United States
Environmental Protection
Agency

Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents

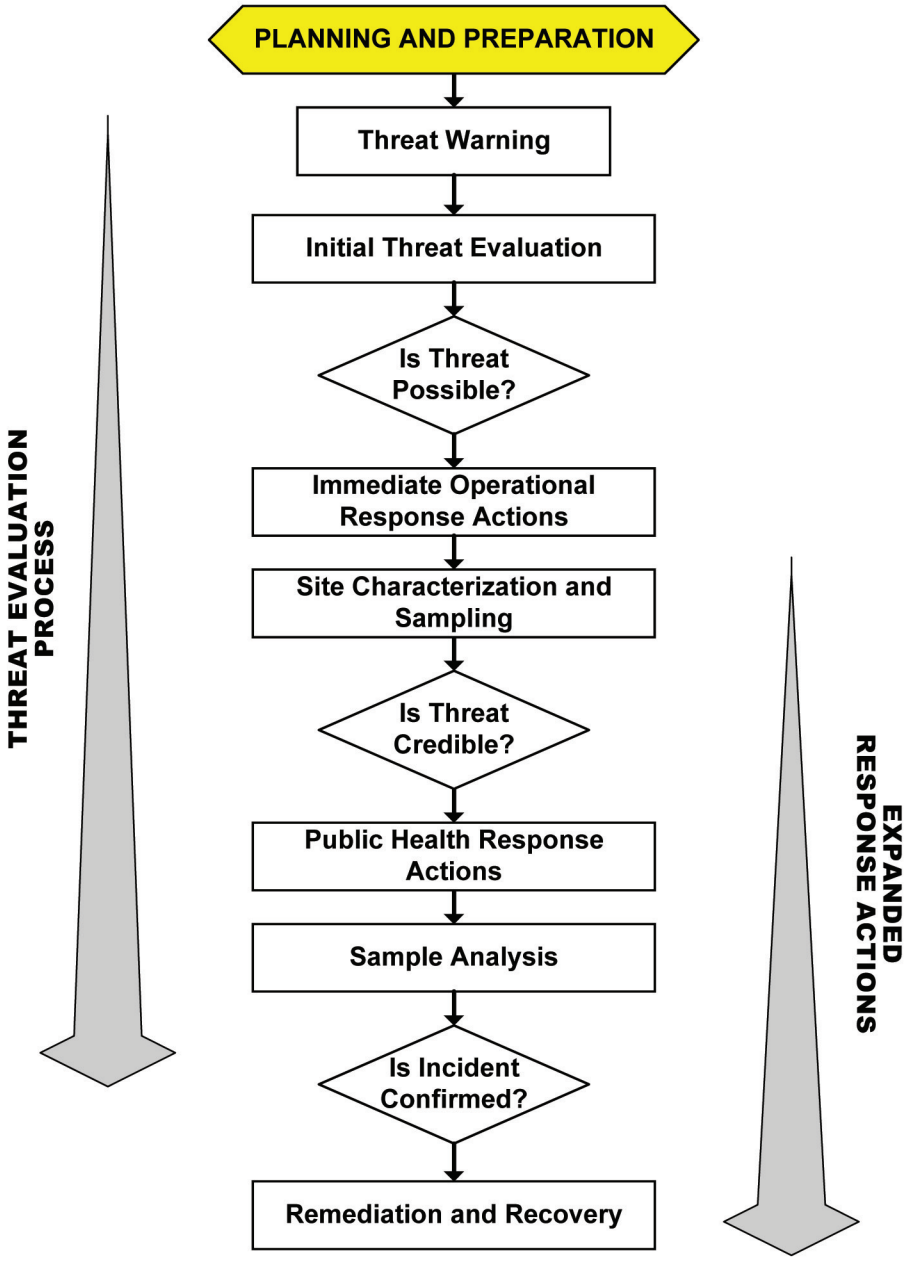
Interim Final - December 2003

Module 1: Water Utilities Planning Guide

Response Protocol Toolbox:
Planning for and Responding to Drinking Water Contamination Threats and Incidents

Module 1: Water Utilities Planning Guide

Interm Final - December 2003



OTHER RESPONSE PROTOCOL TOOLBOX MODULES

Module 1: Water Utility Planning Guide *(December 2003)*
Module 1 provides a brief discussion of the nature of the contamination threat to the public water supply. The module also describes the planning activities that a utility may undertake to prepare for response to contamination threats and incidents.

Module 2: Contamination Threat Management Guide *(December 2003)*
Module 2 presents the overarching framework for management of contamination threats to the drinking water supply. The threat management process involves two parallel and interrelated activities: 1) evaluating the threat, and 2) making decisions regarding appropriate actions to take in response to the threat.

Module 3: Site Characterization and Sampling Guide *(December 2003)*
Module 3 describes the site characterization process in which information is gathered from the site of a suspected contamination incident at a drinking water system. Site characterization activities include the site investigation, field safety screening, rapid field testing of the water, and sample collection.

Module 4: Analytical Guide *(December 2003)*
Module 4 presents an approach to the analysis of samples collected from the site of a suspected contamination incident. The purpose of the Analytical Guide is **not** to provide a detailed protocol. Rather, it describes a framework for developing an approach for the analysis of water samples that may contain an unknown contaminant. The framework is flexible and will allow the approach to be crafted based on the requirements of the specific situation. The framework is also designed to promote the effective and defensible performance of laboratory analysis.

Module 5: Public Health Response Guide *(available March 2004)*
Module 5 deals with the public health response measures that would potentially be used to minimize public exposure to potentially contaminated water. It discusses the important issue of who is responsible for making the decision to initiate public health response actions, and considers the role of the water utility in this decision process. Specifically, it examines the role of the utility during a public health response action, as well as the interactions among the utility, the drinking water primacy agency, the public health community, and other parties with a public health mission.

Module 6: Remediation and Recovery Guide *(available March 2004)*
Module 6 describes the planning and implementation of remediation and recovery activities that would be necessary following a confirmed contamination incident. The remediation process involves a sequence of activities, including: system characterization; selection of remedy options; provision of an alternate drinking water supply during remediation activities; and monitoring to demonstrate that the system has been remediated. Module 6 describes the types of organizations that would likely be involved in this stage of a response, and the utility's role during remediation and recovery.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

AWWARF	American Water Works Association Research Foundation
C/B	Chemical/Biological
CD	Compact disk
CDC	Centers for Disease Control and Prevention
DBP	Disinfection by-product
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
EPA	U.S. Environmental Protection Agency
ERP	Emergency response plans
ESF	Emergency support function
EWS	Early warning system
FBI	Federal Bureau of Investigation
FCO	Federal coordinating officer
FEMA	Federal Emergency Management Agency
FRP	Federal Response Plan
GIS	Geographic information system
GSA	Government services agency
HazMat	Hazardous materials
HHS	Department of Health and Human Services
IC	Incident commander
ICS	Incident Command System
ILSI	International Life Sciences Institute Risk Science Institute
IO	Information officer
JIC	Joint information center
JOC	Joint operations center
LFA	Lead federal agency
LO	Liaison officer
LPoC	Laboratory point of contact
LRN	Laboratory Response Network
NCP	National Oil and Hazardous Substances Pollution Contingency Plan
NIIMS	National Interagency Incident Management System
NIMS	National Incident Management System
NRC	Nuclear Regulatory Commission
NRP	National Response Plan
OSC	On-scene coordinator
PDD	Presidential decision directive
RG	Response guideline

RPTB	Response Protocol Toolbox
RST	Regional support team
SCADA	Supervisory control and data acquisition
SDWA	Safe Drinking Water Act
TOC	Total organic carbon
URL	Uniform resource locator
USACE	United States Army Corps of Engineers
USCG	United States Coast Guard
USDA	United States Department of Agriculture
UV	Ultraviolet
WCIT	Water contaminant information tool
WHO	World Health Organization
WUERM	Water utility emergency response manager
WUOCM	Water utility emergency operations center manager

GLOSSARY

Definitions in this glossary are specific to the Response Protocol Tool Box but conform to common usage as much as possible.

Agency – a division of government with a specific function, or a non-governmental organization (e.g., private contractor, business, etc.) that offers a particular kind of assistance. In the incident command system, agencies are defined as jurisdictional (having statutory responsibility for incident mitigation) or assisting and/or cooperating (providing resources and/or assistance).

Agency Representative – an individual assigned to an incident from an assisting or cooperating agency who has been delegated authority to make decisions on matters affecting that agency's participation at the incident.

Assisting Agency – an agency directly contributing tactical or service resources to another agency.

Bioterrorism Act – the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

Chain of Command – a series of management positions in order of authority.

'Confirmatory' Stage – the third stage of the threat evaluation process from the point at which the threat is deemed 'credible' through the determination that a *contamination incident* either has or has not occurred.

'Confirmed' – in the context of the *threat evaluation* process, a water contamination incident is 'confirmed' if the information collected over the course of the threat evaluation provides definitive evidence that the water has been contaminated.

Contamination Site – the location where a contaminant is known or suspected to have been introduced into a drinking water system. For example, a distribution system storage tank where a security breach has occurred may be designated as a suspected contamination site. The contamination site will likely be designated as an *investigation site* for the purpose of *site characterization*.

Cooperating Agency – an agency supplying assistance, other than direct tactical or support functions, or resources to the incident control effort (e.g., Red Cross, telephone companies).

Coordination – the process of systematically analyzing a situation, developing relevant information, and informing the appropriate command authority of viable alternatives for selection of the most effective combination of available resources to meet specific objectives. The coordination process (which can be either intra- or inter-agency) does not involve dispatch actions. However, personnel responsible for coordination may perform command or dispatch functions within the limits established by specific agency delegations, procedures, legal authority, etc.

'Credible' – in the context of the *threat evaluation* process, a water contamination threat is characterized as 'credible' if information collected during the threat evaluation process corroborates information from the *threat warning*.

'Credible' Stage – the second stage of the threat management process from the point at which the threat is deemed 'possible' through the determination as to whether or not the threat is 'credible'.

Drinking Water Primacy Agency – the *agency* that has primary enforcement responsibility for national drinking water regulations, namely, the Safe Drinking Water Act as amended. Drinking water primacy for a particular state may reside in one of a variety of agencies, such as health departments, environmental quality departments, etc. The drinking water primacy agency is typically the State Health Agency or the State Environmental Agency. The drinking water primacy agency may also play the role of *technical assistance provider* to drinking water utilities.

Emergency Operations Center – a pre-designated facility established by an agency or jurisdiction to coordinate the overall agency or jurisdictional response and support to an emergency.

Emergency Response Plan – a document that describes the actions that a drinking water utility would take in response to various emergencies, disasters, and other unexpected incidents.

Event – a planned, non-emergency activity (e.g., parades, concerts, sporting events, etc.).

Immediate Operational Response – an action taken in response to a 'possible' contamination threat in an attempt to minimize the potential for exposure to the potentially contaminated water. Immediate operational response actions will generally have a negligible impact on consumers.

Incident – a confirmed occurrence that requires response actions to prevent or minimize loss of life or damage to property and/or natural resources. A drinking water contamination incident occurs when the presence of a harmful contaminant has been confirmed.

Incident Command System – a standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure appropriate for the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries.

Incident Commander – the individual responsible for the management of all incident operations.

Incident Objectives – statements of guidance and direction necessary for the selection of appropriate strategy(ies), and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources have been

effectively deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow for strategic and tactical alternatives.

Information Officer – the individual responsible for interfacing with the public and media or with other agencies requiring information directly from the incident. Under the ICS, there is only **one** Information Officer per incident.

Investigation Site – the location where site characterization activities are performed. If a suspected *contamination site* has been identified, it will likely be designated as a primary investigation site. Additional or secondary investigation sites may also be identified due to the potential spread of a contaminant.

Jurisdiction – the range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority for incident mitigation. Jurisdictional authority at an incident can be political/geographic (e.g., city, county, State, or Federal boundary lines) or functional (e.g., police department, health department, etc.).

Multi-jurisdiction Incident – an incident requiring action from multiple agencies that have a statutory responsibility for incident mitigation. In ICS, these incidents will be managed under Unified Command.

