesses more than a third of a mile away. No injuries were reported. The plant remained in operation, its effectiveness reduced. It was about 2 ½ hours after a crew from the bulk transport company erroneously pumped what is believed to be 100 gallons of ferric chloride from a stainless-steel 20-foot truck through the wrong fill pipe into a tank containing 4,200 gallons of sodium hypochlorite. Separately, the chemicals are benign but make a toxic acid when mixed. The resulting chemical reaction produced a rumbling at the bottom of the plant from the creation of the invisible hydrogen chloride gas. The gas began expanding in the plastic sodium hypochlorite tank. It forced its way through vents in the holding tank and the plant’s doors and windows into the air, and began drifting up the street. The plant could not be shut down since there was no way to stop the flow of sewage, estimated at close to 4 million gallons a day. The evacuation zone was set at one-third of a mile. Detectives began conducting interviews even as firefighters were blocked by high chlorine levels from entering the basement holding room where the chemicals continued to stew. The area would not be safe until the following morning.

**Information systems**
Increased reliance on Supervisory Control and Data Acquisition (SCADA) technologies makes the wastewater treatment process more susceptible to cyber attack. Although most industry officials believe that firewalls provide adequate protection, a relatively proficient hacker with some basic knowledge about the wastewater treatment system could exploit this vulnerability.

**Incident - In Queensland, Australia**
On April 23, 2000, police stopped a car on the road to Deception Bay and found a stolen computer and radio transmitter inside. Using commercially available technology, someone had turned his vehicle into a pirate command center for sewage treatment along Australia’s Sunshine Coast. The perpetrator’s arrest solved a mystery that had troubled the Maroochy
Shire Wastewater System for 2 months. Somehow the system was leaking hundreds of thousands of gallons of putrid sludge into parks, rivers, and the manicured grounds of a Hyatt Regency hotel. Janelle Bryant of the Australian Environmental Protection Agency said, “Marine life died, the creek turned black, and the stench was unbearable for residents.” Until the suspect’s capture, during his 46th successful intrusion, the utility’s managers did not know how the attacks were accomplished. To sabotage the system, the suspect set the software on his laptop to identify itself as “pumping station 4,” then suppressed all alarms. He was the “central control system” during his intrusions with unlimited command of 300 SCADA nodes governing sewage and drinking water alike. “He could have done anything he liked to the fresh water,” said Paul Chisholm, chief executive of Hunter Watertech.

**Infrastructure interdependencies**
In this case, the threat is the use of one infrastructure to damage other forms of infrastructure. While there are few examples of such a threat, the blackout in the Northeast and Midwest United States in August 2003 demonstrated the interdependencies among multiple infrastructures and that such a threat is possible.

**Incident**
A lack of emergency back-up power at several regional wastewater treatment plants during the Northeast blackout of 2003 caused the release of millions of gallons of raw sewage. Several sewage plants lost back-up power on August 14, 2003, including one unable to start its stand-by generators when New York’s Con Edison went dark. More than 423 million gallons of waste from 9 treatment plants or pumping stations in New York and New Jersey was dumped into the Hudson River, New York Harbor, and other area waterways before power was restored.

All of these threats may come about through:

- A natural disaster.
- Vandalism.
- Employee sabotage.
- Terrorist sabotage.
- Computer hacking.
- Illicit dumping of chemicals into the sewer.
Law enforcement’s role in assisting wastewater systems might focus on:

- Communications/contacts.
- Surveillance.
- Patrols.
- Site control.
- Investigations.
- Liaison with state and federal law enforcement and intelligence resources.

Questions

1. Have you done a walk through of the wastewater utilities in your jurisdiction with wastewater system personnel?

2. Are you familiar with the type of vulnerabilities particular to these systems?

3. Do you know the wastewater plant’s critical contacts? Do they know yours?

4. Are there abandoned facilities in your community that someone could use to tap into the wastewater system?

5. Are you aware of treatment plant personnel or “unofficial” personnel entering manholes?
Module 5 — Incident Management

How Do You Manage a Threat or Incident?

Learning objectives
After completing this module, participants will be able to:

- Understand the types of threat warnings.
- Understand procedures for evaluating threat credibility.
- Understand the Incident Command System.

One goal of terrorism can be simply to instill fear in a population, not necessarily to cause damage or casualties. This fear can be caused by the mere threat of contamination if the threat is not properly managed. For this reason, both threatened and actual contamination incidents are a concern faced by the public at large and, in particular, wastewater system professionals. In the past, wastewater systems have focused on protecting against vandalism, theft, and natural disasters. Now, they must consider terrorist threats.

What are types of threat warnings?
A threat is an indication that something may have been done to the wastewater system, and may or may not prove to be true.

An incident is a confirmed contamination event or disruption of a wastewater system and requires a response.

Contamination threats and incidents may be of particular concern due to the range of potential consequences:

- Adverse impacts on public health or the environment if untreated wastewater is discharged to a receiving water.

Managing an incident may require familiar tools.
The disruption of system operations and the interruption of wastewater treatment.

Physical damage to system infrastructure.

Long-term denial of wastewater services and the cost of remediation and replacement.

The threat-management process involves two parallel and interrelated activities:

- Evaluating the threat.
- Making decisions regarding appropriate actions to take in response to the threat.

Historical evidence suggests that the probability of intentional disruption of the wastewater treatment process is low; however, experts agree that it is possible to disrupt wastewater treatment or use the infrastructure as a conduit for other activities that could result in adverse public health and environmental consequences. The probability of a disruption threat does exist.

The first critical step in evaluating a threat is the recognition of a threat warning. The utility likely will be in the best position to observe a threat warning and evaluate whether or not the activity is possible (i.e., first decision point in the “Threat Evaluation” process).

Types of threat warnings include:

- Security breaches.
- Witness account.
- Direct notification by perpetrator.
- Public health or environmental notification.
- Notification by law enforcement.
- Notification by news media.
- Unusual water quality parameters.
- Consumer complaint.

The following is a brief description of several types of threat warnings. To learn more, see Module 1 of the EPA “Response Protocol Toolbox.”