National Interagency Incident Management System – a program developed by the National Wildfire Coordinating Group consisting of five major subsystems which collectively provide a total systems approach to all-risk incident management. The subsystems are the Incident Command System, Training, Qualifications and Certification, Supporting Technologies, and Publications Management.

Notification – the process of communication information to interested parties.

Opportunity Contaminant – contaminants that might be readily available in a particular area, even though they may not be highly toxic or infectious or easily dispersed and stable in treated drinking water.

'Possible' – in the context of the *threat evaluation* process, a water contamination threat is characterized as 'possible' if the circumstances of the *threat warning* appear to have provided an opportunity for contamination.

'Possible' Stage – the first stage of the threat management process from the point at which the *threat warning* is received through the determination as to whether or not the threat is 'possible.'

Quality Assurance – an integrated system of management activities involving planning, implementation, documentation, assessment, reporting, and quality improvement, to ensure that a process, item, or service is of the type and quality needed and expected by the client.

Quality Control – the overall system of technical activities that measures the attributes and performance of a process, item, or service against defined standards to verify that they meet the

stated requirements established by the client; operational techniques and activities that are used to fulfill requirements for quality.

Response Guidelines – a manual designed to be used **during** the response to a water contamination threat. Response Guidelines should be easy to use and contain forms, flow charts, and simple instructions to support staff in the field or decision officials in the *Emergency Operations Center* during management of a crisis.

Secure Area – a locked space, such as a cabinet or vault, with access restricted to authorized personnel.

Site Characterization – the process of collecting information from an *investigation site* in order to support the evaluation of a drinking water contamination threat. Site characterization activities include the site investigation, *field safety screening*, *rapid field testing* of the water, and sample collection.

Technical Assistance Provider – any organization or individual that provides assistance to drinking water utilities in meeting their mission to provide an adequate and safe supply of water to their customers. The *drinking water primacy agency* may serve as a technical assistance provider.

Threat – an indication that a harmful *incident*, such as contamination of the drinking water supply, may have occurred. The threat may be direct, such as a verbal or written threat, or circumstantial, such as a security breach or unusual water quality.

Threat Evaluation – part of the threat management process in which all available and relevant information about the threat is evaluated to determine if the threat is 'possible' or 'credible', or if a contamination *incident* has been 'confirmed.' This is an iterative process in which the threat evaluation is revised as additional information becomes available. The conclusions from the threat evaluation are considered when making *response decisions*.

Threat Management – the process of evaluating a contamination threat and making decisions about appropriate response actions. The threat management process includes the parallel activities of the *threat evaluation* and making *response decisions*. The threat management process is considered in three stages: 'possible', 'credible', and 'confirmatory.' The severity of the threat and the magnitude of the response decisions escalate as a threat progresses through these stages.

Threat Warning – an unusual occurrence, observation, or discovery that indicates a potential contamination incident and initiates actions to address this concern.

Unified Command – a unified team effort which allows all agencies with responsibility for the incident, either geographic or functional, to manage an incident by establishing a common set of incident objectives and strategies. This is accomplished without losing or abdicating agency authority, responsibility, or accountability.

Unity of Command – the concept by which each person within an organization reports to only one designated person.

Vulnerability Assessment – a systematic process for evaluating the susceptibility of critical facilities to potential threats and identifying corrective actions that can reduce or mitigate the risk of serious consequences associated with these threats.

Water Contamination Incident – a situation in which a contaminant has been successfully introduced into the system. A water contamination incident may or may not be preceded by a water contamination threat

Water Contamination Threat – a situation in which the introduction of a contaminant into the water system is threatened, claimed, or suggested by evidence. Compare *water contamination threat* with *water contamination incident.* Note that threatening a water system may be a crime under the Safe Drinking Water Act as amended by the Bioterrorism Act.

Water Utility Emergency Operations Center Manager – the individual responsible for carrying out the plan for emergency operations at the water utility during an emergency incident.

Water Utility Emergency Response Manager (WUERM) – the individual(s) within the drinking water utility management structure that has the responsibility and authority for managing certain aspects of the utility's response to an emergency (e.g., a contamination threat) particularly during the initial stages of the response. The responsibilities and authority of the WUERM are defined by utility management and will likely vary based on the circumstances of a specific utility.

1 Introduction: Why Should I Read this Module?

The primary audience for this module is drinking water utilities, which need to **plan** for and **practice** managing and responding to contamination attacks. However, there are many other groups that may be involved in responding to water contamination *threats* and *incidents*, and they also may benefit from reviewing this module to assist in their **planning** activities. These groups include analytical laboratories, emergency responders, state *drinking water primacy agencies*, *technical assistance providers*, public health officials, federal agencies (including EPA), and law enforcement agencies, among others. The objectives of this module are:

- To familiarize the reader with the nature and warning signs of water contamination threats and incidents. The reader will learn that drinking water contamination incidents are possible and that contamination threats are probable.
- To describe the overall framework for responding to a range of contamination threats, ranging from hoaxes to confirmed contamination incidents. This framework, the primary focus of the Response Protocol Toolbox (RPTB), is one of the highest water security priorities identified by the water sector and the EPA.
- To help readers prepare for responding to contamination threats through: 1) Careful planning; 2) Development of *Response Guidelines*; 3) Establishing *notification* procedures and internal *chain of command*; and 4) Performing training exercises.

This module is organized into five sections as described below.

Section 1: Introduction: describes the objectives and overall organization of this module.

Section 2: What are Contamination Threats and Incidents? Provides background information on the contamination threat to water systems, including a discussion of potential warning signs of contamination.

Section 3: How Should I Respond to Water Contamination Threats? Discusses the need for response and introduces the concept of 'due diligence' in responding to contamination threats.

Section 4: What Can I do to Prepare? Highlights several areas in which utilities can enhance their preparedness for contamination threats.

Section 5: References and Resources: Lists the references used in the development of this module as well as additional information resources.

Section 6: Appendices: Provides a sample outline for utility Response Guidelines, describes the roles of federal agencies under two U.S. government response plans, and provides an overview of drinking water security applications for on-line monitoring systems.

2 What are Contamination Threats and Incidents?

2.1 Overview of Contamination Threats and Incidents

Both *water contamination threats* and *water contamination incidents* could be designed to interrupt the delivery of safe water to a population, interrupt fire protection, create public panic, or cause disease or death in a population. A water contamination threat occurs when the introduction of a contaminant into the water system is threatened, claimed, or suggested by evidence. A water contamination incident occurs when a contaminant is successfully introduced into the water supply. The water contamination incident may be preceded by a threat, but not always. Both 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.

Some of these consequences would only be realized in the event of a successful contamination incident; however, the mere threat of contamination can have an adverse impact on a water system if improperly handled.

In characterizing any threat, both the **possibility** and **probability** should be considered. A general assessment of the threat of intentional contamination of drinking water indicates that it is **possible** to cause varying degrees of harm by contaminating a water system. Specifically, this assessment indicates that:

- Only a few contaminants have the potential to produce widespread death or disease in a population. These contaminants include concentrated pathogens, biotoxins, and a few highly toxic chemicals that may remain stable in water long enough to adversely impact public health.
- A larger group of contaminants could produce localized death or disease in a segment of a population, including several dozen toxic chemicals.
- Hundreds of contaminants could potentially disrupt service or undermine consumer confidence but would not result in death or disease in the population.

While it is important to consider the range of possibilities associated with a particular threat, assessments are typically based on the **probability** of a particular occurrence. Determining probability is somewhat subjective, and is often based on intelligence and previous incidents. There are historical accounts of intentional contamination of drinking water supplies with biological or chemical contaminants, but most have been associated with wartime activities (http://www.who.int/emc/pdfs/BIOWEAPONS_FULL_TEXT2.pdf). The few documented accounts of intentional contamination of public water systems in the U.S. have not resulted in any reported fatalities. The American Water Works Association Research Foundation (AWWARF) is preparing a report on this subject (AWWARF, 2003). Based on these accounts, it would appear that the probability of a successful contamination incident on a drinking water system is relatively low. However, there has been a reported increase in the interest of various terrorist groups in biological and chemical weapons. Furthermore, some

intelligence information indicates that terrorist organizations have considered water infrastructure as a possible target. Thus, the potential for such an incident does exist.

While the probability of an actual contamination incident may be considered low relative to other modes of attack, the probability of the **threat** of contamination may be relatively high compared to other forms of attack. Many of the apparent security breaches at drinking water utilities that have occurred since 9/11 have been perceived as potential contamination incidents. Although a few threats have been verbal, most have been circumstantial, such as a low-flying airplane over a reservoir or a lock cut from the hatch of a distribution system storage tank. Given the possibility of contamination, many utilities chose to treat these security breaches as potential contamination threats. These incidents demonstrate the need for a protocol to guide an appropriate response to contamination threats.

In order to prepare for contamination threats, there is a general sense that it is necessary to generate a list of priority contaminants. However, the generation of such a list is a significant challenge due to the wide range of adverse effects that might result from intentional contamination, as discussed at the beginning of this section. Furthermore, no list of contamination threats should be considered definitive or complete. A document prepared under the auspices of the World Health Organization succinctly sums up this dilemma, and places it in the context of planning for a response to a biological or chemical contamination incident:

> "A central consideration in such preparedness planning is that it is neither possible nor necessary to specifically plan for attack by all possible biological and chemical agents. If a country is seeking to increase its preparedness to counter the effects of biological and chemical attacks, the targeting of its preparation and training on a limited but well chosen group of agents will provide the necessary capability to deal with a far wider range of possibilities. Knowledge of the general properties of this representative group of agents will enable certain measures to be taken against virtually any other agent. In addition to being impractical from a preparedness perspective, long and exhaustive lists of agents also give a misleading impression of the extent of possible threats."
>
> In: *Public health response to biological and chemical weapons: WHO guidance, 2nd edition (Draft, March 2003),* (http://www.who.int/csr/delibepidemics/biochemguide/en/index.html)

Nonetheless, many federal and private organizations have generated contaminant lists that reflect the specific priorities and assumptions of that organization. For instance, the military is largely concerned with safeguarding the readiness of our combat troops and hence focuses on the classical weapons of chemical and biological warfare, while other organizations are more focused on infectious diseases. While it is possible to use the experience gained from the preparation of these lists, it is very important to consider the special needs and challenges presented by safeguarding public health through protection of the drinking water supply. For instance, there is essentially no tolerance by the public toward sudden disease and death from tainted water supplies. Another challenge is that drinking water is used not only for consumption but also for other uses such as fire protection, sanitation, and industrial processes. In fact, most treated drinking water is used for purposes other than consumption.

Table 1-1 presents a number of contaminant classes that would potentially have an adverse impact if introduced into the drinking water supply. This is not intended to be an exhaustive list, and there may be many others that may be used to contaminate a water supply.

Table 1-1 Contaminant Classes, their Availabilities, and Restrictions

Class	Examples (not exhaustive)	Sources	Limited access?
MICROBIOLOGICAL CONTAMINANTS			
Bacteria	*Bacillus anthracis, Brucella* spp.*, Burkholderia* spp.*, Campylobacter* spp.*, Clostridium perfringens, E. coli* O157:H7, *Francisella tularensis, Salmonella typhi, Shigella* spp.*, Vibrio cholerae, Yersinia pestis, Yersinia enterocolitica*	Naturally occurring, Microbiological laboratories[1], state-sponsored programs	Yes for Select Agents
Viruses	Caliciviruses, Enteroviruses, Hepatitis A/E, Variola, VEE virus	Naturally occurring, Microbiological laboratories[1], state-sponsored programs	Yes for Select Agents
Parasites	*Cryptosporidium parvum, Entamoeba histolytica, Toxoplasma gondii*	Naturally occurring, Microbiological laboratories[1]	No
CHEMICAL CONTAMINANTS - Inorganic			
Corrosives and caustics	Toilet bowl cleaners (hydrochloric acid), tree-root dissolver (sulfuric acid), drain cleaner (sodium hydroxide)	Retail, industry	No
Cyanide salts or cyanogenics	Sodium cyanide, potassium cyanide, amygdalin, cyanogen chloride, ferricyanide salts	Supplier, industry (esp. electroplating)	Yes
Metals	Mercury, lead, osmium, their salts, organic compounds, and complexes (even those of iron, cobalt, copper are toxic at high doses)	Industry, supplier, laboratory	Yes[2]
Nonmetal oxyanions, organo-nonmetals	Arsenate, arsenite, selenite salts, organoarsenic, organoselenium compounds	Some retail, industry, supplier, laboratory	Yes[3]
CHEMICAL CONTAMINANTS - Organic			
Fluorinated organics	Sodium trifluoroacetate (a rat poison), fluoroalcohols, fluorinated surfactants	Supplier, industry, laboratory	Yes
Hydrocarbons and their oxygenated and/or halogenated derivatives	Paint thinners, gasoline, kerosene, ketones (e.g., methyl isobutyl ketone), alcohols (e.g., methanol), ethers (e.g., methyl *tert*-butyl ether or MTBE), halohydrocarbons (e.g., dichloromethane, tetrachloroethene)	Retail, industry, laboratory, supplier	No
Insecticides	Organophosphates (e.g., Malathion), chlorinated organics (e.g., DDT), carbamates (e.g., Aldicarb) some alkaloids (e.g., nicotine)	Retail, industry, supplier (varies with compound)	Yes
Malodorous, noxious, foul-tasting, and/or lachrymatory chemicals[4]	Thiols (e.g., mercaptoacetic acid, mercaptoethanol), amines (e.g., cadaverine, putrescine), inorganic esters (e.g., trimethylphosphite, dimethylsulfate, acrolein)	Laboratory, supplier, police supply, military depot	Yes
Organics, Water-miscible	Acetone, methanol, ethylene glycol (antifreeze), phenols, detergents	Retail, industry, supplier, laboratory	No

Class	Examples (not exhaustive)	Sources	Limited access?
Pesticides other than insecticides	Herbicides (e.g., chlorophenoxy or atrazine derivatives), rodenticides (e.g., superwarfarins, zinc phosphide, α-naphthyl thiourea)	Retail, industry, agriculture, laboratory	Yes
Pharmaceuticals	cardiac glycosides, some alkaloids (e.g., vincristine), antineoplastic chemotherapies (e.g., aminopterin), anticoagulants (e.g., warfarin). Includes illicit drugs such as LSD, PCP, and heroin.	Laboratory, supplier, pharmacy, some from a natural source	Yes
SCHEDULE 1 CHEMICAL WARFARE AGENTS			
Schedule 1 Chemical Weapons	organophosphate nerve agents (e.g., sarin, tabun, VX), vesicants, [nitrogen and sulfur mustards (chlorinated alkyl amines and thioethers, respectively)], Lewisite	Suppliers, military depots, some laboratories	Yes
BIOTOXINS			
Biologically produced toxins	Biotoxins from bacteria, plants, fungi, protists, defensive poisons in some marine or terrestrial animals. Examples include ricin, saxitoxin, botulinum toxins, T-2 mycotoxins, microcystins.	Laboratory, supplier, pharmacy, natural source[5], state-sponsored programs	Yes
RADIOLOGICAL CONTAMINANTS			
Radionuclides	Does not refer to nuclear, thermonuclear, or neutron bombs. Radionuclides may be used in medical devices and industrial irradiators (Cesium-137 Iridium-192, Cobalt-60, Strontium-90). Class includes both the metals and salts.	Laboratory, state sources, waste facilities	Yes[2]

1. The quantity of bacteria, viruses, or parasites needed for widespread contamination of a water system is not available in a typical clinical laboratory, although the seed cultures could be available. For viruses, vaccine production-grade volumes would be needed, requiring special equipment and facilities, perhaps with state-sponsorship.
2. Availability may be commercially limited for the more toxic metals, especially the heavy metals, which can be quite expensive. Iron and copper are readily available, but not usually in soluble (bio-available) forms.
3. Availability of arsenicals and selenium compounds in the retail sector has been reduced owing to environmental regulations, but such products can occasionally be found as part of older inventories of merchandise, especially in small-town hardware stores. Supplies of such materials may generally be too small to cause concern.
4. This grouping includes riot-control agents and other mucous membrane irritants.
5. The quantity available from laboratories, suppliers, and pharmacies needed for widespread contamination of a water system are typically not available from these sources. Many biotoxins that occur naturally would need to be purified or prepared to be of significant concern to water, which could make production beyond the capabilities of most terrorists.

The specific contaminants in Table 1-1 do not directly correspond to the highest priority contaminants; the table is merely illustrative of the relevant contaminant classes. The list of high priority contaminants was used to inform the development of the material in the RPTB (particularly Module 4). The list of high priority contaminants is not included in the RPTB for two reasons. First, as discussed above, such lists are inherently incomplete and hence may provide a false sense of security. Second, such a list could be used with malicious intent if included in a widely circulated document. Accordingly, to support emergency management of water threats and incidents, a resource for contaminant specific information, the Water Contaminant Information Tool (WCIT), is being developed specifically for use by the water sector. The WCIT, along with related information resources, is described in more detail in Module 2, Appendix 8.9.

In reviewing the contaminant classes listed in Table 1-1, it may be apparent that many are not tightly controlled and are considered to be readily available. Most threat analysts consider availability to be the most important characteristic of a contaminant that might be used in a terrorist or criminal activity. The phrase *opportunity contaminant* has been used to describe contaminants that might be readily available even though they may be considered less than optimal from a lethality or dissemination standpoint. In many cases, specific opportunity contaminants may be more readily available on a regional or local basis. For example, a particular industrial chemical or pesticide may be produced at a facility in close proximity to the water treatment plant and its associated distribution system. **Such site specific considerations should be incorporated into a utility's planning and response activities,** particularly with regards to *threat management* (Module 2) and *analytical approach* (Module 4).

In addition to availability, there are other factors that should be considered to better understand the contamination threat to water. Therefore, a broad group of potential contaminants, similar to those contained in Table 1-1, were prioritized with respect to their ability to adversely impact public health. The criteria used to prioritize the contaminants are described in Table 1-2. This prioritization was not intended to be comprehensive for all potential threats to water, but rather to be inclusive of contaminant classes that warrant consideration during the evaluation of a contamination threat or the analysis of a water sample for an unknown contaminant.

Table 1-2. Prioritization Criteria for Potential Water Contaminants

Criterion	Description
Aesthetic impacts	Changes in appearance, odor, or taste of contaminated water that might alert a consumer to the potential danger.
Availability	The ease with which the material can be obtained, synthesized, or harvested from natural sources.
Chlorine resistance	The time that a contaminant remains toxic or infectious after introduction into water containing a chlorine residual under typical distribution system conditions.
Dispersion	The ease with which a contaminant can be effectively dispersed in water.
Handling difficulty	The technical challenges associated with handling the material and introducing it into water.
Outcome of exposure	The health effects within the population resulting from exposure to the contaminant.
Potency	The amount of contaminant that would be required to contaminate a reference volume of water at a lethal or infectious dose. The smaller the amount of material, the higher the rank.
Public fear factor	Perception of the public regarding the risks associated with the contaminant.
Stability	The time that a contaminant remains toxic or infectious after introduction into an aqueous environment.
Storability	The time that a contaminant remains toxic or infectious while in storage.

2.2 Warnings Signs of a Contamination Threat

A *threat warning* is an occurrence or discovery that indicates a potential contamination threat that triggers an evaluation of the threat. The use of information about a threat warning during the initial stage of the *threat evaluation* process is described in more detail in Module 2. It is important to note that these warnings must be evaluated in the context of typical utility activity and previous experience in order to avoid **false alarms**. Figure 1-1 summarizes several potential threat warnings.

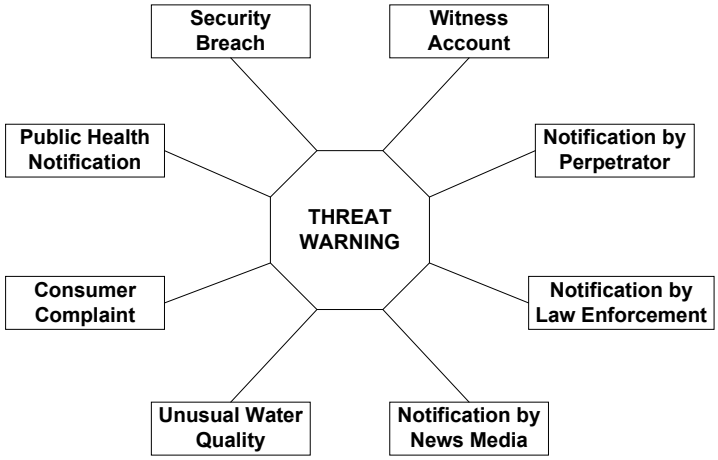


Figure 1-1. Summary of Threat Warnings

The threat warnings shown in this figure are intended to be inclusive of those most likely to be encountered, but this listing is by no means comprehensive. Following is a brief description of each of these warnings. A thorough discussion of these warnings is provided in Module 2.

- Security Breach. Physical security breaches, such as unsecured doors, open hatches, and unlocked/forced gates, are probably the most common threat warnings. In **most** cases, the security breach is 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. Note: the witness may be a utility employee engaged in their normal duties.

- 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 are more likely than written threats. While the notification may be a hoax, threatening a drinking water system may be a crime under the Safe Drinking Water Act as amended by the *Bioterrorism Act*, and should be taken seriously.

- Notification by Law Enforcement. A utility may receive notification about a contamination threat directly 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 to appreciate 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.

- Unusual Water Quality Parameters. The relationship between contamination and changes in water quality parameters is not well understood. However, it is appropriate to investigate the cause of unusual changes in water quality parameters. For water systems, changes in water quality parameters, such as pH, chlorine residual, turbidity, etc. may be detected through the use of either on-line monitors or grab samples. In utility operations, this data may arise from several sources: samples collected for plant operations, routine baseline monitoring programs (Section 4.9), and monitoring systems designed to provide early warning of changes in water quality (Section 6.2). The results of these approaches may be used to warn of a threat. However, as discussed in Sections 4.9 and 4.10, it is vital to consider the reliability of the results from the particular detection method or on-line monitoring system (i.e., false positives/false negatives, known interferences, instrument reliability, and unusual water quality conditions associated with a known cause, such as overdosing of coagulant).

- Consumer Complaint. An unexplained or unusually high incidence of consumer complaints about the aesthetic qualities of drinking water may indicate potential contamination. Many chemicals can impart a strong odor or taste to water, and some may discolor the water. Taste and odor complaints are quite common for water utilities, but unique taste and odor problems, particularly very unusual tastes and odor complaints clustered in a geographical area, may indicate additional problems.

- Public Health Notification. In this case, the first indication that contamination has occurred is the appearance of victims in local emergency rooms and health clinics. Utilities may therefore be notified, particularly if the cause is unknown or linked to water. An incident triggered by a public health notification is unique in that at least a segment of the population has been exposed to a harmful substance. If this agent is a chemical (including biotoxins), then the time between exposure and onset of symptoms may be on the order of hours, and thus there is the potential that the contaminant is still present. On the other hand, the incubation period for most pathogens is on the order of days to weeks; thus, the pathogen may have moved through the distribution system and may therefore be below detectable limits, or present only in trace quantities.

3 How should I Respond to Water Contamination Threats?

This section is not designed to discuss what specific steps to take in responding to a contamination threat. Various "What to do?" steps in the response process will be discussed in Section 4 and associated modules. Rather, the questions addressed in this section are "Why is it necessary to respond to contamination threats at all?" and "When have I done enough?"

3.1 I'm Just a Utility—Why Do I Need to do Anything at All?

As discussed in Section 2, it is technically possible to introduce a contaminant into a public water supply, and historical evidence suggests that the threat of contamination is indeed probable. Regardless of whether contamination is actual or threatened, both deeply impact the public health mission of water utilities. Water utilities play an essential role in providing safe and reliable drinking water supplies, preventing many problems and diseasees that flourish in the absence of safe water programs. Most water utilities take their public health mission very seriously, and some are proactive in developing their plans to respond to water contamination threats. They do this often because they realize that planning for contamination events may also be beneficial in developing a more effective response to other types of emergencies.