Security breaches. A security breach is an unauthorized intrusion into a secured facility that may be discovered through direct observation, an alarm trigger, or signs
of intrusion. Security breaches are probably the most common threat warnings, but in most cases are related to day-to-day operation and maintenance in the wastewater system. Other security breaches may be due to criminal activity such as trespassing, vandalism, or theft.

➢ **Witness account.** A threat warning may come from an individual who directly witnesses suspicious activity, such as trespassing, breaking and entering, or some other form of tampering. The witness could be either a utility employee or a bystander. As a result, the witness report may come directly to the utility, or it may be directed to a 911 operator or law enforcement agency. If the witness reports the incident to a law enforcement agency, a written or verbal report from the police may provide some insight into the event. It is important for the utility to have a relationship with local law enforcement agents, since individuals observing suspicious behavior near wastewater facilities will likely call 911 or law enforcement rather than the wastewater utility.

➢ **Direct notification by perpetrator.** A threat may be made to the wastewater utility, either verbally or in writing. Verbal threats made over the phone are historically the most common type of direct threats from perpetrators: however, written threats have also been delivered to utilities. A direct notification should be evaluated with respect to both the nature of the threat and the specificity of information provided in the threat. In the case of a phone threat, the caller should be questioned about the specifics of the threat: time and location of the incident, name and amount of the contaminant, reason for the attack, the name and location of the caller, etc.

➢ **Notification by public health agency.** Notification from a public health agency or health care providers regarding increased incidence of disease; or notification from an environmental agency about fish kills or other environmental impacts.

➢ **Notification by law enforcement.** A utility may receive notification about a contamination threat direct from law enforcement, including local, county, state, or federal agencies. As discussed previously, such a threat could be a result of suspicious activity reported to law enforcement either by a perpetrator, a witness, or
the news media. Other information, gathered through intelligence or informants, could also lead law enforcement to conclude that there may be a threat to the wastewater system. While law enforcement will have the lead in the criminal investigation, the utility has primary responsibility for the safety of the wastewater facility and environmental and public health. Thus the utility’s role will likely be to help law enforcement to appreciate the public health and environmental implications of a particular threat as well as the technical feasibility of carrying out a particular threat.

Notice by news media. A threat to contaminate the wastewater treatment process might be delivered to the news media, or the media may discover a threat. A conscientious reporter would immediately report such a threat to the police, and either the reporter or the police would immediately contact the wastewater utility. This level of professionalism would provide an opportunity for the utility to work with the media and law enforcement to assess the credibility of the threat before any broader notification is made.

What is the threat-management process?
The goals of threat response and management for a wastewater utility are to evaluate the threat, take necessary steps to protect public health and the environment while the threat is being evaluated, confirm the threat, remediate the wastewater system, if necessary, and return the system to safe normal operation as soon as possible.

The threat-management process is considered in three successive stages: “possible,” “credible,” and “confirmed.” It is important to stress that the response to an incident will be based on incomplete information. Not everything about the incident can be known in the timeframe in which response decisions must be made.

Continued emergency response training allows wastewater suppliers, state officials, and law enforcement to gain an understanding of how to best make decisions without complete information.
Possible
A threat is deemed “possible” if the circumstances indicate the opportunity for contamination.

Example of a possible threat:

- A phone call to the utility telling the utility that the system has been harmed.

The evaluation to determine if a threat is “possible” should be conducted quickly, with a 1-hour goal to determine if additional actions are needed.

Credible
Once a threat is considered possible, additional information will be necessary to determine if the threat is “credible.” The threshold at the “credible” stage is higher than that at the possible stage, and in general there must be information to corroborate the threat in order for it to be considered “credible.” Often this information is circumstantial but, if enough indicators suggest something has taken place, then additional response decisions need to be made. Steps should be initiated to confirm the incident.

The actions to decide if a threat is “credible” should proceed quickly, with a goal of making this determination within 2 to 8 hours.

Preliminary site characterization information will help determine if a threat is credible. In addition, wastewater suppliers and state wastewater officials should be in contact with other supporting agencies, including law enforcement, to gather information to guide the assessment.

The expertise of law enforcement agencies (local, state, and federal) will be critical in evaluating the credibility of a threat. They may have knowledge of recent criminal activity in the area that might help establish credibility or support advanced stages of the investigation.

Confirmed
A contamination incident is “confirmed” once conclusive evidence is obtained. Confirmation implies that definitive evidence and information have been collected to establish the validity of the threat and classify it as an “incident.” Laboratory analyses or
other sources of evidence such as eye witness reports, physical evidence from a location in the wastewater system, or reports by the perpetrators themselves may be adequate to confirm an incident.

**What is the Incident Command System?**

While many entities are involved in a threat evaluation, the **Incident Command System (ICS)** is the accepted model for managing emergencies. It allows its users to adopt an organizational structure to fit any situation regardless of jurisdictional boundaries. The ICS is extremely flexible and can grow or shrink to meet the changing needs of an incident. The organization that assumes responsibility for incident command will vary with the nature and severity of the incident. During the course of managing a contamination threat, the individual designated as incident commander may change as different organizations assume responsibility for managing the situation.

The various organizations that may assume incident command responsibility during an intentional contamination situation include:

- **Wastewater Utility** will likely be responsible for incident command during the initial stages of a situation. The utility will retain this responsibility, by default unless or until another organization (with proper authority) assumes command.

- **Wastewater Primacy Agency** may assume incident command when the utility lacks the resources to manage the threat.

- **Public Health Agency** (state or local) may assume incident command if the situation is a public health crisis (without links to terrorism).

- **Local Law Enforcement** may assume incident command when criminal activity (excluding federal crimes such as terrorism) is suspected. Law enforcement will have the lead in the criminal investigation and will determine whether or not a crime has been committed. EPA CID may assume incident command when the federal crime of tampering with a public water supply is suspected. EPA CID will have the lead in the criminal investigation and will determine whether or not an environmental crime has been committed.
FBI will assume incident command when a crime is suspected to have a nexus to terrorism.

If an organization other than the utility assumes incident command, the utility will play a supporting role during the threat-management process. Regardless of which organization is in charge of managing the overall situation, the wastewater utility will maintain responsibility for the wastewater system.

The National Response Plan (NRP) establishes a comprehensive all-hazards approach to managing domestic incidents. The NRP includes the best practices and procedures from several incident management disciplines (e.g., homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector) and combines them into one. The NRP outlines how federal departments and agencies will work together and how the federal government will coordinate with state, local, and tribal governments and the private sector during incidents. For additional information on the National Response Plan (NRP) go to http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml.

For more information on the threat management process, please see Module 2 of the Response Protocol Toolbox, which can be obtained at EPA’s Water Security Web site (http://www.epa.gov/watersecurity).

Law enforcement will have the lead in the criminal investigation and will determine whether or not a crime has been committed.

Law enforcement and wastewater utilities need to work together to preserve crime scenes, while at the same time allowing wastewater personnel access to facilities as necessary.

Local law enforcement may assume responsibility for incident command in situations in which criminal activity is suspected.
Questions

1. What is the difference between a threat and an incident?

2. What are some of the threat warnings you might encounter from a wastewater facility?

3. Do you have a diagram of the building facilities and a map of the pump stations within the collection system of the wastewater system?

4. Would you be able to access the wastewater treatment plant to respond if there were an incident?

5. Do you have access codes or keys to any locks?

6. Do you know the wastewater treatment plant’s emergency response plan and have you practiced with plant personnel?
Module 6 — Response

What Do You Need To Know To Respond to a Wastewater Threat or Incident?

Learning objectives
After completing this module, participants will be able to:

- Recognize the framework for evaluating a wastewater threat.
- Describe some of the actions that might be implemented in response to a contamination threat.

What do you need to know about your wastewater systems?
Each wastewater system is unique with respect to age, operation, and complexity. Wastewater systems are particularly unique in that many are complex and often an undocumented mix of new and old components.

There are many ways to gain a better understanding of a particular wastewater system, one of which is through its vulnerability assessment, if one has been conducted.

Meet with your wastewater personnel and ask them to share what areas they identified as key locations that are vulnerable to threats. Law enforcement can assist a wastewater plant in improving its physical security.

What do you need to know about your wastewater system personnel?
The employees of your wastewater facility are generally its most valuable asset in preparing for and responding to
wastewater threats and incidents. They have knowledge of the system and may also have experience in dealing with previous threats.

**What do you need to know about your wastewater system’s emergency response plan?**

Wastewater systems should revise their emergency response plans to reflect the findings of any vulnerability assessment performed in order to address terrorist threats.

Law enforcement should have a copy of the utility’s emergency response plan and should practice with utility personnel. How can you practice with a wastewater facility? EPA has developed a Tabletop Exercise CD with several different scenarios involving a wastewater utility. This is a great training tool to bring together all the essential response personnel involved in a water incident, allowing them to practice their roles and to revise any parts of their plan as necessary (http://cfpub.epa.gov/safewater/watersecurity/tools.cfm#cd).

Law enforcement should coordinate with their local EPA CID office.

**What do you need to know about sewer use ordinances?**

A sewer use ordinance sets forth uniform requirements for users of the Publicly Owned Treatment Works. It is essential to have knowledge of local laws regarding manhole tampering, unlawful entry, etc.

**What response actions are considered at the “possible” stage?**

Once a threat has been deemed “possible,” relatively low-level response actions are appropriate. Two response actions that might be considered at this stage are:

- Site characterization.
- Immediate operational response.

Site characterization is one of the critical activities intended to gather critical information to support the “credible” stage. Site characterization is defined as the process of collecting information from an investigation site in order to support the evaluation of a wastewater threat. This process will normally take place within 2-8 hours of the initial event. Site characterization activities include the site evaluation, field safety screening, rapid field testing of the water, and sample collection. The investigation site is the focus of site
characterization activities, and if a suspected contamination site has been identified, it will likely be designated as the primary investigation site. The results of site characterization are of critical importance to the threat evaluation process. Law enforcement serves an integral role in the site characterization process. Certain elements of the site characterization process are to be considered law enforcement investigative functions. These include the supervision of the preservation of the crime scene and the evaluation of information and physical evidence that may be present at the investigation site. The law enforcement evaluation of any existing physical evidence, including forensic evidence, may aid in the determination of the threats credibility.

Immediate operational response actions are primarily intended to limit the potential for exposure of the public to the suspect contaminant while site characterization activities are implemented. For example, if the wastewater utility believes someone has tampered with its chemical feed system, shutting down the chemical feed system would be an operational response.

**What response actions are considered at the “credible” stage?**

The response actions considered at the “credible” stage may involve more effort and have a greater impact than those considered at the “possible” stage.

Three response actions that might be considered at this stage are:

- Sample analysis.
- Continuation of site characterization activities.
- Public health response.

Sample analysis and continuing of site characterization are part of the ongoing threat evaluation and are intended to gather information to “confirm” whether a contamination incident did or did not occur.

Public health response actions are intended to prevent or limit exposure of the public to the suspect contaminant; they are more protective and have a greater impact on the public than the operational response considered at the possible stage.

Local law enforcement may be asked to participate in public notification strategies. Know the clearly established communications responsibilities. In the past, local law
enforcement has been essential in assisting wastewater personnel in notifying the public of emergencies.