Proper planning is a delicate process because public health measures are rarely noticed or appreciated except when they fail. Consumers are particularly upset by unsafe water because safe drinking water is often viewed as an entitlement, and indeed, it is reasonable for consumers to expect a high quality product. Public health failures during response to contamination threats often take the form of too **much** or too **little** action. The results of too little action, including no response at all, can have disastrous consequences potentially resulting in public disease or fatalities. On the other hand, a disproportionate response to contamination threats that have not been corroborated (i.e., determined to be 'credible') can also have serious repercussions when otherwise safe water is unavailable. Not only would the water be unavailable for human consumption, but it would also be unavailable for sanitation, firefighting, industry, and the many other uses of public water supply. These adverse impacts must be considered when evaluating response options to a contamination threat.

Considering the potential risks of an inappropriate response to a contamination threat, it is clear that a systematic approach is needed to evaluate contamination threats. This systematic approach is developed throughout the RPTB. One overriding question is "When has a drinking water utility done enough?" This question may be particularly difficult to address when considering the wide range of agencies that may be involved in a threat situation. Other organizations, such as EPA, CDC, law enforcement agencies, health departments, etc., will each have unique obligations or interests in responding to a contamination threat.

3.2 Due Diligence—When Have I Done Enough?

The guiding principle for responding to contamination threats is one of 'due diligence' or "what is a suitable and sensible response to a contamination threat?" As discussed above, some response to contamination threats is warranted due to the public health implications of an actual contamination incident. However, a utility could spend a lot of time and money over-responding

to every contamination threat, which would be an ineffective use of resources. Furthermore, over-response to a contamination threat carries its own adverse impacts.

Ultimately, the answer to the question of 'due diligence' must be decided at the local level and will depend on a number of considerations. Among other factors, local authorities must decide what level of risk is reasonable in the context of a perceived threat. Careful planning is essential to developing an appropriate response to contamination threats, and in fact, one primary objective of the RPTB is to aid users in the development of their own site-specific plans that are consistent with the needs and responsibilities of the user. Beyond planning, the RPTB considers a careful evaluation of any contamination threat, and an appropriate response based on the evaluation, to be the most important element of due diligence.

Figure 1-2 provides an overview of the response process presented in the RPTB that illustrates (through the two expanding vertical arrows) that response actions escalate as the credibility of a threat increases. In the RPTB, the threat management process is considered in three successive stages: *'possible'*, *'credible'*, and *'confirmed'*. Thus, as the threat escalates through these three stages, the actions that might be considered due diligence expand accordingly. The following paragraphs describe, in general terms, actions that might be considered as due diligence at these various stages. Module 2 describes the evaluation of these stages, and associated response actions that might be considered at each stage.

- Stage 1: "Is the threat possible?" If a utility is faced with a contamination threat, they should evaluate the available information to determine whether or not the threat is 'possible' (i.e., could something have actually happened). If the threat is 'possible,' *immediate operational response* actions might be implemented, and activities such as *site characterization* would be initiated to collect additional information to support the next stage of the threat evaluation.

- Stage 2: "Is the threat 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.' Given the higher threshold at this stage, more significant response actions might be considered, such as restrictions on public use of the water (e.g., issuance of a 'do not drink' notice). Furthermore, steps should be initiated to confirm the incident and positively identify the contaminant.

- Stage 3: "Has the incident been confirmed?" Confirmation implies that definitive evidence and information have been collected to establish the presence of a harmful contaminant in the drinking water. Obviously, at this stage the concept of due diligence takes on a whole new meaning since authorities are now faced with a potential public health crisis. Response actions at this point include all steps necessary to protect public health, to supply the public with an alternate source of drinking water, and to begin remediation of the system.

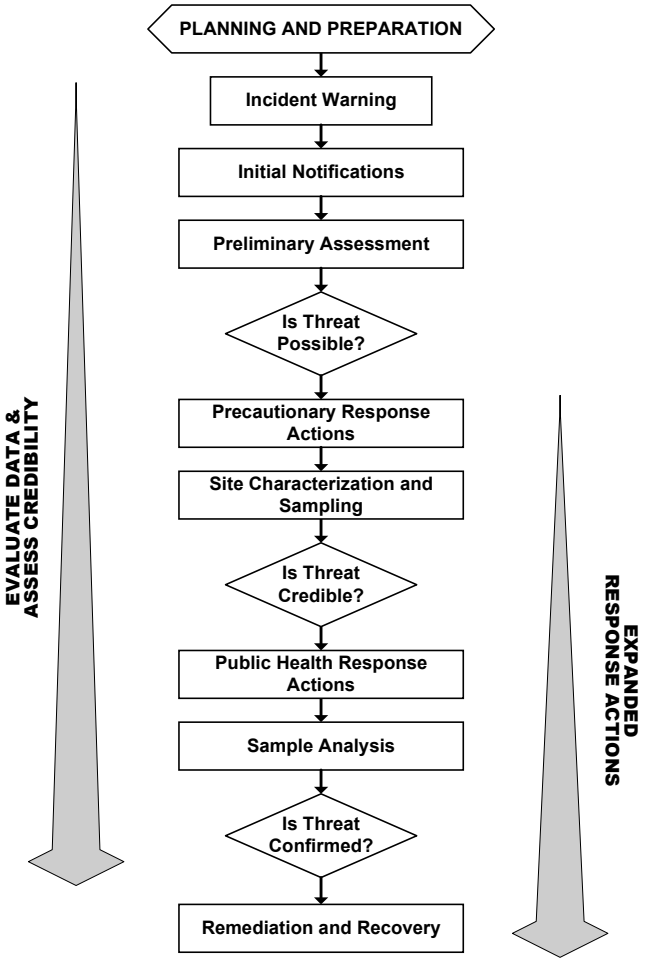


Figure 1-2. Overview of Response to a Contamination Threat

If the process outlined in Figure 1-2 is followed as far as the situation warrants, and the responsible parties use it as a guide in making appropriate response decisions, then they may be viewed as exercising 'due diligence.' All the modules of the RPTB contain in-depth information about the application of the process. In particular, Module 2 describes threat management and the three stages of the threat evaluation in great detail. **The application of this process to a specific contamination threat will vary significantly with the circumstances of the threat.** In summary, judgment must be exercised when determining how to appropriately manage a specific contamination threat. Tabletop exercises, described below in Section 4.7, may provide valuable practice in this regard.

4 What Can I do to Prepare?

One of the steps that utilities can take to prepare for contamination threats is to **read relevant modules of the "Response Protocol Toolbox" and use the information contained within to develop their own specific Response Guidelines and updated Emergency Response Plans!** Specific planning and preparation activities are summarized in the following subsections.

4.1 Know your Water System

4.1.1 Construction and Operation

Each water system is unique with respect to age, operation, and complexity. Distribution systems are particularly unique in that many are a complex, and often undocumented, mix of relatively new and old components. Accordingly, understanding a distribution system as it relates to water security and response planning may be an equally complex task. Despite the challenges to understanding a water supply system, the benefits of doing so could include effectively managing threats and preventing the spread of potentially contaminated water. For instance, the water system may have structural features that enable effective isolation of a contaminated area. Also, it may be readily apparent from knowledge of system vulnerabilities that it would be very easy to introduce a contaminant at a particular location.

There are many ways to gain a better understanding of a particular water system, one of which is through a *vulnerability assessment*. Perpetrators who intentionally contaminate water may seek to produce an adverse consequence through exploitation of vulnerabilities. All drinking water plants are, to some degree, vulnerable to intentional contamination incidents. The nature and extent of these vulnerabilities depends on a number of factors such as source water type, treatment plant type, type of primary disinfectant used, residual disinfectant used in the distribution system, and security measures already in place. An assessment of the drinking water plant and system may help to identify key locations that are vulnerable to intentional contamination, or the availability of opportunity contaminants that might be prevalent in the area. Better understanding the vulnerabilities of a water system provide a basis for improving physical security against intentional contamination and preparing for the evaluation of contamination threats. Accordingly, the Bioterrorism Act established requirements that community water systems serving more than 3,300 individuals perform a system specific vulnerability assessment for potential terrorist threats, including intentional contamination (http://www.epa.gov/safewater/security/community.html).

Another aspect of the water system that may be important, particularly in evaluating the potential spread of a suspected contaminant, is its hydraulic configuration and operation. Propagation of a contaminant through a system is dependent on a number of factors, including: mixing conditions at the point of contamination, hydraulic conditions within the system at the time of the contaminant introduction, and reactions between the contaminant and other materials in the system. There are several techniques for understanding the hydraulics of a water supply system. As discussed more completely in Module 2, Section 2.3.1, developing this understanding may be as complex as utilizing a GIS system in conjunction with a hydraulic modeling program or as simple as manually mapping the pressure and flow zones within a system.

Information about construction materials used in the system may be contained within the utility records and can be useful in evaluating the fate and transport of a particular contaminant through a system. For example, a particular contaminant may adsorb to the pipe material used in a utility's distribution system, and this type of information would be critical in evaluating remediation options following a contamination incident (see Module 6).

4.1.2 Personnel

The employees of a 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 importance of knowledgeable and experienced personnel is highlighted by the complexity of most water treatment and distribution systems. This complexity makes a successful contamination of a specific target contingent upon detailed knowledge of the system configuration, hydraulic conditions, usage patterns, and water quality. If perpetrators have somehow gained a sophisticated understanding of a water supply system, the day-to-day experience of water system personnel will prove an invaluable tool to countering any attacks. For instance, personnel may continually look for unusual aspects of daily operation that might be interpreted as a potential threat warning, and may also be aware of specific characteristics of the system that make it vulnerable to contamination.

4.1.3 Customers

Knowledge of water system customers is an important component of preventing and managing contamination incidents. Prevention is based largely on understanding potential targets of contamination. Of special concern may be hospitals, schools, government buildings, or other institutions where large numbers of people could be directly or indirectly affected by a contamination threat or incident. Steps taken to protect the drinking water supply for these critical customers, such as enhancements to the physical security of distribution system elements at these locations, may deter the attack itself.

Water customers vary significantly with regard to their expectations of what constitutes acceptable water service, so it is necessary to consider the manner in which water is used in a particular system. For example, high water demand that is largely driven by industry has different implications compared to high usage rates in an urban center with a high population density. Some customers, such as hospitals and nursing homes, may have certain water quality requirements. Sensitive sub-populations, including children and the elderly, can exhibit adverse health effects at doses more than an order of magnitude lower than those necessary to produce disease or death in a healthy adult. That being said, for the purposes of managing water contamination threats, it is important to keep in mind that the most important goal is protecting the health of the public as a whole. Planning, preparation, and allocation of resources should be directed toward protecting the public at large, beyond specific demographic groups or individual users.

4.2 Update Emergency Response Plans for Intentional Contamination

Emergency response plans (ERPs) are nothing new to water utilities, since many have developed ERPs to deal with natural disasters, accidents, civil unrest, etc. Because water utilities are a vital part of the community, it has been prudent for many utilities to develop these in order to help ensure the continuous flow of water to the community. However, many water utility ERPs developed prior to 9/11 do not explicitly deal with terrorist threats, such as intentional contamination. Recently, the U.S. Congress required community water systems serving a population greater than 3,300 to prepare or revise, as necessary, an ERP to reflect the findings of their vulnerability assessment and to address terrorist threats (http://www.epa.gov/safewater/security/community.html).

In response to the legal mandate to revise ERPs, there is an increased demand for guidance that addresses terrorist threats to water supply systems. The U.S. EPA is preparing this guidance, which will be published in a separate document (U.S. EPA, 2003b, "Drinking Water Model Emergency Response Plan," in development. See also U.S. EPA, 2003c, "Large Water System Emergency Response Plan Outline: Guidance to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002). For those existing plans that can be revised, information contained in this RPTB may help utilities to address the contamination threat in their revised ERPs, although it should be noted that there is no regulatory requirement to use the RPTB in this manner. However, the RPTB does provide a framework that will aid utilities in planning an effective response to contamination threats, which might be considered during revision to their ERP.

4.3 Develop Response Guidelines for Intentional Contamination

Although not a formal part of an ERP, utilities may wish to develop *Response Guidelines* (RGs) for managing contamination threats. RGs are different from ERPs in that they are essentially a "field guide" for responding to contamination threats. RGs may be developed in many different formats, but a core feature of any RG is that it is easy to use in the field and under crisis conditions. Because RGs are used in the field, they should be action-oriented, easy to follow, and contain all the necessary forms and information. For instance, they should contain forms to document observations at the site of a suspected contamination incident and to log samples collected from the site. Additionally, the guidelines might include flow charts depicting the steps of a process, simple reference tables, and other information that can easily be used during the intense period of an initial response to a threat. A trained individual should be able to follow a well organized RG with minimal difficulty. While the RPTB is not set up in the streamlined format of an effective set of RGs, the material contained in the RPTB can certainly support the development of guidelines, and an example outline for a set of RGs is included in Appendix 5.1 of this Module. The outline may be filled using model text, figures, and forms contained in the various modules of the RPTB, in addition to the users' own materials.

4.4 Establish Structure for Incident Command

One of the primary reasons that ERPs and RGs fail (for any type of emergency, not just water contamination) is that there is no clear leader established by the plan. Thus, in planning for a water emergency, it is important to establish a command structure. This involves establishing a

chain of command, identifying key individuals, and clearly defining their roles and responsibilities, so that they may effectively manage the emergency situation. This section describes an incident command structure based on the *Incident Command System (ICS)*. See http://training.fema.gov/EMIWeb/IS/is195.asp for ICS training material produced by FEMA.

In summary, ICS is the model tool for command, control, and coordination of a response to a public crisis. The tool provides a means to coordinate the efforts of individual agencies as they work toward the common goal of stabilizing the incident and protecting life, property, and the environment. The rationale is that large-scale disasters may be multi-jurisdictional and require cooperation among several agencies. Furthermore, ICS is used by many local, state and federal response agencies and is part of the National Interagency Incident Management System (NIIMS). Note that NIIMS is different than the National Incident Management System (NIMS), which is under development for use by the National Response Plan (see Appendix 6.2 of this Module).

Federal law requires hazardous materials (HazMat) responders to use ICS, and many States are adopting ICS as their standard for responding to all types of incidents. However, in the 'possible' stage of the evaluation of a water contamination threat, HazMat will probably not be involved, and the mandated ICS may not be applied. Rather, the utility, or possibly a technical assistance provider such as a state drinking water primacy agency, would manage the threat. However, at some point following the determination that a contamination threat is 'credible,' the existing ICS at the local or State level would likely be implemented. For major disasters and emergencies, including terrorist acts, the Federal Response Plan (see Appendix 6.3 of this Module) provides the mechanism for federal departments and agencies to coordinate delivery of Federal assistance and resources to augment efforts of overwhelmed local and State governments. Fortunately, one of the benefits of ICS is its ability to expand and contract based on the needs of the situation. Thus, to make potential expansion as seamless as possible, it seems logical that utilities adopt ICS conventions during their response to a contamination threat, even during the 'possible' stage, to facilitate coordination between the utility and other responding agencies that may become involved at a later stage.

Figure 1-3 (left) provides a schematic of ICS for a water utility during a 'possible' threat, in which utility staff have primary responsibility for managing the threat (see Module 2, Section 3). It is anticipated that during this initial stage, the water utility staff will conduct the threat evaluation (Figure 1-3, top middle). At some point during the response to a 'credible' threat, various responding agencies would be organized under ICS according to the principle of *unified command*, and the IC might be someone from an outside organization such as FBI or the State/local health department (Figure 1-3, bottom middle). Unified command is a team effort which allows all agencies with responsibility for the incident, either geographic or functional, to manage an incident by establishing a common set of incident objectives and strategies. This is accomplished without abdicating agency authority, responsibility, or accountability. When command is transferred, it is anticipated that water utility staff will continue to occupy roles in the command structure, but this is at the discretion of the new incident commander. Figure 1-2 (right) is an example of unified command under ICS that might be assembled to respond to a 'confirmed' water contamination incident. For 'confirmed' incidents, it is assumed that an agency external to the water utility has assumed responsibility for incident command. However,

the utility will still have a role in this incident command structure since they are responsible for the operation and maintenance of the drinking water system.

Figure 1-3 is primarily intended to illustrate the expanding nature of the incident, show model ICS structures, and point out the changing role of the water utility in the command structure. It must be customized for a particular situation, and should be expanded and contracted as necessary. Regardless of the size and shape, the command structure operates most efficiently if each person in an organization reports only to one designated individual, a concept known as *unity of command*. Likewise, communication outside of the command structure should be made only through designated individuals (i.e., information officers, liaison officers, or points of contact). Following are some definitions used in Figure 1-3.

1. *Incident commander* (IC): The IC sets incident objectives and priorities, and has overall responsibility for management of the incident. Thus, for water contamination, the incident commander coordinates all the activities involved, whether they are related to the water utility, local civil defense, public health, public works, etc. One key role of incident command is to effectively communicate with all participants involved in the management of the incident, including those outside of the water utility's own command structure. Various individuals may assume the role of incident commander depending on the stage of the response. In ICS, the initial incident commander is traditionally defined as the senior first-responder to arrive at the scene. However, due to the nature of water contamination events triggered by the warnings described above, it is likely that there will need to be a designated individual at the water utility who becomes the incident commander when a threat is reported. This individual is known as the water utility emergency response manager (WUERM).

2. *Water Utility Emergency Response Manager* (WUERM): The WUERM is an individual (or several individuals) with designated responsibility for managing the utility's response to a contamination threat or incident. As discussed above, the WUERM will likely serve as IC during the early stages of the response. Given this responsibility, the WUERM should be empowered to make decisions regarding the threat evaluation (i.e., determining whether or not a threat is 'possible') and response decisions in the early stages of the threat management process. Should the threat rise to an appropriate level, the WUERM may recommend that the *emergency operations center* (EOC) be activated. Once the threat or incident rises to a level such that responsibility for incident command is transferred to another organization, the WUERM will still have a significant role in the response, and will likely serve as the utility's representative in the ICS structure.

3. *Water Utility Emergency Operations Center Manager* (WUOCM): The WUOCM is an 'emergency manager' who heads the water utility's EOC, which is responsible for operational and resource management during an emergency. The general position of 'emergency manager' is described in FEMA's training documents, http://training.fema.gov/EMIWeb/IS/is1.asp, although specific duties for water utilities may differ. In most cases, responsibilities of the WUOCM and the WUERM will fall upon different individuals.

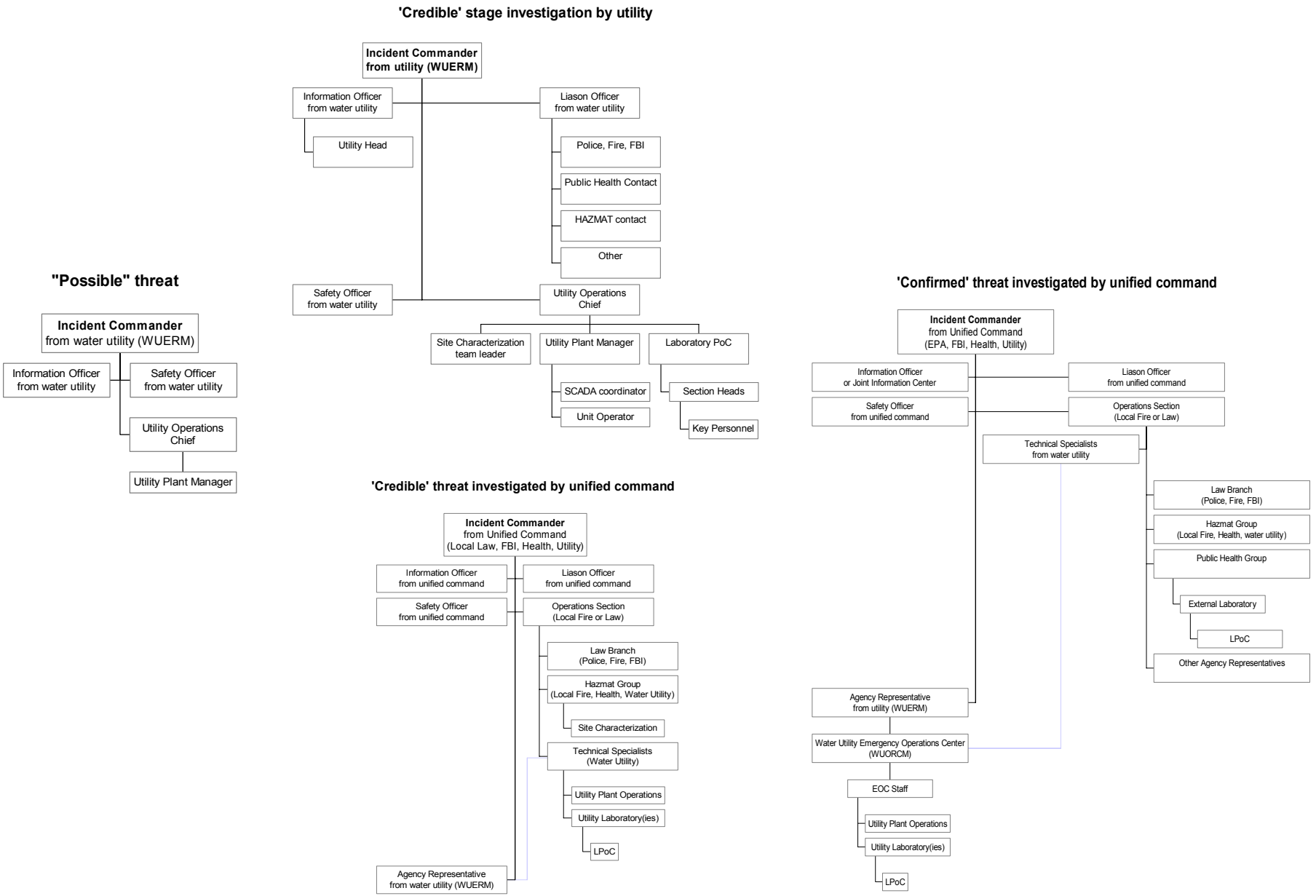


Figure 1-3. Expansion of, and Changes to, Incident Command Structure for the Three Threat Evaluation Stages

4. *Information Officer (IO)*: The IO is part of the command staff and reports directly to the IC. The IO is responsible for planning the information strategy, discussed in Section 4.5 below. Another very important role of the IO is interfacing with the media and disseminating public information.

5. *Liaison Officer (LO)*: The LO is part of the command staff and is the on-scene contact for representatives from other agencies assisting with the incident.

6. *Laboratory Point of Contact (LPoC)*: The LPoC is the designated person at the laboratory with whom the WUERM (or IC) communicates. The LPoC coordinates analytical activities with the WUERM (or IC) and reports analytical results only to the WUERM (or IC).

7. *Safety Officer*: The Safety Officer's function is to develop and recommend measures for assuring personnel safety, and to assess and/or anticipate hazardous and unsafe situations. Only one Safety Officer should be assigned per incident. The Safety Officer may have assistants as necessary, and the assistants may also represent assisting agencies or jurisdictions. Safety assistants may have specific responsibilities such as air operations, hazardous materials, etc.

8. *Agency Representatives*: In many *multi-jurisdiction incidents*, an agency or jurisdiction will send a representative to assist in coordination efforts. An Agency Representative is an individual assigned to an incident from an *assisting agency* or *cooperating agency* who has been delegated authority to make decisions on matters affecting that agency's participation at the incident. Agency Representatives report to the Liaison Officer, or to the Incident Commander in the absence of a Liaison Officer. As illustrated in Figure 1-3, if the WUERM is not the incident commander, then the WUERM may be the agency representative for the drinking water utility in the ICS.

9. *Technical Specialists*: Certain incidents or events may require the use of Technical Specialists who have a specialized knowledge and expertise. As illustrated in Figure 1-3, Technical Specialists may be assigned to any aspect of the response where their services are required. Because water utility staff have intimate knowledge of their own system, there role in this position will be invaluable during every stage of the response.

The identity of the WUERM, WUOCM, IO, LO, LPoC, and other designated individuals should be determined locally, based on the utility's size, needs, and responsibilities. Large systems may need to designate multiple WUERMs such that one is always available. Small utilities and small communities may have an abbreviated version of command structure. In this case, the WUERM, WOURC, IO, LO, and other designation individuals could be the same person, or some of these positions may be filled by individuals outside of the utility (e.g., from local government). For the case of the small utility, it may greatly enhance the response process if the particular individual understands ICS, because the small utility may need to coordinate with a larger, better resourced organization, like a state or federal entity. Also, in small systems, the WUERM will likely need to engage other decision officials at the state or local level earlier in the process than will the WUERM at large utilities.