**What response actions are considered at the “confirmatory” stage?**

Once a contamination incident has been confirmed, it will be necessary to move into full-response mode. Organizations that may be actively engaged in the response include the wastewater primacy agency, the public health agency, emergency response agencies, and law enforcement. All of these participating organizations likely will be coordinated under existing incident command structures designed to manage emergencies at the state or local level. States and local entities likely have established their own response plans that would be in effect if the incident were managed at this level. In any case, the wastewater system

<table>
<thead>
<tr>
<th>Threat Evaluation Stage</th>
<th>Possible</th>
<th>Credible</th>
<th>Confirmatory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Location of security breach.</td>
<td>· Results of site characterization at location of security breach.</td>
<td>· Results of site characterization at other investigation sites.</td>
<td></td>
</tr>
<tr>
<td>· Time of security breach.</td>
<td>· Previous security incidents.</td>
<td>· Input from primacy agency and public health agency.</td>
<td></td>
</tr>
<tr>
<td>· Information from alarms.</td>
<td>· Additional details from the threat warning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Observations when security breach was discovered.</td>
<td>· Observations when security breach was discovered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Additional details from the threat warning.</td>
<td>· Additional details from the threat warning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Evaluation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Was there an opportunity for contamination?</td>
<td>· Do site characterization results reveal signs of contamination?</td>
<td>· Were unusual contaminants detected during analysis? Do they pose a risk to the public?</td>
<td></td>
</tr>
<tr>
<td>· Has normal operational activity been ruled out?</td>
<td>· Is this security breach similar to previous security incidents?</td>
<td>· Do site characterization results reveal signs of contamination?</td>
<td></td>
</tr>
<tr>
<td>· Have other “harmless” causes been ruled out?</td>
<td>· Does other information (e.g., water quality) corroborate threat?</td>
<td>· Is contamination indicated by a “preponderance of evidence”?</td>
<td></td>
</tr>
<tr>
<td><strong>Notifications</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Notifications within utility.</td>
<td>· State agency.</td>
<td>· Emergency response agencies.</td>
<td></td>
</tr>
<tr>
<td>· Local law enforcement agencies.</td>
<td>· State/local public health agency.</td>
<td>· National Response Center.</td>
<td></td>
</tr>
<tr>
<td>· EPA CID</td>
<td>· EPA CID, FBI.</td>
<td>· Other state and federal assistance providers.</td>
<td></td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>· Isolate affected area.</td>
<td>· Implement appropriate public health protection measures.</td>
<td>· Characterize affected area.</td>
<td></td>
</tr>
<tr>
<td>· Initiate site characterization.</td>
<td>· Analyze samples.</td>
<td>· Revise public health protection measures as necessary.</td>
<td></td>
</tr>
<tr>
<td>· Estimate spread of suspected contaminant.</td>
<td>· Perform site characterization at additional investigation sites.</td>
<td>· Plan remediation activities.</td>
<td></td>
</tr>
<tr>
<td>· Consult external information sources.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
will still have a role in the implementation of full response actions; however, it will generally act in a technical support role.

The following is an example of a threat warning with a contamination management threat matrix presented. This is a tabular summary that lists the following at each stage of the threat evaluation:

- Information considered during the threat evaluation.
- Factors considered during the threat evaluation.
- Potential notifications unique to a specific stage of a particular threat warning.
- Potential response actions.

**Security Breach**

*How should law enforcement and wastewater utilities work together to address threats or to respond to incidents?*

- Law enforcement should meet wastewater personnel face-to-face and should know officials’ vehicles and identification badge or card type.

- Wastewater systems and law enforcement should share critical contact lists.

- Law enforcement can share information with police dispatchers on critical wastewater facilities as well as the wastewater system critical contact list.

- Before an incident, law enforcement should work with the wastewater system on how to protect the crime scene.

- Law enforcement can work with the wastewater system and Neighborhood Watch groups to build awareness around suspicious activities near critical wastewater structures.

- Law enforcement should be aware of a wastewater system’s “Single Points of Failure” and pay special attention to them, especially in times of heightened threat levels.
How do utilities use the Homeland Security Advisory System?
EPA provides guidance to water-sector utilities at each threat alert level. Work with your wastewater facility to see what assistance law enforcement can offer at various threat levels. Also know what operational changes may take place at different threat levels. The following is a brief review of the Homeland Security Advisory System. For more detailed information see the EPA document *Guarding Against Terrorist and Security Threats: Suggested Measures for Wastewater Utilities* (August 2004).

**Homeland Security Advisory System**

**Green**

**Low Risk of Terrorist Attack**

Protective measures for the wastewater utility should focus on ongoing facility assessments and the development, testing, and implementation of emergency response plans. Wastewater utilities should post emergency evacuation plans in an accessible, secure location near the entrance for immediate access by law enforcement, fire response, and other first responders.

**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, and reviewing and exercising emergency plans.

The wastewater utility will reaffirm communication and coordination protocols (embedded in the utility’s emergency response plan) with local authorities such as police and fire departments, HAZMAT teams, hospital, and other first responders. The wastewater utility is also encouraged to develop intelligence contacts with state and local law enforcement, EPA CID field offices, FBI field offices, and Water Information Sharing and Analysis Center (Water ISAC).

**Yellow**

**Elevated Significant Risk of Terrorist Attack**

Protective measures should focus on increasing surveillance of critical facilities; coordinating and practicing emergency response plans with allied utilities and response teams and local agencies; and implementing emergency plans, as appropriate.
The wastewater utility may ask law enforcement to increase surveillance activities in remote or isolated reaches of the service are where illicit dumping might occur.

Law enforcement should also have the critical contact lists available for all wastewater utility personnel.

**Orange**

**High Risk of Terrorist Attack**

Protective measures by the wastewater utility should focus on limiting facility access to essential staff and contractors and coordinating security efforts with local law enforcement officials and the armed forces, as appropriate.

Law enforcement may be asked to increase surveillance, particularly of critical assets and otherwise unprotected areas.

**Red**

**Severe Risk of Terrorist Attack**

Protective measures should focus on the decision to close specific facilities and the redirection of staff resources to critical operations. As appropriate, wastewater utilities will request increased law enforcement or security agency surveillance, particularly of critical assets and otherwise unprotected areas.
Questions

1. Do you know what threats are of concern to the wastewater systems in your jurisdiction?

2. Do you know the key utility personnel contacts for the wastewater systems in your jurisdiction?

3. Do you have a copy of the wastewater utility emergency response plans for the utilities in your jurisdiction and have you conducted any exercises with the utilities to test the plan?