4.5 Develop Information Management Strategy

As described previously, the role of the IO is to manage the large amount of information that might be used during the threat evaluation process and to support decisions about various response actions. For instance, Module 2 describes a number of information resources that may be of use during the threat evaluation process, but only if the information has been properly managed and is readily accessible. Thus, provisions should be made to readily access this information.

Crisis Information Management Software (CIMS) may be useful, especially when interfaced with a central data repository and/or electronic data management system. A description and comparison of several commercial CIMS packages has been prepared by the Department of Justice (DOJ, http://www.ncjrs.org/pdffiles1/nij/197065.pdf). A Field Operations and Records Management System (FORMS), originally developed for EPA's Contract Laboratory Program, may also help manage records relevant to sample documentation, analysis, and tracking during evaluation of water threats (http://www.epa.gov/superfund/programs/clp/f2lite.htm).

Another component of information management is planning for the flow of information during the response to a threat or incident. The individuals or agencies responsible for receipt and management of information are related to the communication strategy described in the next section. However, as part of the information management strategy, a plan must be developed for the flow of information to appropriate individuals within the ICS structure. The release of inaccurate information at an inappropriate time can have severe consequences for the response, criminal investigation, and well-being of the public.

The proper flow of communications during a crisis can be facilitated through the establishment of a Joint Information Center (JIC), a structure that works within the framework of ICS (See http://www.nrt.org/production/nrt/home.nsf/Resources/publications/$FILE/JIC.pdf for a JIC model). This model documents a plan for conducting crisis communications during response to emergencies in which multiple organizations need to collaborate to provide timely, useful, and accurate information to the public and other stakeholders. The model was designed based on requirements identified by the National Response Team (http://www.nrt.org). Although the model was not developed expressly for water utilities, some of the criteria used in the model's development are appropriate for a water utility's information management strategy. Because it is designed on the basis of function, the model can be used during any situation in which there is a need for centralized communications support involving multiple organizations.

It is important to highlight the IO's responsibility as a contact for the media and public. In this manner, the media and public receive information from a single source, which may help eliminate the confusion inherent to an emergency situation. It is important for the media and public to understand that the IO is the only official source of information about the emergency, and that they are receiving information from a consistent source. For this reason, it may be desirable that the IO remains the same even if the incident commander changes, as may be the case for incidents that reach the 'confirmed' stage (see Figure 1-3).

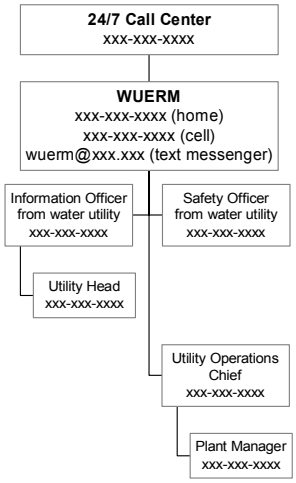
4.6 Establish Communication and Notification Strategy

The ICS requires communication strategies be planned and made available to all potential participants prior to an actual incident or threat. For the purposes of responding to a water contamination threat, the ICS structure illustrated in Figure 1-3 indicates there could be several management levels within the utility, as well as external to the utility, that may be involved in the management of a contamination threat. The hierarchy of potential participants includes: the utility, local government, the regional government (e.g., county), state government, and federal government. Not all of these levels would necessarily be involved in every situation; however, the mechanism and process through which they interact must be decided in advance of an incident to achieve optimal public health and environmental protection. Due to the number and variety of possible participants, **planning for effective communication is critical.** ICS employs two main strategies to ensure effective communication. The first is the use of common terminology, and the second is unity of command.

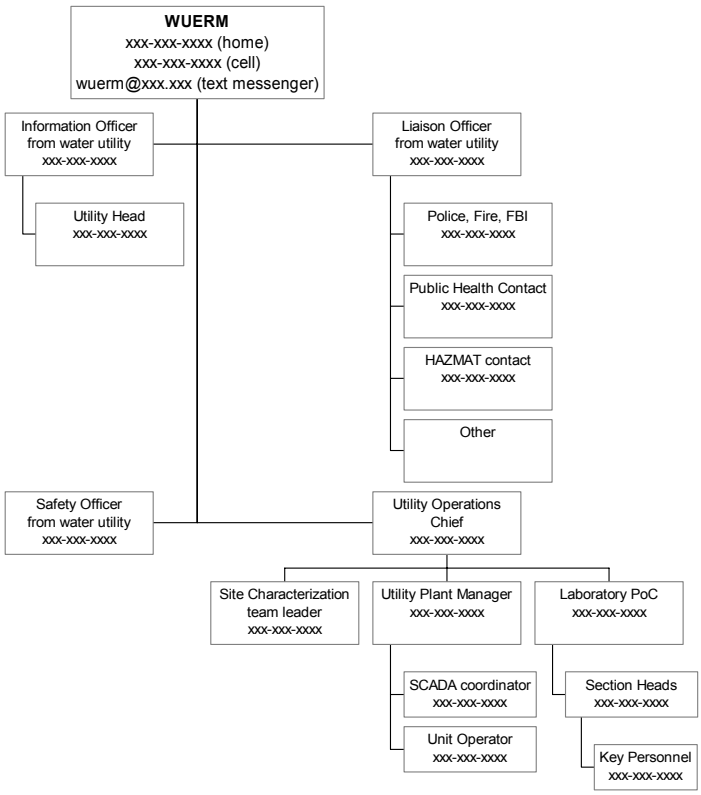
Regardless of the strategy employed within the ICS, developing the plan requires a significant level of effort. An effective communication plan is more than just the telephone directory of utility employees and external contacts, although such a directory is often beneficial. Rather, planning communications involves developing a notification hierarchy for reporting threat warnings and other critical information to appropriate individuals at each stage of the response. Many of the individuals that would need to be notified at key points in the response are identified in the ICS, but others may be outside the ICS chain of command. For example, the head of the utility or the drinking water primacy agency may wish to be notified in the case of any threat, although neither may be in the ICS chain of command. However, in general, communications should proceed along the chain of command of the ICS. The number of people notified will increase as the incident expands and decreases as it contracts toward its conclusion. The exact persons notified will be at the discretion of the IC with interaction with the IO, and should be planned in advance. Local requirements may influence the required communication at the various stages.

Figure 1-4 is designed to illustrate the expanding nature of notifications as the threat evaluation proceeds through the 'possible,' 'credible,' and 'confirmed' stages. Figure 1-4 is primarily intended to show the utility's role in the communications, which is based on the ICS structure shown in Figure 1-4. Accordingly, the communications depicted in Figure 1-4 are only those parts of Figure 1-3 in which the utility is involved. The three stages in Figure 1-4 illustrate a possible structure of the communication hierarchy upon expansion but does not necessarily define the exact path or circumstances under which expansion will occur as a threat escalates. Careful planning and thoughtful actions during the management of the threat will dictate how this expansion will occur. Figure 1-4 shows an example notification hierarchy for each stage of the threat management process, and in the situation in which the credibility determination is made by the utility and the credibility determination is made by an external organization. Utilities should plan communication schemes for both of these cases because, although the role of individuals within the ICS may change, the individual involved will not.

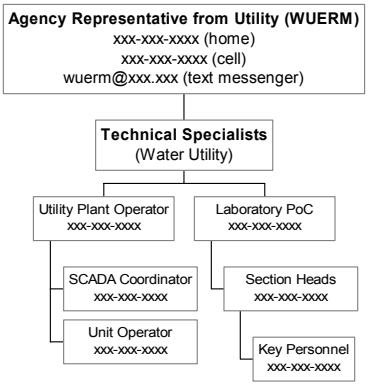
'Possible' stage evaluation by utility



'Credible' stage evaluation by utility



'Credible' stage evaluation by unified command



'Confirmed' stage evaluation by unified command

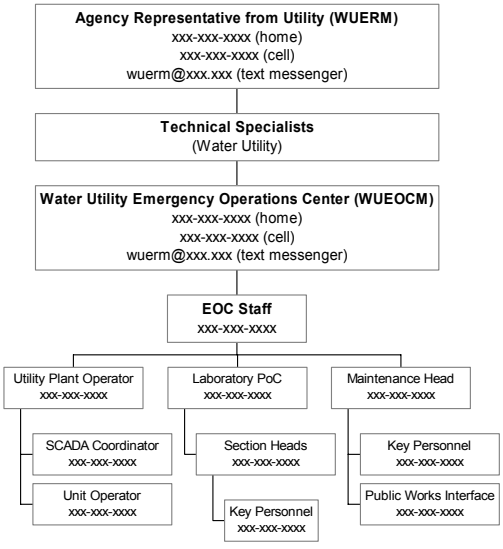


Figure 1-4. Sample Communication Schemes for the Three Threat Evaluation Stages

For the 'possible' stage (Figure 1-4, top left), most of the communications and notifications are internal and begin with the WUERM being notified about the threat. However, depending on the nature of the threat warning, it may be necessary to notify external agencies at the 'possible' stage (e.g., notification of law enforcement in the case of a direct threat from a perpetrator). Utilities must establish some mechanism for informing the WUERM of the incident. A 24/7 operations center may be effective for this purpose. The scale and staffing of an operations center will vary substantially with utility. For example, a large utility may have a continually staffed center. A smaller utility may provide the WUERM(s) with a cell phone or perhaps leverage other call centers that exist within the local government.

The WUERM is notified first, and then the WUERM may notify the heads of other departments to get their support for the threat evaluation. The WUERM would also continue notification along the management chain to keep them apprised of the situation. As the threat management process expands, it may be necessary to activate the IO to manage communications with the utility's management chain, as well as external parties. This will allow the WUERM to focus on the overall management of the response to the contamination threat.

It is likely that the utility will carry out the initial phases of the threat evaluation at the 'credible' stage. Figure 1-4 (top right) shows a sample communication scheme, based on internal utility staff and also external parties that may be able to provide information and technical assistance relevant to the threat evaluation. Figure 1-5 expands on some of the "other" external parties that the IO or LO in Figure 1-4 (top right) may need to contact. Note that the local entities in this figure may be contacted earlier than those at higher levels of government.

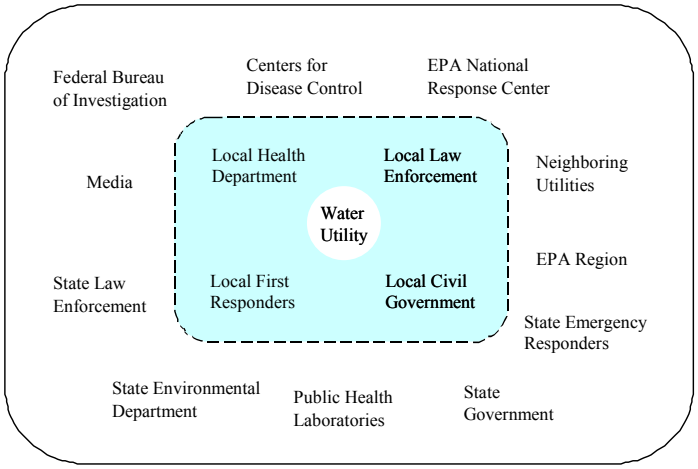


Figure 1-5. Overview of Potential External Notifications

Figure 1-5 does not seek to define a notification scheme or their possible role within the ICS structure – both of these tasks will be incident-specific and/or dictated at the local level. Rather, the figure provides a basic structure for the parties typically involved. These parties are divided into those that are external but still local, and those that are external but at higher levels of government. Notifications by the utility during the threat evaluation at the 'credible' stage

include the drinking water primacy agency (often the State), the emergency response community (including HazMat, EMS, etc.), law enforcement agencies (local, state, and/or federal), government agencies (local, state, and/or federal), the public health community, and external laboratories. Not all of these notifications need to be made in every incident—the overall response plan may dictate what level of notifications should occur and at what stage of the threat evaluation, which in turn dictates who will make the notification. For instance, depending on State requirements, it may not be appropriate for the utility to contact the EPA National Response Center directly. Nevertheless, contact information should be available for all individuals and organizations that may need to be contacted.

If additional support agencies (e.g., HazMat or law enforcement) respond during the 'credible' stage of the threat evaluation, then incident command may be transferred to one of these agencies (Figure 1-4, bottom left). However, staff from the utility's command structure, such as the WUERM, IO and the LO, may still be extremely helpful advisors to the new incident commander; thus, the utility's contact list should be available to unified command. Unified command will handle most communications at this point, so Figure 1-4 (bottom left) only depicts those parts of the ICS structure in which the utility will be involved. The communication strategy represented in Figure 1-4 (bottom left) conforms to Figure 1-3. In this case, more specialized individuals at the water utility become involved as technical specialists, and the WUERM is now acting as the Agency Representative from the water utility. The technical specialists will be a very important part of the ICS, and the utility should plan communication with these individuals carefully.

The 'confirmed' stage pictured in Figure 1-4 (bottom right), represents a significant change in the communication structure because an external agency operating under unified commend will be in charge of the response. Also, the Water Utility Emergency Operations Center (WUEOC) will likely be activated (if it was not already during the 'credible' stage). The chain of communications may proceed through the WUEOC manager (WUEOCM). Technical Specialists that participate in the ICS operated under unified command may also be part of the EOC staff. Additional technical specialists may need to be notified, such as those responsible for repair and maintenance, who would not necessarily be engaged before the incident is confirmed. The role of the utility in overall management and command of the incident may proportionally decrease as many other external parties become involved (see Figure 1-5).

4.7 Perform Training and Desk/Field Exercises

In addition to a lack of planning, another reason that emergency response plans fail is lack of training and practice. Training provides the necessary means for everyone involved to acquire the skills to fulfill their role during an emergency. It may also provide important 'buy-in' to the response process from both management and staff, which is essential to the success of any response plan. Desk exercises (also known as 'tabletops' or 'sand lots') along with field exercises allow participants to practice their skills. Also, these exercises will provide a test of the plan itself, revealing strengths and weakness that may be used to improve the overall plan. Improvements can include measures not only for intentional contamination of water, but also for other emergencies faced by the water utility and the community at large.

Training may be available from EPA or other federal partners. For instance, several online training courses relevant to emergency management are available on-line from FEMA (http://training.fema.gov/EMIWeb/IS/crslist.asp). These courses cover a range of topics including community disaster exercises, emergency manager orientation, and animal health and safety during disasters. Further, it is worthwhile mentioning some areas where formal training is desirable, but not currently available. For example, in addition to training for sampling and site characterization, there are also training needs for a general understanding of the overall threat management process and the ability to make important decisions quickly and with limited information. In the absence of formal training, the reports, forms, templates, SOPs, and checklists that make up a set of RGs may be used as worksheets to practice potential scenarios.

4.8 Enhance Physical Security

Denying physical access to key sites within the water system may act as a deterrent to a perpetrator. Criminals often seek the easiest route of attack, just like a burglar prefers a house with an open window. Aside from deterring actual attacks, enhancing physical security has other benefits. For example, installation of fences and locks may reduce the rate of false alarms. Without surveillance equipment or locks, it may not be possible to determine whether a suspicious individual has actually entered a vulnerable area. The presence of a lock and a determination as to whether it has been cut or broken provides sound, although not definitive, evidence that an intrusion has occurred. Likewise, security cameras can be used to review security breaches and determine if the incident was simply due to trespassing or is a potential contamination threat. The costs of enhancing physical security may be justified by comparison to the cost of responding to just one 'credible' contamination threat involving site characterization and laboratory analysis for potential contaminants.

The correct choice of security enhancements varies by utility, and a number of resources are available to assist in this selection process. For instance, a vulnerability assessment (see Section 4.1.1) may provide a sound basis for making security upgrades. The American Water Works Association has developed a field guide (AWWA, 2002) to help meet security challenges. EPA has developed a series of Security Product Guides to assist treatment plant operators and utility managers in reducing risks from, and providing protection against, possible natural disasters and intentional terrorist attacks (http://www.epa.gov/safewater/security/guide/index.html).

4.9 Establish Baseline Monitoring Program

Background concentrations of suspected or tentatively identified contaminants may be extremely important in determining if a contamination incident has occurred. In some cases, and for some contaminants, background levels may be at detectable concentrations. **If unrecognized, these may be confused with an actual contamination incident.** Baseline occurrence information, discussed more thoroughly in Module 3, Section 3.5, is derived from monitoring data and is used to characterize typical levels of a particular contaminant or water quality parameter. Baseline data may be used for two purposes in the context of emergency water sampling:

- If general water quality parameters, such as pH, chlorine residual, or conductivity, among others, are used as indicators of possible contamination incidents, a baseline must be established such that significant deviations from the baseline can be observed.

- If a specific contaminant is detected in the water, knowledge of typical background levels may be necessary to properly interpret the results.

4.10 Utilize and Understand On-line Monitoring

On-line monitors are a topic of much interest, although there is a significant level of debate regarding their effectiveness as an early warning system (EWS). AWWARF has published a report discussing on-line monitoring for drinking water utilities (AWWARF, 2002), which outlines the cost-benefit analysis for online monitoring. Many of the costs and benefits are based on issues of general water quality, plant operations, and regulatory compliance. One definite benefit is early detection of changes in water quality parameters, such as pH, chlorine residual, and turbidity. Changes in these parameters relate to treatment plant operation, and may also indicate potential water contamination if properly interpreted. For instance, on-line monitoring may help establish typical background levels of the monitored parameters. These established background levels can then be compared with levels recorded during a suspected contamination incident. Another benefit of on-line monitoring for water security is that it can free operators from manual data collection, and facilitate analysis and interpretation of the data for routine as well as security purposes. Such information should be integrated into the information management plan (see Section 4.5).

In summary, the use of on-line monitors may serve to increase the quality of water in general, but there are unanswered questions regarding their applicability as EWSs. Currently, there are efforts underway within EPA and the water industry to attempt to resolve these issues and also to verify that commercially available on-line monitors perform as effectively as their manufacturers claim. Results of this work may be reported in later versions of the RPTB. The results of EPA efforts to verify monitoring technologies can be found at http://www.epa.gov/etv. Because of interest in on-line monitoring systems that are currently available, a discussion of the two main types, conventional systems and EWSs, is included in Appendix 6.2.

5 References and Resources

References and information cited or used to develop this module are listed below. The URLs of several sources are cited throughout the text. These URLs were correct at the time of the preparation of this document. If the document is no longer available at the URL provided, please search the sponsoring organization's Web site or the World Wide Web for alternate sources. A copy of referenced documents may also be provided on the CD version of this module, although readers should consult the referenced URL for the latest version.

AWWA. 2002. Water System Security: A Field Guide, American Water Works Association, Denver, CO.

AWWARF. 2002. Online monitoring for drinking water utilities. Editor, Erika Hargesheimer, AWWA Research Foundation and CRS PROAQUA, American Water Works Association, Denver, CO.

AWWARF. 2003. Actual and Threatened Security Events, AWWARF Project 2810, American Water Works Association, Denver, CO.
http://www.awwarf.org/research/TopicsAndProjects/projectSnapshot.aspx?pn=2810

DHS. 2003a. "Initial National Response Plan"
http://www.dhs.gov/interweb/assetlibrary/Initial_NRP_100903.pdf

FEMA. 2003a. "IS-195 Basic Incident Command System – EMI Independent Study Program"
http://training.fema.gov/EMIWeb/IS/is195.asp

FEMA. 2003b. "Independent Study Course List"
http://training.fema.gov/EMIWeb/IS/crslist.asp

FEMA. 2003c. "Federal Response Plan"
http://www.fema.gov/rrr/frp/

DOJ/NIJ. 2002. "Crisis Information Management Software (CIMS) Feature Comparison Report"
http://www.ncjrs.org/pdffiles1/nij/197065.pdf

WHO. 2001. "Health Aspects of Biological and Chemical Weapons"
http://www.who.int/emc/pdfs/BIOWEAPONS_FULL_TEXT2.pdf

U.S. EPA. 2002. "EPA Community Drinking Water Security Requirements"
http://www.epa.gov/safewater/security/community.html

U.S. EPA. 2003a. "The Safe Drinking Water Act"
http://www.epa.gov/safewater/sdwa/sdwa.html

U.S. EPA. 2003b. Model Emergency Response Plan, in preparation.

U.S. EPA. 2003c. "Large Water System Emergency Response Plan Outline: Guidance to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002"
http://www.epa.gov/ogwdw/security/pdfs/erp-long-outline.pdf

U.S. EPA. 2003d. "FORMS II Lite" http://www.epa.gov/superfund/programs/clp/f2lite.htm

U.S. EPA. 2003e. "Security Product Guides"
http://www.epa.gov/safewater/security/guide/index.html

U.S. EPA. 2003f. "Environmental Technology Verification (ETV) Program"
http://www.epa.gov/etv

International Life Sciences Institute Risk Science Institute. (ISLI). 1999. Early Warning Monitoring to Detect Hazardous Events in Water Supplies. ILSI PRESS, Washington, DC.
http://www.ilsi.org/file/EWM.pdf

NRT. 2000. "NRT Joint Information Center Model: Collaborative Communications During Emergency Response"
http://www.nrt.org/production/nrt/home.nsf/Resources/publications/$FILE/JIC.pdf

NRT. 2003. "National Response Team" (2003) http://www.nrt.org

WHO. 2003. "Public health response to biological and chemical weapons: WHO guidance, 2nd edition (Draft, May 2003)" http://www.who.int/csr/delibepidemics/biochemguide/en/index.html

6 Appendices

6.1 Sample Outline of Response Guideline

A Response Guideline is essentially a "field guide" for responding to contamination threats, and may be composed of appropriate figures, forms, templates, text, and checklists, which can be found in Modules 2 through 6. Expanding the outline below with the content from Modules 1-6 (as listed and/or linked within the outline) should result in an essentially complete response guideline. See the table of contents for the modules for exact locations.

EMERGENCY RESPONSE GUIDE OUTLINE

1. Overview of/Introduction to Response Guidelines (Module 1, Section 4.3)
2. Threat Warning Descriptions (Module 1, Section 2.2)
3. Initial Communication and Notifications (Module 1, Section 4.6)
4. Threat Evaluation
    a. Threat Warning Report Forms (Module 2, Appendix 8.3-8.8)
    b. Threat Evaluation Worksheets (Module 2, Appendix 8.2)
5. Site Characterization
    a. Site Characterization Plan Template (Module 3, Appendix 8.1)
    b. Field Testing Results Form (Module 3, Appendix 8.3)
    c. Site Characterization Report Form (Module 3, Appendix 8.2)
    d. Sample Documentation Form (Module 3, Appendix 8.4)
6. Planned Responses
    a. Response Planning Matrix (Module 2, Appendix 8.1)
    b. Action Plan (Module 2, Section 2.4)
    c. Guidelines for Contaminant Containment (Module 5, Section 4)
    d. Contaminant Identification (Module 4)
    e. Treatment, Removal And/or Disposal of Contaminant (Module 6, Section 6)
    f. Public Notification (Module 5, Section 5)
    g. Alternate Domestic Water (Module 6, Section 5)
    h. Fire Flow Supply (Module 6, Section 5)
    i. Expanded Communications (Module 1, Section 4.6)
7. Plan for Return of Water System to Service (Module 6, Section 8)
8. Appendixes
    a. Appendix I: Phone Directories for Notifications (Module 1, Section 4.6)
    b. Appendix II: Drinking Water Advisories (Module 5, Appendices 8.2 – 8.5)

6.2 U.S. Government Response Plans

6.2.1 National Response Plan

The U.S. Department of Homeland Security was tasked by the Homeland Security Presidential Directive 5 (HSPD-5) to develop, submit to the Homeland Security Council, and administer a National Response Plan (NRP). HSPD-5 required the development and publication of an Initial NRP (INRP), which was released on September 30, 2003. Pending the development of the full NRP, the INRP provides an interim implementation of the domestic incident management authorities, roles, and responsibilities of the Secretary of Homeland Security as defined in HSPD-5. It also provides interim guidance on Federal coordinating structures and processes for domestic incident management. The INRP is applicable to domestic incident management in the context of terrorist attacks, major disasters, and other emergencies. A final NRP will eventually replace the INRP. In the interim period, until the full NRP becomes effective, current Federal incident management and emergency response plans remain in effect, except as specifically modified by the INRP. The full text of the INRP is available at http://www.dhs.gov/interweb/assetlibrary/Initial_NRP_100903.pdf and a fact sheet is found at http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0278.xml

INRP represents a significant first step towards an overall goal of integrating the current family of Federal domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all-hazards plan. The INRP will be supported by the National Incident Management System (NIMS), a national system under development that creates standardized incident management processes, protocols, and procedures.

There are five current emergency response plans that are linked by the INRP:

- Federal Response Plan
- U.S. Government Interagency Domestic Terrorism Concept of Operations Plan
- Federal Radiological Emergency Response Plan
- Mass Migration Response Plans
- National Oil and Hazardous Substances Pollution Contingency Plan

Of these, perhaps the Federal Response Plan is most relevant to water contamination, and it is more completely described below in Appendix 6.2.2.

6.2.2 Federal Response Plan

The Federal Response Plan (FRP, http://www.fema.gov/rrr/frp/) provides the mechanism for federal departments and agencies to coordinate delivery of Federal assistance to State and local governments during a major disaster or emergency, including terrorist acts. The FRP supports implementation of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), as amended (42 U.S. Code 5121, et seq.), as well as individual agency statutory authorities. Under the Stafford Act, a State Governor may request the President to declare a major disaster or an emergency if an event is beyond the combined response capabilities of the

State and affected local governments. Only after the President makes a declaration is the FRP used.

As directed by Presidential Decision Directive (PDD)-39, U.S. Policy on Counter-terrorism, and as articulated in the FRP (FEMA, 2003c), the Department of Justice (DOJ) is designated as the lead federal agency for threats or acts of terrorism within U.S. territory. DOJ assigns lead responsibility for "crisis management" to the Federal Bureau of Investigation (FBI), who acts predominantly in a law enforcement capacity. Crisis management refers to the process by which resources needed to apprehend and prosecute perpetrators are identified, acquired and utilized. Within that process, the FBI operates as the on-scene manager for the Federal Government. It is FBI policy that crisis management will involve only those Federal agencies requested by the FBI to provide expert guidance and/or assistance, as described in the PDD-39 Domestic Deployment Guidelines (classified) and the FBI Weapons of Mass Destruction (WMD) Incident Contingency Plan.

FEMA, a branch of the Department of Homeland Security (DHS), supports the lead federal agency for "consequence management" throughout the Federal response, or serves as the lead federal agency when the Attorney General transfers the role to DHS. Consequence management refers to measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. It is DHS policy to use FRP (FEMA, 2003c) structures to coordinate all Federal assistance to State and local governments for consequence management.

The FRP provides more detailed guidance on the post-incident management and responsibilities of various federal departments and agencies (see Terrorism Incident Annex, Section V, FEMA 2003c). In summary, no single agency or organization at the Federal, State, local, or private-sector level possesses the authority and expertise to unilaterally implement remediation and recovery actions. If Federal assistance is provided under the authorities of the Stafford Act, responsibility for specific tasks will be delegated by the lead agency to those entities that possess the skills and resources required for implementing them. Key areas of responsibility that would potentially support water system remediation and recovery efforts are highlighted below:

DOJ/FBI. DOJ delegates the role of lead federal agency (LFA) to the FBI for operational response. The FBI responsibilities potentially supportive of remediation and recovery will include:

- Designating and establishing a Joint Operations Center (JOC) in the field;
- Appointing an FBI On-Scene Commander (OSC) who will convene and chair meetings of operational decision makers representing lead State and local agencies, DHS/FEMA, and other supporting Federal agencies (e.g., EPA);
- Working with DHS to establish and operate a Joint Information Center (JIC) in the field as a focal point for information to the public and media concerning Federal response;
- Issuing and tracking the status of crisis management actions assigned by the FBI; and
- Designating appropriate liaison and advisory personnel to support DHS.

DHS. DHS supports the overall LFA by operating as the lead agency for consequence management until the overall LFA role is transferred to DHS. DHS will:

- Work with the FBI to establish and operate a JIC in the field as the focal point for information to the public and the media concerning the Federal response to the emergency;
- Establish the primary Federal operations centers for consequence management in the field and Washington, DC;
- Appoint a Regional Support Team (RST) Director or Federal Coordinating Officer (FCO) to manage and coordinate the Federal consequence management response in support of State and local governments. In coordination with the FBI, the RST Director or FCO will convene meetings with decision makers to formulate incident action plans, define priorities, review status, resolve conflicts. These meetings may also be used to identify issues that require decisions from higher authorities, and evaluate the need for additional resources. Decision makers present at meetings may include Federal, State, and local emergency management and technical support agencies, as appropriate;
- Issue and track the status of consequence management actions assigned by DHS;
- Designate appropriate liaison and advisory personnel to support the FBI; and
- As needed, provide assets of the National Disaster Medical System and/or the Metropolitan Medical Response System.

HHS. As directed in PDD-39, the Department of Health and Human Services (HHS) will activate technical operations capabilities to support the Federal response to threats or acts of WMD terrorism. HHS may coordinate with individual agencies identified in the HHS Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological (C/B) Terrorism. Coordination efforts will use the structure, relationships, and capabilities described in the HHS plan to support response operations. Note that CDC, and thus the Laboratory Response Network (LRN), is part of HHS. If the HHS plan is implemented:

- The HHS on-scene representative will coordinate the HHS plan response with the DHS;
- The HHS plan response may include consultation, agent identification, epidemiological investigation, hazard detection and reduction, decontamination, public health support, medical support, and pharmaceutical support operations; and
- HHS will issue taskings that draw on funding from the responding HHS plan agencies.

EPA. As directed in PDD-39, the EPA will activate technical operations capabilities to support the Federal response to acts of WMD terrorism. EPA may coordinate with individual agencies identified in the National Oil and Hazardous Substances Pollution Contingency Plan (NCP)[1] to use the structure, relationships, and capabilities of the National Response System as described in the NCP [40 CFR Part 300 subpart B] to support response operations. If the NCP is implemented:

- The Hazardous Materials On-Scene Coordinator under the NCP will coordinate the NCP response with the DHS official (either the RST Director or the FCO), who is responsible under PDD-39 for on-scene coordination of all Federal support to State and local governments; and

[1] Agencies listed in the NCP include: USCG, FEMA, DOD, DOE, USDA, DOC, HHS, DOI, DOJ, DOL, DOT, DOS, NRC, and GSA.

- The NCP response may include threat assessment, consultation, agent identification, hazard detection and reduction, environmental monitoring, decontamination, and long-term site restoration (environmental cleanup) operations.

USACE. Under FRP Emergency Support Function (ESF) #3, Public Works and Engineering Annex, the U.S. Army Corps of Engineers (USACE) serves as the primary agency responsible, in part, for emergency restoration of critical public facilities. Activities can include the temporary restoration of water supplies and emergency contracting to support public health and safety, such as providing for potable water.

State and Local Authorities. State and local authorities maintain initial responsibility for managing domestic incidents. The Federal Government will assist State and local authorities when their resources are overwhelmed or when Federal interests are involved. In those cases, the local or state agencies (e.g., local health department) should work in partnership with the LFA.

Water Utility. The water utility will possess the most detailed first-hand knowledge and technical expertise regarding the configuration and operation of the water source, storage, treatment, and distribution systems. Accordingly, water utility personnel will serve as technical advisors to lead agency personnel responsible for system characterization, remediation, and recovery. If Federal assistance is provided under the authorities of the Stafford Act, responsibility for specific tasks most likely will be delegated to the water utility by DHS/FEMA or EPA (who will support long-term site restoration and environmental cleanup). In addition, the water utility can play a key role in planning for a remedial response to contamination, including evaluating containment options, and ensuring rapid site access and access to operating records, engineering drawings, etc., that may be required by response action personnel.

6.3 On-Line Monitoring Systems

6.3.1 Conventional systems

Conventional on-line monitoring systems are largely designed to measure typical water quality parameters in a near-real or real-time fashion. Examples of these parameters include: temperature, turbidity, particle counts, color, conductivity, total dissolved solids, alkalinity, pH, chlorine residual, specific UV absorbance, TOC, along with a host of inorganic and organic chemicals. In addition, water flow, level, and pressure may be automatically recorded. Many of these systems are designed to meet regulatory goals related to the reduction of turbidity, DBP formation, and other water quality parameters. These systems are often connected to a utility's SCADA and/or GIS system. The water quality parameters accessible through these systems may also have water security applications, specifically by providing a warning of a possible threat, as discussed in Section 2.2. However, interpretation of this data must be performed cautiously, as discussed in Module 2.

6.3.2 Early warning systems

The goal of an early warning system (EWS) is to identify a low probability/high impact contamination incident in a water system allowing sufficient time for an appropriate response that mitigates or eliminates any adverse impact resulting from the incident (ILSI, 1999). Typically, an EWS for water would be designed to detect the introduction of toxic or infectious contaminants that pose a risk to public health. According to the ILSI report, an ideal EWS would 1) be fully automated, 2) have a rapid response time and high sampling rate, 3) provide a specific and sensitive screen for a range of contaminants, 4) have a low occurrence of false positives and negative, 5) be reliable and rugged, 6) be easy to use, and 7) be affordable to install and operate. Although there are many on-line monitoring systems currently being discussed for use as EWSs, currently, an EWS with all of these features does not exist.

Among the technologies currently promoted as potential EWSs are toxicity monitors, which rely on a biological species as a sentinel for the presence of the contaminant. These range from large animals such as fish to various microbial species of algae. Another approach relies on conventional monitors, in which changes in conventional water quality parameters, such as temperature, chlorine residual, color, conductivity, and pH, are used discretely or in a multi-parameter analysis to infer the presence of a contaminant. Ideally, computerized data systems for these detectors may automatically report significant changes in these parameters. It is important to note, however, that the baseline of these parameters needs to be carefully understood, as well as the relationship between changes in the water quality parameters and the presence of specific contaminants.

Implementation of a poorly characterized monitoring technology will result in a false sense of security since there is no assurance that it is capable of meeting the monitoring objectives. In a worst-case scenario, implementation of a poorly characterized system could result in false alarms that undermine the effectiveness of a monitoring program and result in a needless expenditure of resources to follow up on the false positive result.

Before initiating an early warning monitoring program, the objectives of the program should be clearly defined, and a plan should be developed for the interpretation, use, and reporting of monitoring results. It is critical that this plan be developed before there is a need to monitor or respond to a threat warning and that the plan be developed in coordination with the water utility, local and state health departments, emergency response units, and local political leadership. The consequences of improper coordination among authorities or inappropriate responses to monitoring results can be severe. The key is to have these guidelines and procedures in place prior to deployment of the monitoring system.

As part of the monitoring plan, a hierarchy for dissemination of positive monitoring results should be developed, and this notification hierarchy should be consistent with the utility's overarching ERP. This hierarchy should be based on consideration of who needs the information to make public health decisions and at what time the information is needed. Initially, the results might need to be rapidly disseminated to the WUERM, utility management, emergency response personnel, and the State or local health department. These preliminary monitoring results might trigger various response actions, such as a threat evaluation, additional sampling and confirmatory analysis, and immediate operational response actions.

Another consideration is whether or not to communicate to the public information regarding monitoring efforts designed to counter terrorism. On one hand, public support may be necessary to secure funding for such a monitoring effort, and this may bolster public confidence in the water supply. Also, it could be argued that monitoring could serve as a deterrent to potential criminal or terrorist activities. However, the counter argument is that publicizing a monitoring system, or other security measures, may be viewed as a challenge to terrorists and may increase the likelihood of threats, hoaxes, or attacks. Furthermore, it may provide enough information to allow a criminal entity to determine which contaminants are being monitored and to simply use a contaminant that cannot be detected in an attack on a water supply. It has been suggested that efforts taken to counter terrorism and improve security be put into a context of general preparedness for a variety of incidents or emergencies (ILSIRI, 1999). This will allow a utility to communicate efforts that are being taken to ensure continued operation and the safety of the water supply without focusing on any one specific threat, such as intentional contamination through terrorist activity.

Office of Ground Water and Drinking Water
Water Security Division
EPA 817-D-03-001
www.epa.gov/safewater/security
December 2003

Recycled/Recyclable • Printed with Vegetable Oil Based Inks on
100% Postconsumer, Process Chlorine Free Recycled Paper