4. Are you familiar with the response actions your utilities might take to possible, credible, or confirmed incidents?

5. Have you worked with wastewater utility personnel to explain how they should protect a potential crime scene?

6. Do you work with the utilities in your jurisdiction to provide appropriate assistance for changing national and local threat levels?
Summary

The following are bullets of all the law enforcement actions suggested throughout Part II: Wastewater Security.

Law enforcement should get to know personnel at their wastewater treatment facility and become familiar with the operation:

- Meet your wastewater personnel face-to-face.
- Know the key contacts and their telephone numbers.
- Know their official vehicles and any identifying logos or insignias.
- Know what type of identification card they have, if any.

Law enforcement should be aware of a wastewater system’s “single points of failure” and pay special attention to them, especially in times of heightened threat levels.

Law enforcement may be able to assist a wastewater utility in determining what assets are vulnerable, and law enforcement may be able to assist the utility in becoming a less attractive target.

Law enforcement can provide some assistance in working with wastewater personnel in surveillance and in responding to alarms. Working with wastewater personnel to reduce incidents or false alarms will help maintain everyone’s vigilance in securing these important assets.

Law enforcement’s role in assisting wastewater utilities might focus on:

- Surveillance.
- Patrols.
- Communications/24hr. contacts.
- Physical security.
- Site control.
- Public Notification.
- Investigations.
Threat warnings.
Liaison with state and federal law enforcement and intelligence resources.

Law enforcement’s role in assisting wastewater systems might focus on:

- Communications/contacts.
- Surveillance.
- Patrols.
- Site control.
- Investigations.
- Liaison with state and federal law enforcement and intelligence resources.

Law enforcement will have the lead in the criminal investigation and will determine whether or not a crime has been committed.

Law enforcement and wastewater utilities need to work together to preserve crime scenes, while at the same time allowing wastewater personnel access to facilities as necessary.

Local law enforcement may assume responsibility for incident command in situations in which criminal activity is suspected.

Meet with your wastewater personnel and ask them to share what areas they identified as key locations that are vulnerable to threats. Law enforcement can assist a wastewater plant in improving its physical security.

Law enforcement should have a copy of the utility’s emergency response plan and should practice with utility personnel. How can you practice with a wastewater facility? EPA has developed a Tabletop Exercise CD with several different scenarios involving a wastewater utility. This is a great training tool to bring together all the essential response personnel involved in a water incident, allowing them to practice their roles and to revise any parts of their plan as necessary (http://cfpub.epa.gov/safewater/watersecurity/tools.cfm#cd).
Local law enforcement may be asked to participate in public notification strategies. Know the clearly established communications responsibilities. In the past, local law enforcement has been essential in assisting wastewater personnel in notifying the public of emergencies.

Law enforcement should meet wastewater personnel face-to-face and should know officials' vehicles and identification badge or card type.

Wastewater systems and law enforcement should share critical contact lists.

Law enforcement can share information with police dispatchers on critical wastewater facilities as well as the wastewater system critical contact list.

Before an incident, law enforcement should work with the wastewater system on how to protect the crime scene.

Law enforcement can work with the wastewater system and Neighborhood Watch groups to build awareness around suspicious activities near critical wastewater structures.

Law enforcement should be aware of a wastewater system’s “Single Points of Failure” and pay special attention to them, especially in times of heightened threat levels.

The wastewater utility may ask law enforcement to increase surveillance activities in remote or isolated reaches of the service area where illicit dumping might occur.

Law enforcement should also have the critical contact lists available for all wastewater utility personnel.

Law enforcement may be asked to increase surveillance, particularly of critical assets and otherwise unprotected areas.
Resources

U.S. Environmental Protection Agency (EPA) Security Initiatives
http://cfpub.epa.gov/safewater/watersecurity/index.cfm

Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents (RPTB), Interim Final; December 2003. The RPTB is composed of six interrelated modules that focus on different aspects of planning a response to contamination threats and incidents long before they occur. The RPTB is a planning tool, and it should be integrated into a user’s specific emergency response planning activities in order to effectively manage an actual threat.
http://cfpub.epa.gov/safewater/watersecurity/home.cfm?program_id=8#response_toolbox

Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents, Interim Final; August 2004; Response Guidelines.


Water Sector-Specific Plan.

Water Watchers — Helping to Protect Your Local Water System - a brochure for citizens.

CDC Emergency Preparedness and Response: http://www.bt.cdc.gov/
U.S. EPA's List of Drinking Water Contaminants & Maximum Contaminant Levels (MCLs):
http://www.epa.gov/safewater/mcl.html#mcl

U.S. Coast Guard. 2001 “Chemical Hazards Response Information System” http://www.chrismanual.com

U.S. Army. 2002 “Toxic Chemical Agent Safety Standards”

Water Security Product Guide
http://cfpub.epa.gov/safewater/watersecurity/tools.cfm

Center for Nonproliferation Studies, Monterey Institute of International Studies
http://www.cns.miis.edu

American Water Works Association: http://www.awwa.org

Water Environment Research Foundation: http://www.werf.org


National Response Center (NRC) and National Response Team (NRT): http://www.nrt.org

National Incident Management Training
http://www.fema.gov/emergency/nims/index.shtm

National Infrastructure Protection Plan: http://www.dhs.gov/nipp

EPA's Safe Drinking Water Hotline
(800) 426-4791
Threat Evaluation Worksheet

INSTRUCTIONS
The purpose of this worksheet is to help organize information about a contamination threat warning that would be used during the Threat Evaluation Process. The individual responsible for conducting the Threat Evaluation (e.g., the Water Utility Emergency Response Manager [WUERM]) should complete this worksheet. The worksheet is generic to accommodate information from different types of threat warnings; thus, there will likely be information that is unavailable or not immediately available. Other forms in the Appendices are provided to augment the information in this worksheet.

<table>
<thead>
<tr>
<th>THREAT WARNING INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time threat warning discovered: ...........................................</td>
</tr>
<tr>
<td>Utility Name and Address: .................................................................</td>
</tr>
<tr>
<td>Name/Number of person who discovered threat warning: ....................................</td>
</tr>
<tr>
<td>Type of threat warning:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Identity of the contaminant:</td>
</tr>
<tr>
<td>If known or suspected, provide additional detail below</td>
</tr>
<tr>
<td>Chemical</td>
</tr>
<tr>
<td>Describe: ..........................................................................................................................</td>
</tr>
<tr>
<td>Time of contamination:</td>
</tr>
<tr>
<td>If known or estimated, provide additional detail below</td>
</tr>
<tr>
<td>Date and time of contamination: .................................................................</td>
</tr>
<tr>
<td>Additional Information: ........................................................................................................</td>
</tr>
<tr>
<td>Mode of contamination:</td>
</tr>
<tr>
<td>If known or suspected, provide additional detail below</td>
</tr>
<tr>
<td>Method of addition:</td>
</tr>
</tbody>
</table>
| Other: _________________________
Amount of material: __________________________________________________________

Additional Information: ______________________________________________________

**Site of contamination:**  
☐ Known  ☐ Suspected  ☐ Unknown

*If known or suspected, provide additional detail below*

Number of sites: ___________________________________________________________________

*Provide the following information for each site.*

**Site #1**

Site Name: _____________________________________________________________________

Type of facility
- ☐ Source water
- ☐ Ground storage tank
- ☐ Distribution main
- ☐ Other

Other: _________________________________________________________________________

Address: _____________________________________________________________________

Additional Site Information: ______________________________________________________

**Site #2**

Site Name: _____________________________________________________________________

Type of facility
- ☐ Source water
- ☐ Ground storage tank
- ☐ Distribution main
- ☐ Other

Other: _________________________________________________________________________

Address: _____________________________________________________________________

Additional Site Information: ______________________________________________________

**Site #3**

Site Name: _____________________________________________________________________

Type of facility
- ☐ Source water
- ☐ Ground storage tank
- ☐ Distribution main
- ☐ Other

Other: _________________________________________________________________________

Address: _____________________________________________________________________

Additional Site Information: ______________________________________________________
ADDITIONAL INFORMATION

Has there been a breach of security at the suspected site?  □ Yes □ No
   If “Yes”, review the completed ‘Security Incident Report’ (Appendix A, page 7)

Are there any witness accounts of the suspected incident?  □ Yes □ No
   If “Yes”, review the completed ‘Witness Account Report’ (Appendix A, page 11)

Was the threat made verbally over the phone?  □ Yes □ No
   If “Yes”, review the completed ‘Phone Threat Report’ (Appendix A, page 15)

Was a written threat received?  □ Yes □ No

Are there unusual water quality data or consumer complaints?  □ Yes □ No

Are there unusual symptoms or disease in the population?  □ Yes □ No

Is a ‘Site Characterization Report’ available?  □ Yes □ No

Are results of sample analysis available?  □ Yes □ No

Is a ‘Contaminant Identification Report’ available?  □ Yes □ No

Is there relevant information available from external sources?  □ Yes □ No
   Check all that apply
   □ Local law enforcement  □ FBI  □ DW primacy agency
   □ Public health agency  □ Hospitals / 911 call centers  □ US EPA / Water ISAC
   □ Media reports  □ Homeland security alerts  □ Neighboring utilities
   □ Other

Point of Contact: ____________________________________________________________

Summary of key information from external sources (provide detail in attachments as necessary):
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
THREAT EVALUATION

Has normal activity been investigated as the cause of the threat warning? □ Yes □ No

Normal activities to consider
- Utility staff inspections
- Construction or maintenance
- Operational changes
- Other

Yes
No

Has normal activity been investigated as the cause of the threat warning?

Is the threat ‘possible’? □ Yes □ No

Summarize the basis for this determination: ________________________________

Response to a ‘possible’ threat:
- None
- Increased monitoring/security
- Site characterization
- Isolation/containment
- Other

Is the threat ‘credible’? □ Yes □ No

Summarize the basis for this determination: ________________________________

Response to a ‘credible’ threat:
- Sample analysis
- Partial EOC activation
- Site characterization
- Isolation/containment
- Public notification
- Provide alternate water supply
- Other

Is a contamination incident been confirmed? □ Yes □ No

Summarize the basis for this determination: ________________________________

Response to a confirmed incident:
- Sample analysis
- Full EOC activation
- Site characterization
- Isolation/containment
- Public notification
- Provide alternate water supply
- Initiate remediation and recovery
- Other

How do other organizations characterize the threat?

<table>
<thead>
<tr>
<th>Organization</th>
<th>Evaluation</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Law Enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Possible</td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Credible</td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Confirmed</td>
<td></td>
</tr>
<tr>
<td>FBI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Possible</td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Credible</td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Confirmed</td>
<td></td>
</tr>
<tr>
<td>Public Health Agency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Possible</td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Credible</td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Confirmed</td>
<td></td>
</tr>
<tr>
<td>Drinking Water Primacy Agency</td>
<td>Possible</td>
<td>Credible</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Other</td>
<td>Possible</td>
<td>Credible</td>
</tr>
<tr>
<td>Other</td>
<td>Possible</td>
<td>Credible</td>
</tr>
</tbody>
</table>

**SIGNOFF**

Name of person completing this form:

Print name: ___________________________  Phone Number: ___________________________

Signature: ____________________________  Date/Time: ________________
Security Incident Report Form

INSTRUCTIONS
The purpose of this form is to help organize information about a security incident, typically a security breach, which may be related to a water contamination threat. The individual who discovered the security incident, such as a security supervisor, the Water Utility Emergency Response Manager (WUERM), or another designated individual may complete this form. This form is intended to summarize information about a security breach that may be relevant to the threat evaluation process. This form should be completed for each location where a security incident was discovered.

DISCOVERY OF SECURITY INCIDENT
Date/Time security incident discovered: ________________________________

Name of person who discovered security incident: ____________________________

Mode of discovery:
☐ Alarm (building) ☐ Alarm (gate/fence) ☐ Alarm (access hatch)
☐ Video surveillance ☐ Utility staff discovery ☐ Citizen discovery
☐ Suspect confession ☐ Law enforcement discovery
☐ Other

Did anyone observe the security incident as it occurred?  ☐ Yes ☐ No
If “Yes”, complete the ‘Witness Account Report’ (Appendix A, page 11)

SITE DESCRIPTION
Site Name: ________________________________

Type of facility
☐ Source water ☐ Treatment plant ☐ Pump station
☐ Ground storage tank ☐ Elevated storage tank ☐ Finished water reservoir
☐ Distribution main ☐ Hydrant ☐ Service connection
☐ Other

Address: ________________________________________________________________

Additional Site Information: _______________________________________________

BACKGROUND INFORMATION
Have the following “normal activities” been investigated as potential causes of the security incident?
☐ Alarms with known and harmless causes ☐ Utility staff inspections
☐ Routine water quality sampling ☐ Construction or maintenance
☐ Contractor activity ☐ Other ________________________________

Was this site recently visited prior to the security incident?  ☐ Yes ☐ No
If “Yes,” provide additional detail below

Date and time of previous visit: ____________________________________________

Name of individual who visited the site: ____________________________________
Additional Information: ____________________________________________________________

Has this location been the site of previous security incidents?  □ Yes  □ No

If “Yes,” provide additional detail below

Date and time of most recent security incident: ________________________________

Description of incident: _________________________________________________________

What were the results of the threat evaluation for this incident?

□ ’Possible’ □ ’Credible’ □ ’Confirmed’

Have security incidents occurred at other locations recently?  □ Yes  □ No

If “Yes,” complete additional ‘Security Incident Reports’ for each site

Name of 1st additional site: _______________________________________________________

Name of 2nd additional site: _____________________________________________________

Name of 3rd additional site: _____________________________________________________

SECURITY INCIDENT DETAILS

Was there an alarm(s) associated with the security incident?  □ Yes  □ No

If “Yes,” provide additional detail below

Are there sequential alarms (e.g., alarm on a gate and a hatch)?  □ Yes  □ No

Date and time of alarm(s): _______________________________________________________

Describe alarm(s): _____________________________________________________________

Is video surveillance available from the site of the security incident?  □ Yes  □ No

If “Yes,” provide additional detail below

Date and time of video surveillance: _____________________________________________

Describe surveillance: __________________________________________________________

Unusual equipment found at the site and time of discovery of the security incident:

□ Discarded PPE (e.g., gloves, masks) □ Empty containers (e.g., bottles, drums)

□ Tools (e.g., wrenches, bolt cutters) □ Hardware (e.g., valves, pipe)

□ Lab equipment (e.g., beakers, tubing) □ Pumps or hoses

□ None □ Other ________________________________

Describe equipment: ____________________________________________________________

___________________________________________________________

___________________________________________________________

___________________________________________________________
Unusual vehicles found at the site and time of discovery of the security incident:
- Car/sedan
- SUV
- Pickup truck
- Flatbed truck
- Construction vehicle
- None
- Other

Describe vehicles (including make/model/year/color, license plate #, and logos or markings): ___

Signs of tampering at the site and time of discovery of the security incident:
- Cut locks/fences
- Open/damaged access hatches
- Open/damaged gates, doors, or windows
- Facility in disarray
- Missing/damaged equipment
- None
- Other

Are there signs of sequential intrusion (e.g., locks removed from a gate and hatch)?
- Yes
- No

Describe signs of tampering:

Signs of hazard at the site and time of discovery of the security incident:
- Unexplained or unusual odors
- Unexplained dead or stressed vegetation
- Unexplained clouds or vapors
- Unexplained dead animals
- Unexplained liquids
- None
- Other

Describe signs of hazard:

SIGNOFF
Name of person responsible for documenting the security incident:

Print name ____________________________
Signature ____________________________ Date/Time: ______________
Witness Account Report Form

INSTRUCTIONS
The purpose of this form is to document the observations of a witness to activities that might be considered an incident warning. The individual interviewing the witness, or potentially the witness, should complete this form. This may be the Water Utility Emergency Response Manager (WUERM) or an individual designated by incident command to perform the interview. If law enforcement is conducting the interview (which may often be the case), then this form may serve as a prompt for “utility relevant information” that should be pursued during the interview. This form is intended to consolidate the details of the witness account that may be relevant to the threat evaluation process. This form should be completed for each witness that is interviewed.

BASIC INFORMATION
Date/Time of interview: ______________________________________________________

Name of person interviewing the witness: __________________________________________

Witness contact information
Full Name: __________________________________________________________________
Address: ____________________________________________________________________
Day-time phone: __________________________________________________________________
Evening phone: __________________________________________________________________
E-mail address: __________________________________________________________________

Reason the witness was in the vicinity of the suspicious activity:
___________________________________________________________________________

WITNESS ACCOUNT
Date/Time of activity: ______________________________________________________

Location of activity:
Site Name: __________________________________________________________________

Type of facility
☐ Source water  ☐ Treatment plant  ☐ Pump station
☐ Ground storage tank  ☐ Elevated storage tank  ☐ Finished water reservoir
☐ Distribution main  ☐ Hydrant  ☐ Service connection
☐ Other  ___________________________________________________________________

Address: ____________________________________________________________________

Additional Site Information: __________________________________________________________________

Type of activity
☐ Trespassing  ☐ Vandalism  ☐ Breaking and entering
☐ Theft  ☐ Tampering  ☐ Surveillance
☐ Other  ___________________________________________________________________
Additional description of the activity __________________________________________________________

_____________________________________________________________________________________

Description of suspects
Were suspects present at the site? ☐ Yes ☐ No

How many suspects were present? ______________________________________________________

Describe each suspect’s appearance:

<table>
<thead>
<tr>
<th>Suspect #</th>
<th>Sex</th>
<th>Race</th>
<th>Hair color</th>
<th>Clothing</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Where any of the suspects wearing uniforms? ☐ Yes ☐ No
If “Yes,” describe the uniform(s): ________________________________________________________

Describe any other unusual characteristics of the suspects: __________________________________

_____________________________________________________________________________________

Did any of the suspects notice the witness? ☐ Yes ☐ No
If “Yes,” how did they respond: _________________________________________________________

Vehicles at the site
Were vehicles present at the site? ☐ Yes ☐ No

Did the vehicles appear to belong to the suspects? ☐ Yes ☐ No

How many vehicles were present? ______________________________________________________

Describe each vehicle:

<table>
<thead>
<tr>
<th>Vehicle #</th>
<th>Type</th>
<th>Color</th>
<th>Make</th>
<th>Model</th>
<th>License plate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Where there any logos or distinguishing markings on the vehicles? ☐ Yes ☐ No
If “Yes,” describe: __________________________________________________________________
Provide any additional detail about the vehicles and how they were used (if at all): ____________________________

_________________________________________________________

_________________________________________________________

_________________________________________________________

Equipment at the site
Was any unusual equipment present at the site? □ Yes □ No

☐ Explosive or incendiary devices
☐ PPE (e.g., gloves, masks)
☐ Tools (e.g., wrenches, bolt cutters)
☐ Lab equipment (e.g., beakers, tubing)
☐ Other

☐ Firearms
☐ Containers (e.g., bottles, drums)
☐ Hardware (e.g., valves, pipe, hoses)
☐ Pumps and related equipment

Describe the equipment and how it was being used by the suspects (if at all): ____________________________

_________________________________________________________

_________________________________________________________

_________________________________________________________

Unusual conditions at the site
Were there any unusual conditions at the site? □ Yes □ No

☐ Explosions or fires
☐ Dead/stressed vegetation
☐ Other

☐ Fogs or vapors
☐ Dead animals

☐ Unusual odors
☐ Unusual noises

Describe the site conditions: ____________________________

_________________________________________________________

_________________________________________________________

_________________________________________________________

Additional observations
Describe any additional details from the witness account: ____________________________

_________________________________________________________

_________________________________________________________

_________________________________________________________

SIGNOFF
Name of interviewer:
Print name ____________________________________________
Signature ____________________________________________ Date/Time: ____________

Name of witness:
Print name ____________________________________________
Signature ____________________________________________ Date/Time: ____________
**Phone Threat Report Form**

**INSTRUCTIONS**
This form is intended to be used by utility staff that regularly answer phone calls from the public (e.g., call center operators). The purpose of this form is to help these staff capture as much information from a threatening phone call while the caller is on the line. It is important that the operator keep the caller on the line as long as possible in order to collect additional information. Since this form will be used during the call, it is important that operators become familiar with the content of the form. The sections of the form are organized with the information that should be collected during the call at the front of the form (i.e., Basic Call Information and Details of Threat) and information that can be completed immediately following the call at the end of the form (i.e., the description of the caller). The information collected on this form will be critical to the threat evaluation process.

*Remember, tampering with a drinking water system is a crime under the SDWA Amendments!*

**THREAT NOTIFICATION**

Name of person receiving the call: ________________________________

Date phone call received: ____________  Time phone call received: ____________

Time phone call ended: ____________  Duration of phone call: ____________

Originating number: ________________________________  Originating name:

*If the number/name is not displayed on the caller ID, press *57 (or call trace) at the end of the call and inform law enforcement that the phone company may have trace information.*

Is the connection clear?  

☐ Yes  ☐ No

Could call be from a wireless phone?  ☐ Yes  ☐ No

**DETAILS OF THREAT**

Has the water already been contaminated?  

☐ Yes  ☐ No

Date and time of contaminant introduction known?  

☐ Yes  ☐ No

Date and time if known: ________________________________

Location of contaminant introduction known?  

☐ Yes  ☐ No

Site Name: ________________________________

Type of facility

☐ Source water  ☐ Treatment plant  ☐ Pump station

☐ Ground storage tank  ☐ Elevated storage tank  ☐ Finished water reservoir

☐ Distribution main  ☐ Hydrant  ☐ Service connection

☐ Other  ________________________________

Address: ____________________________________________

____________________________________________________

Additional Site Information: ____________________________________________
Name or type of contaminant known? □ Yes □ No

Type of contaminant
□ Chemical □ Biological □ Radiological

Specific contaminant name/description: ____________________________

Mode of contaminant introduction known? □ Yes □ No

Method of addition: □ Single dose □ Over time □ Other ____________

Amount of material: ____________________________

Additional Information: ____________________________

Motive for contamination known? □ Yes □ No

□ Retaliation/revenge □ Political cause □ Religious doctrine
□ Other ____________

Describe motivation: ____________________________

CALLER INFORMATION

Basic Information:
Stated name: ____________________________
Affiliation: ____________________________
Phone number: ____________________________
Location/address: ____________________________

Caller's Voice:
Did the voice sound disguised or altered? □ Yes □ No
Did the call sound like a recording? □ Yes □ No
Did the voice sound? □ Male / □ Female □ Young / □ Old
Did the voice sound familiar? □ Yes □ No
If 'Yes,' who did it sound like? ____________________________
Did the caller have an accent? □ Yes □ No
If 'Yes,' what nationality? ____________________________

How did the caller sound or speak?
□ Educated □ Well spoken □ Illiterate
□ Irrational □ Obscene □ Incoherent
□ Reading a script □ Other ____________________________
What was the caller’s tone of voice?

- Calm
- Excited
- Slow
- Soft
- Laughing
- Deep
- Other

- Angry
- Nervous
- Rapid
- Loud
- Crying
- High

- Lisping
- Sincere
- Normal
- Nasal
- Clear
- Raspy

- Stuttering/broken
- Insincere
- Slurred
- Clearing throat
- Deep breathing
- Cracking

Were there background noises coming from the caller’s end?

- Silence
- Voices
- Children
- Animals
- Factory sounds
- Office sounds
- Music
- Traffic/street sounds
- Airplanes
- Trains
- Ships or large boats
- Other

- describe
- describe
- describe
- describe
- describe
- describe
- describe
- describe
- describe
- describe

SIGNOFF

Name of call recipient:

Print name
Signature
Date/Time:

Name of person completing form (if different from call recipient):

Print name
Signature
Date/Time: