

Security and Emergency Planning

for Water and Wastewater Utilities

Stanley States, PhD



American Water Works
Association

The Authoritative Resource on Safe Water®

Advocacy
Communications
Conferences
Education and Training
Science and Technology
Sections

Security and Emergency Planning

for Water and Wastewater Utilities

Stanley States, PhD

Security and Emergency Planning

for Water and Wastewater Utilities

Stanley States, PhD



**American Water Works
Association**

Security and Emergency Planning for Water and Wastewater Utilities
Copyright © 2010 American Water Works Association

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information or retrieval system, except in the form of brief excerpts or quotations for review purposes, without the written permission of the publisher.

Disclaimer

This handbook is provided for informational purposes only, with the understanding that the publisher, editors, and authors are not thereby engaged in rendering engineering or other professional services. The authors, editors, and publisher make no claim as to the accuracy of the handbook's contents, or their applicability to any particular circumstance. The editors, authors, and publisher accept no liability to any person for the information or advice provided in this book or for loss or damages incurred by any person as a result of reliance on its contents. The reader is urged to consult with an appropriate licensed professional before taking any action or making any interpretation that is within the realm of a licensed professional practice.

AWWA Publications Manager/Technical Editor: Gay Porter De Nileon
Production Editor: Cheryl Armstrong

Library of Congress Cataloging-in-Publication Data

States, Stanley.

Security and emergency planning for water and wastewater utilities / Stanley States.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-58321-745-0

1. Waterworks--Security measures. 2. Water utilities--Security measures. I. Title.

TD487.5.S73 2010

363.325'96281--dc22

2009038653

ISBN 1-58321-745-2
9781583217450



6666 West Quincy Avenue
Denver, CO 80235-3098
303.794.7711
www.awwa.org

CONTENTS

PREFACE ix

CHAPTER 1

TERRORISM 1

| | |
|--|----|
| Terrorism in General | 2 |
| Definition of Terrorism | 3 |
| Why Choose Terrorism | 4 |
| Goals of Terrorists | 5 |
| Selection of Targets and Timing of Attacks | 6 |
| Perpetrators | 7 |
| Weapons of Mass Destruction | 11 |
| Islamic Fundamentalism | 12 |
| References | 16 |

CHAPTER 2

THE THREAT TO DRINKING WATER SYSTEMS 17

| | |
|---|----|
| Why Drinking Water Systems Could Be a Target | 19 |
| Scenarios of Concern | 20 |
| Potential Sites for Contamination | 25 |
| Contaminants | 31 |
| What Has Already Occurred at Drinking Water Utilities | 42 |
| References | 48 |

CHAPTER 3

THE THREAT TO WASTEWATER SYSTEMS 53

| | |
|--|----|
| Why Wastewater Systems Might Be Targeted | 53 |
| Scenarios of Concern | 54 |
| Contamination Endpoints of Concern | 56 |
| Documented Incidents in Wastewater Systems | 56 |
| Conclusions | 61 |
| References | 61 |

CHAPTER 4

LEGISLATIVE AND REGULATORY ASPECTS OF WATER SECURITY AND EMERGENCY PREPAREDNESS 63

| | |
|---|----|
| Homeland Security Presidential Directives | 67 |
| Conclusions | 71 |
| References | 72 |

CHAPTER 5

THE WATER SECTOR-SPECIFIC PLAN AND ACTIVE AND EFFECTIVE SECURITY PROGRAMS 73

| | |
|--|----|
| Sector-Specific Plans | 73 |
| Ten Features of Active and Effective Security Programs | 75 |
| Security Performance Measurement | 77 |
| Conclusions | 78 |
| References | 78 |

CHAPTER 6

REPORTS AND TOOLS TO IMPROVE SECURITY AND EMERGENCY PREPAREDNESS 79

| | |
|---|----|
| Baseline Threat Documents | 79 |
| USEPA Water Security Web Site | 80 |
| Security Product Guide | 80 |
| National Homeland Security Research Center | 81 |
| Response Protocol Toolboxes | 81 |
| Environmental Laboratory Compendium | 82 |
| ERP Guidelines | 82 |
| Security Research Plans and Homeland Security Strategy | 82 |
| Government Accountability Office (GAO) Reports | 83 |
| Environmental Technology Verification and Technology Testing and Evaluation Programs | 83 |
| Threat Ensemble Vulnerability Assessment | 84 |
| USEPA Water Security Division | 85 |
| Water Security Initiative (WSI) | 85 |
| Hydraulic Models | 86 |
| Water Contaminant Information Tool (WCIT) | 87 |
| FBI InfraGard Program | 88 |
| Water Information Sharing and Analysis Center | 88 |
| Threat-Based Security Guidelines | 89 |
| Conclusions | 90 |
| References | 90 |

CHAPTER 7

VULNERABILITY ASSESSMENT 91

| | |
|--|----|
| Vulnerability Assessments (VAs) | 92 |
| Risk Assessment Methodology for Water | 93 |
| Vulnerability Self-Assessment Tool (VSAT) | 95 |
| Protection of Sensitive Information | 97 |
| Risk Analysis Management for Critical Asset Protection | 98 |
| References | 98 |

CHAPTER 8

MITIGATION OF RISK THROUGH PHYSICAL PROTECTION SYSTEMS 99

| | |
|-----------------------------------|-----|
| Physical Protection Systems (PPS) | 101 |
| External Asset Protection | 112 |
| Security Guards and Patrols | 114 |
| Conclusions | 115 |
| References | 116 |

CHAPTER 9

MITIGATION OF RISK THROUGH OPERATIONAL MEASURES 117

| | |
|------------------------------------|-----|
| System Redundancy and Backups | 117 |
| Chemical Treatment Countermeasures | 120 |
| Backflow-Prevention Program | 122 |
| System Plans and Modeling | 122 |
| References | 123 |

CHAPTER 10

MITIGATION OF RISK THROUGH POLICIES, PROCEDURES, AND TRAINING 125

| | |
|---|-----|
| Release of Sensitive Information | 125 |
| Records Management | 126 |
| Crisis Management Human Resources Program | 127 |
| Community Awareness of Security | 129 |
| Public Access to Reservoirs | 130 |
| Controlled Access to Key Facilities | 131 |
| Security Training | 132 |
| Key Security | 132 |
| Emergency Notifications | 133 |
| Deliveries | 133 |
| Emergency Contracts | 134 |
| Mutual Aid Agreements | 134 |
| References | 135 |

CHAPTER 11

MITIGATION OF RISK THROUGH CYBER MEASURES 137

| | |
|-------------------------------------|-----|
| VAs for Cyber Systems | 140 |
| Recommendations for Risk Reduction | 140 |
| Roadmap to Security Control Systems | 143 |
| Conclusions | 144 |
| References | 144 |

CHAPTER 12

CONTAMINATION WARNING SYSTEMS 147

| | |
|---|-----|
| Approaches for Online Monitoring | 148 |
| Conclusions Concerning Continuous Monitoring Technology | 165 |
| Placement of Sensors | 165 |
| Integrated Contaminant Warning Systems | 167 |
| Hydraulic Models | 168 |
| Automatic Sample Archiving | 168 |
| Tiered Approach to Monitoring | 169 |
| Comprehensive CWS | 169 |
| USEPA Water Security Initiative | 170 |
| Cities Developing a CWS | 171 |
| Additional Resources | 171 |
| References | 172 |

CHAPTER 13

RESPONSE TO INCIDENTS AND THREATS 175

| | |
|--|-----|
| Emergency Response Plans (ERPs) | 176 |
| Emergency Notifications | 178 |
| Emergency Operational Response | 181 |
| Role of Utility Personnel in Responding to Emergencies | 182 |
| USEPA Response Protocol Toolboxes | 183 |
| References | 187 |

CHAPTER 14

EMERGENCY MANAGEMENT OF DRINKING WATER AND WASTEWATER INCIDENTS 189

| | |
|--|-----|
| National Incident Management System | 190 |
| National Response Plan and National Response Framework | 190 |
| Incident Command System (ICS) | 192 |
| Emergency Operations Center | 195 |
| Departmental Operations Center | 197 |
| Conclusions | 197 |
| References | 198 |

CHAPTER 15

ANALYTICAL RESPONSE TO WATER CONTAMINATION THREATS 199

| | |
|--|-----|
| Field Safety Screening | 200 |
| Rapid Field Testing of Water | 201 |
| Sample Concentration in the Field | 211 |
| Sample Collection | 214 |
| Definitive Laboratory Analysis | 214 |
| California Mutual Aid Laboratory Network | 216 |
| CDC Laboratory Response Network | 216 |
| USEPA Environmental Laboratory Networks | 217 |
| Commercial Laboratories | 218 |
| Mobile Laboratories | 219 |
| Water Contaminant Information Tool | 219 |
| USEPA Laboratory Compendium | 219 |
| Standardized Analytical Methods | 220 |
| NEMI–CBR | 220 |
| References | 221 |

CHAPTER 16

EMERGENCY COMMUNICATIONS WITH THE PUBLIC 223

| | |
|---|-----|
| Crisis Communications Overview | 224 |
| Dealing With the Media | 225 |
| Advice From Crisis Communications Specialists | 228 |
| Crisis Communication Plan | 229 |
| Message Mapping | 230 |
| Public Notification | 231 |
| National Communications System | 233 |
| Conclusions | 234 |
| References | 235 |

CHAPTER 17

EMERGENCY RESPONSE TRAINING 237

| | |
|---|-----|
| Exercises | 237 |
| Pre-Exercise Training | 239 |
| Conducting the Exercise | 240 |
| Additional Training During the Exercise | 242 |
| Hot Wash | 242 |
| Guidance Materials | 243 |
| References | 243 |

CHAPTER 18

REMEDIATION AND RECOVERY 245

| | |
|--|-----|
| Decontamination of Water Systems | 245 |
| Decontamination of Infrastructure | 247 |
| Decontamination Procedures | 249 |
| Remediation and Recovery Research | 251 |
| Decontamination of Wastewater Systems | 252 |
| Mutual Aid Among Utilities | 254 |
| Remediation Case Study | 255 |
| Alternate Water Supplies and Sanitary Services | 256 |
| USEPA Remediation and Recovery Guidance | 257 |
| Government Assistance | 258 |
| Business Continuity Plans (BCP) | 259 |
| References | 260 |

CHAPTER 19

PANDEMIC FLU 261

| | |
|---|-----|
| Background | 261 |
| Effects of Pandemics on Water Utilities | 265 |
| Preparing for, Responding to, and Recovering From a Pandemic | 266 |
| Infection Control in the Workplace | 268 |
| Influenza Transmission Via Water | 268 |
| Additional Information | 270 |
| References | 271 |

CHAPTER 20

CONCLUSIONS 273

LIST OF ABBREVIATIONS/ACRONYMS 275

ABOUT THE AUTHOR 281

INDEX 283



PREFACE

On Tuesday morning Sept. 11, 2001, I was working in my laboratory at the Pittsburgh Water and Sewer Authority. We were analyzing river and finished water samples for the presence of *Giardia* cysts and *Cryptosporidium* oocysts using the US Environmental Protection Agency (USEPA) method 1623 microscopic technique. Just as in the rest of the northeastern portion of the country, it was, ironically, a beautiful late summer morning in Pittsburgh. Once we started receiving the news of events that were unfolding in New York, Washington D.C., and Shanksville, Pa.—located roughly 70 miles from Pittsburgh—our activities in the Water Quality Section quickly shifted to ensuring that the safety of our city's drinking water was intact.

For the next several days we collected numerous water samples from our distribution system and conducted a variety of analyses to ensure that there were no signs of significant change. At some point during the afternoon of September 11, someone at the treatment plant suggested that in light of the day's events we might want to consider locking the front door to the plant and securing the front gate. Prior to that day, this was never considered necessary when the daytime staff was manning the plant. As a result of the terrible events of that day, it became apparent to many of us at the utility that our daily concerns and operations would be somewhat different in the future.

Since 1973, the American Water Works Association (AWWA) has published several editions of Manual M19, *Emergency Planning for Water Utilities*. The purpose of the manual has been to help drinking water managers and operators prepare their utilities to protect against, and respond to, a variety of emergencies ranging from natural disasters to manmade emergencies. Traditionally, the emphasis of M19 has been on natural events. The fourth edition of M19 was published and released in 2001 (AWWA 2001), shortly before the terrorist attacks.

Following the attacks, with a pressing need to provide additional information on preparation for, and response to, malevolent acts directed toward public water supplies, AWWA quickly produced a supplement to the manual entitled *Security Analysis and Response for Water Utilities* (Burns et al. 2001). This 20-page supplement provided information on vulnerability assessment, mitigation of risk, response planning, and crisis communications to address the new fears concerning terrorism. In 2002, AWWA expanded this guidance with the publication of a more comprehensive document entitled *Water System Security: A Field Guide* (Bernosky 2002), which was a comprehensive update of the manual supplement. Since that time, a great deal of work has been done to improve the ability of water operators to deal with the contingency of malevolent acts directed toward public water systems. A large amount of research has been conducted on the topic of homeland security for the drinking water and wastewater infrastructure, and a number of articles and guidance documents have been published. Following the hurricanes of 2005 that devastated the city of New Orleans and portions of several coastal states, the emphasis on utility security against manmade events was broadened to an all-hazards approach that includes preparedness against the whole gamut of natural disasters and accidents as well as intentional events.

This book is intended to be a compilation of the developments during the past eight years. The goal is to provide a practical reference document for use by both drinking water and wastewater managers and operators in dealing with homeland security and general emergency preparedness issues at their facilities. While some time has passed since 9/11, concern about intentional and unintentional emergencies at water utilities remains relatively high as demonstrated by recent national (AWWA Water Security Congress 2009) and international (World Water Organization High-Level Symposium on Water Security at the United Nations 2009) conferences held on these topics.

As the author of this handbook, I feel comfortable addressing this topic with water industry personnel because I have been the water quality manager for the Pittsburgh Water and Sewer Authority for the past 33 years. In that capacity, I deal on a practical level, 365 days per year, with water quality and analysis, treatment, and regulatory issues. Since 9/11, my duties have included security issues at my utility. I have been very involved during the past eight years with applied research on development of security-related rapid analytical techniques and online monitoring capabilities for drinking water and wastewater systems. Additionally, since 9/11 I have served on a number of security committees for government agencies, including USEPA, Department of Homeland Security (DHS), and the US Army, as well as industry associations including AWWA and the Water Environment Federation (WEF). I have also written and delivered a series of courses on homeland security to audiences throughout the United States and overseas. The sponsors of these webcasts, workshops, and tabletop exercises have included

the US Justice Department, DHS, USEPA, the Centers for Disease Control and Prevention, US Army, AWWA, and WEF. Much of this work has been conducted under contract with Texas A&M University's Texas Engineering Extension Service and the National Emergency Response and Rescue Training Center.

Through these courses I have had the pleasure of meeting and working with several thousand drinking water and wastewater utility personnel, as well as representatives from agencies that work with utilities to protect the nation's infrastructure. These have included elected officials, health department personnel, federal and state regulatory agency personnel, emergency responders, consultants, and law enforcement personnel including local and state police, as well as the FBI and US Secret Service. I have learned a great deal from my contact with all of these dedicated individuals, and much of what appears in this handbook was derived from my interaction with them.

A consideration in writing a handbook such as this is the sensitivity of the topic. There is certainly no classified information discussed in this text. However, the reality is that in addition to preparation and response to natural disasters and accidents, the subject matter deals with protection against intentional actions directed against public water systems with the intent of inflicting harm on people and damage to infrastructure and private property. There is always the concern that publication of homeland security information could provide ideas for individuals or groups with malevolent intent. The concern must be delicately balanced against the need to provide necessary information to utility personnel and others who must be aware of the plausibility of various threats.

This dilemma has been acknowledged by authors of other works of this nature such as Falkenrath and colleagues in their 1998 report on nuclear, biological, and chemical terrorism; the National Research Council in its 2002 report on the role of technology in countering terrorism (NRC, 2002); and Pontius (2003) in his chapter on water system security. Therefore, I have made a conscious effort to avoid detailed discussion of certain vulnerabilities, scenarios, and contaminants that might provide otherwise difficult-to-obtain details to those who don't have a legitimate need for the information. Unfortunately, a great deal of sensitive information is already available and fairly easy to find on the Internet and in the open literature for individuals with some technical background in this area.

Because this is probably the only book that I will ever write, I hope that it serves a useful purpose in helping to guarantee the safe delivery of drinking water and wastewater services to our customers. It is my hope that preparing for homeland security contingencies in our industry may help to ensure that we never have to respond to a real event. It is also hoped that preparations for intentional malevolent acts will help utilities deal with more likely accidental situations and natural disasters.

I would like to dedicate this book to my wife Kathleen, and my three sons: Tom, Mike, and Joe.

Stanley States
July 2009

References

- American Water Works Association (AWWA). 2001. *Emergency Planning for Water Utilities*. Manual of Water Supply Practices—M19, 4th ed. Denver, Colo.: AWWA.
- AWWA Water Security Congress. 2009. Washington D.C.: AWWA.
- Bernosky, J. 2002. *Water System Security: A Field Guide*. Denver, Colo.: AWWA.
- Burns, N.L., C.A. Cooper, D.A. Dobbins, J.C. Edwards, and L.K. Lampe. 2001. *Security Analysis and Response for Water Utilities*. Denver, Colo.: AWWA.
- Falkenrath, R.A., R.D. Newman, and B.A. Thayer. 1998. *America's Achilles Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*. Cambridge, Mass.: MIT Press.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington D.C.: National Academies Press.
- Pontius, F.W. 2003. *Drinking Water Regulations and Health*. New York: Wiley & Sons, Inc.
- World Water Organization High-Level Symposium on Water Security at the United Nations. 2009. New York City, February 4–6.

TERRORISM

For most Americans, Sept. 11, 2001, signaled the beginning of terrorism as an issue of concern for this country. However, terrorism is not a new phenomenon. Its roots extend back in history at least 2,000 years, although the frequency of incidents, scope of activity, and overall ferocity have increased in recent years. Undoubtedly, a variety of factors contribute to the elevation in terrorist activity, including the intensification of ethnic conflict and religious radicalism, the end of the cold war and breakup of the former Soviet Union, and the opening of borders and increase in commercial exchange that have made it easier for terrorists to move about and acquire more dangerous weapons. Paradoxically, democratization, globalization, and the explosion of computer technology have also contributed to the recent upsurge in terrorist activity. Regardless of contributing factors, the conventional wisdom is that terrorism is a global problem that will probably not be eliminated in the foreseeable future.

The United States is no stranger to terrorism (Hewitt 2003). Since 1950, more than 3,000 terrorist attacks have occurred in this country, resulting in several thousand terrorism-related fatalities. These range from the Ku Klux Klan's campaign of terror against the civil rights movement, to attacks by neo-Nazi and militia groups, and finally to the actions of al-Qaida.

Prior to 9/11, malevolent acts directed toward public drinking water supplies and wastewater systems were of little concern. Most, but not all, incidents were simple acts of vandalism. However, with the changing national and international climate and the possibility of drinking water or wastewater systems being selected as a target for terrorism, the water industry is now expected—by customers, government, and a sense of professional responsibility—to devote some attention and resources to protecting water systems against this possibility.

While detailed coverage of terrorism and the current domestic and international situation is not within the realm of this book, some discussion of the phenomenon of terrorism may be helpful to industry policymakers and utility managers who must make decisions concerning the allocation of resources for protection of public water systems.

Consequently, this chapter consists of a general discussion of the threat of terrorism to all facets of society. Chapters 2 and 3 will then focus specifically on the threat of malevolent acts directed toward drinking water and wastewater systems.

TERRORISM IN GENERAL

"Part of the difficulty in improving awareness of the terrorist threat is that much of the earlier violence had occurred elsewhere and had not been aimed directly at Americans. Over the decades of the 1980s and 1990s only 871 Americans died in the thousands of terrorist incidents that were recorded. Roughly 20 percent of those victims perished in a single incident, a purely home-grown plot in which an American blew up the Alfred P. Murrah Federal Building in Oklahoma City on April 10, 1995. The vast majority of deaths caused by terrorists have been foreign citizens in their own lands. Averaging the number of Americans killed in terrorist attacks over the number of years of data, typical formulations have it that a chicken bone stuck in the throat is deadlier, or that one has a higher probability of being struck twice by lightning. Americans did not focus on this issue until the tragedy of September 11 brought the terrorism question home to so many so personally."

—From John Prados's book, *America Confronts Terrorism* (2002)

At the beginning of a new century in which the United States finds itself as the world's superpower, one would expect that, unlike earlier periods of active warfare and cold war that this country has lived through, security could now be taken for granted. However, as the bombings of the World Trade Center in 1993 and the Alfred P. Murrah Federal Building in 1995, the airplane assaults on the World Trade Center and Pentagon in 2001, and the anthrax mail attacks in 2001 dramatically indicated, we have entered a new era of security concerns. Differences of opinion between the United States and certain domestic groups and individuals, international groups, and foreign states still exist. However, the unrivaled power of the United States has forced weaker adversaries to use unconventional, asymmetrical methods such as terrorism to confront this country. Through terrorism, relatively small groups and nations can attempt to influence the political and social attitudes and policies of a large country or society.

While the United States had experienced some domestic terrorism in the past, the number of incidents was relatively low compared with the number of terrorist incidents in many other nations. This trend changed in the 1990s. The frequency and lethality of attacks on the United States and its interests by transnational groups, both in this country and overseas, increased. Domestic extremist groups grew in number and activity. And, the potential for the use of weapons of mass destruction also appeared to increase.

DEFINITION OF TERRORISM

The phenomenon of terrorism is difficult to define partially because of differences in the perspectives of individuals observing an act, and partially because the nature and character of terrorist acts are not static. The US Justice Department defines terrorism in the following way:

“Terrorism is the unlawful use of force or violence, or threatened use of force or violence, against persons and places for the purpose of intimidating and/or coercing a government, its citizens or any segment thereof for political or social goals.” (28 Code of Federal Regulations Section 0.85)

The definition used by the US State Department is similar:

“Terrorism is premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national or clandestine agents usually intended to impress an audience.”

The perpetrator’s motive is a key factor in determining whether an act constitutes terrorism. Is the incident intimidating or coercing (i.e., does it feature a threat or demand)? Does the incident address political or social goals (i.e., is a larger agenda involved)? While all acts of terrorism are criminal, all criminal acts are certainly not terrorism.

Recent terrorist acts in the United States have resulted in the passage of laws that further complicate the determination of whether a particular criminal act is actually terrorism. Generally, crimes that involve the use of a weapon of mass destruction (WMD) have been investigated, at least initially, as terrorism. Whether federal terrorism charges are actually brought against the defendant(s) usually depends on an interpretation of the perpetrator’s intent or motive, as well as consideration of the target itself. While use of a WMD should alert responders to the possibility of a terrorist act, the mere use of such a weapon doesn’t necessarily constitute terrorism.

Additionally, the perspective of the observer plays a role in the public’s interpretation of the terrorist nature of an incident or a figure. For example, an individual’s perception of George Washington as either a freedom fighter or a terrorist was probably influenced by the side of the Atlantic Ocean a person was living on in the late 1700s.

A distinction between a terrorist act and a similar crime or act of war is that terrorist acts deliberately target innocent third parties in an effort

to coerce the opposing group into some desired political or social course of action. Victims are chosen not because of personal guilt, or membership in an opposing military or governmental organization, but rather because their injuries or deaths will so shock the opposition that a concession will be forced (Combs and Slann 2003).

WHY CHOOSE TERRORISM

The ultimate reason why a group or individual would choose terrorism as a tactic is because sometimes it works. For example, during the final years of the British Empire in the 20th century, England faced terrorist movements in several of its Middle Eastern dependencies. The Greeks in Cyprus, the Jews in Palestine, and the Arabs in Aden, acting from nationalist motives, used attacks on military installations, and even on administrative installations and personnel, to persuade the imperial power that staying in the region was not worth the cost in blood. All three movements were successful. The US government quickly withdrew its troops from Beirut, Lebanon in 1983 after the suicide truck bombing of the US Marine headquarters killed 241 Marines, and again withdrew troops from Somalia following the atrocities carried out against US troops there in 1993.

In recent years, most countries have become more steadfast in refusing to accede to terrorists' demands, in large part to eliminate success as a motivation for terrorism. However, even a concerted effort on the part of government cannot guarantee that terrorism will not still be successful. In Spring 2004, bombs on four commuter trains in Madrid killed 191 people and injured another 1,400. The attack was widely believed to have changed the outcome of the national election held several days later. Al-Qaida may have struck Spain in an effort to turn popular support against the conservative government that backed the war in Iraq and was up for re-election.

While these incidents demonstrate that terrorist acts have occasionally produced the results sought by the perpetrators, most experts agree that terrorism is usually a failure (Hewitt 2003). Even the September 11 attacks have hardly influenced the basic American socioeconomic system, political system, or key policies such as support for Israel. It may be argued that the subsequent invasions and occupations of Afghanistan and Iraq were results quite contrary to the intentions of the terrorists.

Terrorism is also chosen because it is a feasible approach for asymmetric conflicts in which small entities confront much stronger entities. It would be foolhardy for a small nation or special interest group to directly attack a superpower. However, through terrorism, David can take a stand against Goliath.

Additionally, terrorism is an attractive option because it can be cost effective and can be carried out using a wide variety of technical approaches. Historically, terrorism has been shown to produce results with a relatively small commitment of resources, especially compared with head-on confrontation.

And, terrorists can use a wide variety of weapons, ranging from crudely manufactured explosives and incendiary devices to sophisticated, bioengineered, drug-resistant pathogens.

Terrorism also offers the advantage that the act can be deniable. A perpetrator can maintain anonymity by making sure that he is far away from the scene by the time an infectious agent with an extended incubation period begins to produce clinical symptoms. A classic example is the individual who laced several letters with anthrax spores in 2001 and mailed them to US government officials and media figures. It took seven years for the Federal Bureau of Investigations to finally gather enough evidence to identify Bruce Ivins, a longtime government researcher at the US Army's Ft. Detrick Pathogen Lab, as the likely culprit in this series of fatal attacks (Shane 2009). The suspect committed suicide before he could be tried for the crime.

GOALS OF TERRORISTS

While there are nearly as many ideologies as there are extremist groups worldwide, most terrorists can be broadly characterized as being motivated by ideologies falling into one of the following categories: religious, political, social, environmental, single issue, or special interest.

Terrorist attacks can achieve a number of goals. As explained by historian Bernard Lewis (2003), thanks to the rapid development of the media, the more recent forms of terrorism are aimed not at specific and limited enemy objectives but at public opinion. Terrorism's primary purpose is not to defeat or even to weaken the enemy militarily, but to gain publicity and inspire fear—a psychological victory.

This kind of terrorism has been practiced by a number of European groups, notably in Germany, Italy, Spain, and Ireland. Among the most successful and enduring terrorist organizations has been the Palestine Liberation Organization (PLO). According to the former director general of M15, the British Security Service, al-Qaida itself claims that 50 percent of its war is conducted through the media (Manningham-Buller 2006). In Iraq, attacks have been videoed and the footage downloaded onto the Internet within 30 minutes following an incident. Virtual media teams then edit the result, translate it into English and many other languages, and package it for a worldwide audience.

Terrorist acts can also be used to make a political statement and attract notoriety for a cause. The events of Sept. 11, 2001, completely captured the attention of the United States and were a major news item throughout the world.

A terrorist attack can produce large numbers of casualties among either a select group (government officials, members of a particular racial or ethnic segment) or random casualties. It is amazing that the attack on the World Trade Center on a business day morning did not produce more than 3,000 fatalities. However, it should be noted that effective terrorism does

not necessarily require large numbers of casualties. The mailborne anthrax attacks in 2001 effectively terrorized the United States while resulting in only five deaths and a small number of illnesses.

A successful terrorist attack can also negatively impact federal, state, and local governments. The attacks of 9/11, and subsequent threats and alerts, have diverted huge amounts of government resources toward public protection. The attacks also resulted in the most significant restructuring of the US federal government in decades, with the establishment of the Department of Homeland Security (DHS).

Still another goal of terrorism can be to create widespread economic loss and undermine the economic well being of a nation. The events of 9/11 had a devastating effect on the US airline industry and stock market, and have been blamed by some analysts for much of the national economic malaise experienced in the United States during the years following the attacks.

Similarly, a terrorist act or threat can be designed to coerce a specific decision or action from government leaders, such as the release of political prisoners. A terrorist group may also carry out an attack in retaliation for an action carried out by the target nation or group.

Finally, a terrorism goal can be to demonstrate to followers how strong a particular movement is, and how helpless society is to defend itself against it. A successful incident can produce a lack of confidence and a sense of insecurity among the citizens at large. This can create a feeling of distrust toward the government and its ability to protect the population. An effective act, or series of acts, can cause people to disrupt their normal activities and way of life and ultimately encourage them to persuade their government to change its policies.

SELECTION OF TARGETS AND TIMING OF ATTACKS

Obviously, targets of terrorist acts are often selected based on their symbolic importance. The World Trade Center was chosen as a target in 1993 and again in 2001 because it was the symbol of American capitalism and economic success. The Pentagon was attacked on Sept. 11, 2001, because it represents the centerpiece of U.S. military might. The fourth plane in the 9/11 attacks, brought down by the passengers over Shanksville, Pa., is believed to have been headed for the White House or Capitol Building in Washington D.C., principal symbols of US political power.

Similarly, attacks are sometimes timed for symbolic significance. Apr. 19, 1993 was selected by Timothy McVeigh as the date for the truck bombing of the federal building in Oklahoma City because it coincided with the second anniversary of the FBI storming of the Branch Davidian Compound in Waco, Texas.

PERPETRATORS

While terrorists certainly comprise a diverse set of people, with a variety of motivations and causes, attempts have been made to construct a general profile of individuals that have been associated with past acts. In his studies of domestic and foreign terrorists, sociologist Christopher Hewitt (2003) has observed that most terrorists are between 18 and 30 years of age, with few older than 50. Additionally, many do not come from poor backgrounds or suffer from some form of socioeconomic disadvantage. For example, the revolutionary, left-wing Weathermen in the 1960s consisted of political activists from privileged backgrounds. Most of the 19 perpetrators of the 9/11 attacks came from middle-class backgrounds. Khalid Sheikh Mohammed, who planned 9/11 and other attacks, has a degree in mechanical engineering. Osama bin Laden was well educated and raised in an extremely wealthy family. The terrorist cell that attempted several highly publicized car bombings in London and Scotland in the summer of 2007 included a neurosurgeon and several other practicing physicians (Cowell and Bonner 2007).

In contrast to popular belief, most terrorists do not suffer from psychiatric or personality disorders, nor do they exhibit abnormal social characteristics. Rather, they are often intelligent, adjusted individuals with extreme dedication to a cause. Conversely, the “lone wolf” terrorist category, individuals acting out on their own, often includes individuals who are more likely to be mentally unstable than would typically be found in terrorist groups. In fact, it can be argued that lone wolves pose a particular danger because their actions are not moderated or held in check by other, possibly more rational, members of extremist organizations. The alleged lone perpetrator of the 2001 mailborne anthrax attacks, Bruce Ivins, had battled mental health problems for years and had told a therapist that he had experienced homicidal thoughts as far back as graduate school.

A variety of types of terrorist groups and individuals have been responsible for documented incidents in the past. The following classification is one approach to describing them.

State Terrorism consists of governments that have employed terrorist-type tactics, such as kidnapping, torture, and murder, against their internal opponents. The most devastating state terror has occurred when an ideological fraction acquires absolute power and targets its political enemies for extermination, or in the case of racial or nationalistic differences, ethnic cleansing. Notorious examples during the last half-century include the Chinese Cultural Revolution under Mao Tse-tung and the regime of Cambodian dictator Pol Pot.

State-Sponsored Terrorist Groups are the terrorist organizations with the greatest financial and technological resources. Consequently, the use of certain chemical, biological, and nuclear weapons of mass destruction are limited to these groups because of the significant resources required for their development. Interestingly, to date no case is publicly known of a state assisting a terrorist organization in acquiring nuclear, biological, or chemical

weapons, perhaps because of the great risks assumed by a sponsor arming a potentially unreliable, uncontrollable group (Falkenrath et al. 1998).

The motivation for nations in sponsoring or supporting terrorist groups has traditionally been to use force or violence as an instrument of foreign policy. Such terrorism is used to produce fear and confusion within target countries. It is designed to demonstrate vulnerabilities in opposing governments for the purpose of making the adversaries more willing to cooperate. For example, some nations in the Middle East have sponsored Palestinian groups and individuals engaged in terrorist acts as a less risky approach to redressing Palestinian grievances—less risky than provoking another war with Israel.

Terrorist acts that can be clearly attributed to a specific government are easier for a nation as powerful as the United States to respond to than those perpetrated by small clandestine organizations. In April 1986, the United States launched an air attack against two Libyan cities in retaliation for that nation's involvement in the bombing of a West German disco in which two US servicemen were killed. Many observers, both American and Libyan, believe that Libyan leader Mu'ammar Qadhafi himself was a target in this retaliatory response. Consequently, terrorism directly sponsored by Libya and other foreign states has diminished during the past two decades. The US State Department has identified a number of countries that have sponsored terrorism, including Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. Most states that remain designated by the US State Department as sponsors of terrorism now only offer safe haven to terrorist groups rather than training, weapons, or logistical support (Combs and Slann 2003).

International (Transnational) Terrorist Groups have become increasingly active over the past several decades. These include, among others: al-Qaida (the foundation), Hamas (the movement of the Islamic resistance) and Palestine Islamic Jihad (PIJ), which are regional jihad forces whose battlefield is restricted to Palestine; Hezbollah (Party of God); Lashkar-e-Taiba; Irish Republican Army (IRA); Red Army Faction (Baader-Meinhof Gang); the PLO; the Basque ETA (Fatherland and Liberty); Kurdish Workers' Party (PKK); and German neo-Nazis. Some of these are nationalist–separatist organizations.

Over the past 15 years, a number of terrorist acts have been carried out, or attempted, against the United States and its interests in this country and abroad by transnational groups. Major incidents include the 1983 bombing of the marine barracks in Lebanon; the 1993 ambush of US Marines in Somalia; the 1993 bombing of the World Trade Center; the 1996 truck bombing of the Khobar Towers in Saudi Arabia; the 1998 bombings of the American embassies in Kenya and Tanzania; the 1999 thwarted attempt of Ahmed Rassam to cross the US–Canadian border with bomb-making materials (118 pounds of urea crystals, 14 pounds of sulfate powder, and 48 ounces of nitroglycerin) intended for detonation at Los Angeles International Airport; the 2000 suicide bombing of the USS Cole in Yemen, and the attacks of Sept. 11, 2001.

Domestic Groups and Individuals have been responsible for the majority of terrorist acts in the United States. This has included cults and other religious organizations, white supremacists, militias harboring resentment toward the allegedly over-powerful government, paramilitary groups struggling for control of territory or influence, people who hate corporations, eco-terrorists, and anti-abortionists. Domestic terrorism in the United States has been typified by a prevalence of lone wolves. Notorious examples include Timothy McVeigh, Eric Rudolph, and the Unabomber, Theodore Kaczynski. In fact, US terrorism differs from terrorism in other countries in that a significant proportion of terrorist acts have been carried out by unaffiliated individuals rather than by members of terrorist organizations (Hewitt 2003).

The deadliest instance of domestic terrorism in the United States was the 1995 bombing of the Murrah Federal Building in Oklahoma City that killed 168 people, many of them children. This act was carried out by a right-wing extremist loner, Timothy McVeigh, who attached himself to a political ideology and acted from political motivation, but was not actually a member of an extremist group at the time of the attack. McVeigh began planning the bombing after a Michigan militia group distanced itself from him because his views were too radical.

As has been reported numerous times in the media (Copeland 2004), the FBI considers the eco-terrorist group Earth Liberation Front (ELF) to be the most significant domestic terrorist group in the United States. ELF is generally considered to be an amalgam of ELF and the former Animal Liberation Front, which is motivated by a radical concern for the protection of animals. ELF has been connected to dozens of acts of vandalism and arson since 1996.

During the past several years there has been a disturbing trend toward radicalization of young people within a targeted nation's border ("home-grown" jihadists). These are often groups of Muslim men who have adopted drastic measures to promote their cause. Typically, the individuals are second- and third-generation children of immigrants, fluent in the language and customs of the adopted country, who use their legal rights as citizens to rebel from within. They learn the Koran and terrorist tactics from the Internet and sometimes form small clusters of 20 to 25 mostly young men who share feelings of alienation, a longing for self-importance, and a need to become part of a larger group or movement. They have developed what has been termed *adversarial assimilation* (Zuckerman 2006).

While their cause is modeled after the jihadist movements in the Middle East, these home-grown terrorist cells typically have no direct association, and receive no direct training, operational guidance, or financial support from terrorist organizations overseas. In many cases, their activity has been described by terrorism specialists and the media as more inspirational than operational. However, it is not inconceivable that an unsophisticated but zealous group of home-grown jihadists could accumulate the relatively small amount of technical information required for the type of fertilizer-oil bomb

used so effectively in the 1995 Oklahoma City bombing. It is also not out of the realm of possibility that an amateurish home-grown terrorist cell could contemplate a low-tech intentional contamination attack on a lightly protected drinking water utility using materials such as pesticides purchased from local hardware stores.

Home-grown Muslim terrorist cells were responsible for the 2004 train attacks in Madrid, and the 2005 subway attacks in London. The media has covered the infiltration and breakup of several of these types of cells in North America including a 17-man unit in Toronto, Canada, and smaller cells found in Lodi, Calif.; Atlanta, Ga.; and Miami, Fla. “The vast majority of would-be terrorists are now freelancers and self-starters, which means that while we’re going to see more duds like the car-bomb attacks (in London, summer 2007), we are likely to see a lot more attempts” (*Time Magazine* 2007). To the extent that the killing of 13 individuals and wounding of 29 soldiers and civilians at Fort Hood, Texas, in November, 2009 is considered a terrorist act rather than a case of workplace violence, the alleged perpetrator, Major Nidal Hassan, may fit this model of a home-grown terrorist (*Time Magazine* 2009). The issue of domestic radicalization has received the attention of the US Congress as well as the DHS and the FBI (Thompson 2007).

Insiders. There are a number of reasons why a disgruntled employee might perpetrate a malevolent act against a water utility or other business. These may include revenge, retaliation, or venting of anger over a real or imagined affront to this individual by the employer. A malicious act could also be aimed at job preservation or self promotion. For example, in a small town in Western Pennsylvania in the 1980s, two drinking water treatment plant operators intentionally overdosed the finished water with potassium permanganate. Fortunately, no one was injured. However, the town’s drinking water turned purple in color and consumers became alarmed and upset. Allegedly, the employees’ motive was to demonstrate that the water company’s plan to downsize the workforce potentially affected the safety of the water system. These individuals were arrested and served a several-year prison sentence for their actions.

Vandals. Most malevolent acts carried out against utilities and other entities over the years have been acts of vandalism. The motivation for vandalism ranges from simple mischief to a rebellion against private or public property as symbols of authority.

Unfortunately, in the post-9/11 environment, even vandalism may be treated as a potential terrorism incident until an investigation proves otherwise. The impact on the community can be pronounced because officials may be forced to notify the public and issue “do not consume” or “do-not-use” advisories for the water supply while the situation is fully investigated and water samples are tested for a range of contaminants.

There is always the possibility that a simple act of vandalism could end up jeopardizing the safety of the drinking water supply. In 2002, students at a small liberal arts college in Ohio complained about the presence of animal

hair in faucet water and toilet water in one of the buildings on campus. An investigation revealed that someone had unscrewed the well cap for the well serving the building, dumped a groundhog into the well, and then replaced the cap (*Dayton Daily News* 2002). While the incident may have been a bizarre act of vandalism, had the animal been infected with a pathogenic microorganism such as the parasites *Giardia* or *Cryptosporidium*, the apparent prank could have led to a waterborne disease outbreak.

WEAPONS OF MASS DESTRUCTION

WMD are weapons capable of killing large numbers of people at one time and include conventional or nuclear bombs, weaponized chemicals such as nerve gases, and biological weapons including pathogens and biotoxins. They are defined by the US government (Title 18, U.S.C. 2332a) as:

1. "Any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, missile having an explosive or incendiary charge of more than one-quarter ounce, mine, or device similar to the above."
2. Poison gas
3. Any weapon involving a disease organism
4. Any weapon that is designed to release radiation, or radioactivity at a level dangerous to human life."

A significant concern is the limited ability to detect some of these weapons, such as pathogens with incubation periods of several days, or odorless chemicals or radionuclides. Limited detection ability may mean that the discovery of an attack comes only with the appearance of casualties. These weapons are also of particular concern because of their psychological impact. The fears among millions of Americans following the anthrax letter attacks in late 2001 were certainly out of proportion with the small numbers of deaths and injuries associated with the actual event.

In the drinking water industry, concerns over the use of NBC (nuclear, biological, chemical) weapons focus on the clandestine, intentional introduction of pathogens, biotoxins, weaponized chemicals, industrial chemicals, or radionuclides into public water supplies. In the wastewater industry, NBC concerns include the introduction of these types of agents into sanitary or stormwater collection systems, or directly into wastewater treatment facilities with a resulting negative effect on utility workers, the public, and the infrastructure. In the case of wastewater systems, as described in chapter 3 of this handbook, the NBC attack could be aimed directly at the wastewater system. Alternatively, and perhaps even more likely, these contaminants could end up in a wastewater system as a result of water discharged to the sanitary or stormwater collection system following cleanup efforts of contaminated buildings, or following a general contamination of the drinking water system in the community served.

The use of biological and chemical substances as weapons has its roots in antiquity. In Greek mythology, after Hercules killed the multiheaded hydra, he dipped his arrows in the creature's venom. His quiver was never again without a supply of poison arrows. In fact, the word *toxic* is derived from the Greek word *toxon*, which means *arrow* (Mayor 2003).

Falkenrath and colleagues (1998) discuss in great detail the documented use of NBC weapons in the past and the likelihood of their use in the future. They point out that during the past 100 years, NBC weapons have been used on a number of occasions by nation-states against each other during war. These include the use of weaponized chemicals during the First World War and during the Iraq–Iran War in the 1980s, the United States' use of nuclear weapons against Japan during the Second World War, and Japan's use of biological weapons against China during World War II. Falkenrath and colleagues indicate that nations have been reluctant to use NBC agents covertly because of international distaste for these weapons and fear of significant reprisals.

To date, there are almost no documented cases of terrorist groups or individuals successfully acquiring and utilizing NBC agents. The few exceptions are the successful nerve gas attack in the Tokyo subway system by the Japanese domestic terrorist group Aum Shinrikyo in 1995, and the mailborne anthrax attacks in the United States in 2001. However, the US Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism released a report in December 2008 on the potential for use of nuclear and biological weapons by terrorists in coming years. The Commission concluded that the threat, especially for bioterrorism, is increasing. The authors attributed this to the fact that many biological pathogens and nuclear materials around the world are poorly secured. They also attributed the increasing risk to the observation that biotechnology has spread globally, increasing the availability of pathogens and technologies that can be used for sinister purposes (Commission on Prevention of Weapons of Mass Destruction Proliferation and Terrorism 2008).

ISLAMIC FUNDAMENTALISM

Concerns about security and emergency preparedness in the water industry, as well as in other sectors of the society and economy, were obviously heightened by the al-Qaida attacks in 2001. Following the overthrow of the Shah of Iran in 1979, and especially since the events of 2001, Islamic fundamentalism has been an important issue in American foreign policy and homeland security in the United States. According to former secretary of the US DHS, Michael Chertoff (2008), "Just as totalitarian communism and fascism were the main ideological threats of the 20th century, it is the totalitarian ideology and practice of violent extremist Islamism that threatens our world today."

Virtually the entire Muslim world has experienced a religious resurgence or a revival of Islamic fundamentalism during the past few decades (D'Souza 2002). Of the 22 nations of the Muslim world, none has been exempt from

influence by the current fundamentalist movement. Fundamentalist surges have occurred several times throughout the existence of the religion and involve an appeal for a return to observance of the literal teachings of the Koran. The most recent fundamentalist movement had its origins at the end of World War I with the collapse of the Ottoman Empire, the assumption of authority over the Middle East heartland by Britain and France, and the abolition of the Islamic caliphate by the Turkish reformer Kemal Ataturk (Chertoff 2008). The caliphate had existed for 1,500 years until 1924, first under Arab control and eventually under Ottoman Turkish control.

These events were viewed by a number of Muslim intellectuals as humiliating setbacks to the advance of Islamic civilization. It is in this period that the Muslim Brotherhood was founded in 1928 by an Egyptian school teacher, Hassan al-Banna. Blaming his civilization's problems on the rise of foreign influences, al-Banna favored a return to a romanticized, ideologically pure pan-Islamic movement whose leaders would become masters of the Middle East and beyond.

By the end of World War II, al-Banna's organization claimed more than 500,000 members in Egypt alone. In the 1950s and 1960s, al-Banna's successor, Sayyid Qutb, continued to articulate this Islamist vision. Qutb's extremist ideology advocated that the Muslim Brotherhood pursue the establishment of a world caliphate utilizing revolutionary methods that removed traditional restraints on warfare. In the early 1970s, Brotherhood members in Saudi Arabia recruited a young Osama bin Laden.

The fundamentalists feel threatened by the perception that the United States is exporting secularism that undermines traditional Islamic values and by US support for secular dictators in Pakistan, Jordan, Egypt, and Saudi Arabia. Today, bin Laden and his followers view themselves as fighting a *jihad* (holy war) against the US and its allies. The objectives of al-Qaida were clearly outlined by bin Laden prior to the attacks on the United States. The strategic goal is to drive the United States and its allies out of the Middle East, particularly American troops from Saudi Arabia, "the holy soil of Islam." Additional goals include cessation of US support for Israel, and the overthrow of the "corrupt" secular governments in the Middle East, followed by reestablishment of a fundamentalist Muslim caliphate in their place. The tactical approach to achieving al-Qaida's goals is to inflict so much death, injury, economic damage, and fear on the United States and allied countries that they accede to al-Qaida's demands.

As explained by former director general of the British Security Service M15 (Manningham-Buller 2006), extremists are motivated by a sense of grievance and injustice driven by their interpretation of the history between the West and the Muslim world. Al-Qaida has developed an ideology which claims that Islam is under attack and needs to be defended. In al-Qaida's eyes, the Western hostility to Islam is demonstrated by longstanding disputes such as Palestine–Israel and Kashmir, as well as by more recent events in Afghanistan, the Balkans, Chechnya, Iraq, and Lebanon.

"The video wills of British suicide bombers make it clear that they are motivated by perceived worldwide and long-standing injustices against Muslims; an extreme and minority interpretation of Islam promoted by some preachers and people of influence; and their interpretation as anti-Muslim of UK foreign policy, in particular the UK's involvement in Iraq and Afghanistan."

Since 2001, terrorist cells in Britain, some directed from or with links to al-Qaida in Pakistan, are suspected of having plotted approximately 30 attacks on targets in the UK or on aircraft leaving for the United States. All but the July 2005 attack on the London public transit system have been disrupted (Riedel 2007).

Much of bin Ladin's popularity is associated with his emphasis on symbols of Islam's past greatness when the religious movement, in a period of just one century following Mohammed's life, spread from the Arabian Peninsula through the Middle East, North Africa, and even into Europe. Bin Ladin promises to restore pride to people who consider themselves to be the victims of a series of foreign masters. In the opinion of some observers (Friedman 2003), Osama bin Ladin is a Robin Hood for many young Arabs and Muslims. What attracts them to him is not his vision of the ideal Muslim society, which few would want to live in, but rather his sheer defiance of their hypocritical rulers, Israel, US dominance, and their own economic backwardness.

There are several particularly difficult factors involved in defending against religiously motivated terrorist groups, such as the Islamic fundamentalist groups. These individuals do not consider themselves "illegal terrorists." They not only believe they have a cause, as most terrorists around the world do, but they have the conviction of divine sanction: they believe they represent the will of Allah on earth (Phares 2005). Some observers think that religiously motivated terrorists are more willing than secular terrorists to carry out mass attacks against civilian targets because the victims are considered to be unbelievers and infidels (Stern 2000).

Another critical aspect of dealing with religiously motivated groups is their willingness to die for the cause. Such a death is believed to guarantee a reward in the next life. A common prayer among jihadists is "Let me be a martyr in the service of jihad" (Ervin 2006). Defending against adversaries with such an intense level of dedication is certainly more difficult than defending against individuals who are concerned with their own survival as well as accomplishment of the mission.

The depth of anti-American sentiment and the long-range intentions of al-Qaida are evident in Osama bin Ladin's published statements (9/11 Commission 2004). From his headquarters in Afghanistan, in February 1998, bin Ladin delivered a *fatwa*—an Islamic religious ruling—in the name of his organization, The World Islamic Front for Jihad Against Jews and Crusaders. Claiming that the United States had declared war against God and his messenger, bin Ladin called for the murder of any American anywhere on

earth as the “individual duty for every Muslim who can do it in any country in which it is possible to do it.”

Three months later, when interviewed in Afghanistan by ABC-TV, bin Ladin expanded on these themes. When asked whether he approved of terrorism and of attacks on civilians, he replied:

“We believe that the worst thieves in the world today and the worst terrorists are the Americans. Nothing could stop you except perhaps retaliation in kind. We do not have to differentiate between military or civilian. As far as we are concerned, they are all targets.... We are certain that we shall—with the grace of Allah—prevail over the Americans.”

He went on to warn that “If the present injustice continues..., it will inevitably move the battle to American soil.”

In the view of some Middle East and terrorism specialists (Pipes 2003, Manningham-Buller 2006), militant Islam will remain a force for some time to come, probably decades rather than years. A National Intelligence Estimate on Trends in Global Terrorism concluded that “Activists identifying themselves as jihadists, although a small percentage of Muslims, are increasing both in number and geographic dispersion.... If this trend continues, threats to US interests at home and abroad will become more diverse, leading to increasing attacks worldwide” (DHS 2006).

According to some observers, al-Qaida continues to be a dangerous enemy that could attack the US homeland again (Riedel 2007). Al-Qaida has suffered some setbacks since Sept. 11, 2001. It has lost its state-within-a-state in Afghanistan and several of its top officials have been killed. However, the organization has established a base of operations in Pakistan. Its reach appears to have spread throughout the Muslim world, where it has developed a cadre of operatives, and in Europe, al-Qaida has laid claim to some disenfranchised Muslim locals and members of the Arab and Asian diasporas.

Osama bin Laden has mounted a propaganda campaign to make himself and his movement the primary symbols of Islamic resistance worldwide. The jihadists believe that by crushing homeland security in the United States, they can defeat American power worldwide. They are convinced that at some point the American public will no longer tolerate the pain resulting from terrorism, and this will lead the United States to surrender its interests in the Middle East. In the opinion of some observers (Phares 2005), acquiring WMD (nuclear, chemical, or biological) is a major goal of jihadists in order to establish a “balance of terror” with the West.

It is the willingness to kill indiscriminately, apparent in bin Ladin’s pronouncements and in the attacks of Sept. 11, 2001, that has motivated the US government and the water industry to reexamine the security of drinking water and wastewater systems in this country. Because the water industry outside of Iraq has not yet been significantly impacted by terrorism in the period since 9/11, there is a tendency to become complacent and dismiss drinking water and wastewater systems as potential direct or indirect targets

of malevolent acts. However, as exemplified by the 2001 airplane attacks on New York and Washington, the 2001 mailborne anthrax attacks in the United States, the 2004 train attacks in Madrid, the 2005 transit attacks in London, and the commando-style small arms attacks on hotels and train stations in Mumbai, India in November 2008, a key objective of terrorism is to achieve surprise and strike at targets, some of which are not usually considered to be the highest priority for defense, but can result in significant human and material damage. Water systems, along with many other “soft targets,” fall into this category.

REFERENCES

- Chertoff, M. 2008. The Ideology of Terrorism: Radicalism Revisited. *Brown Jour. of World Affairs*, 15(1):11.
- Combs, C.C., and M. Slann. 2003. *Encyclopedia of Terrorism*. New York: Checkmark Books.
- Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism. 2008. *World at Risk*. New York: Vintage Books.
- Copeland, L. 2004. Domestic Terrorism: New Trouble at Home. *USA Today*, November 15.
- Cowell, A. and R. Bonner. 2007. Medical Workers Emerge as Focus in British Inquiry. *New York Times*, July 3.
- Dayton Daily News*. 2002. Groundhog Put in College Well. *Dayton Daily News*, February 13.
- Department of Homeland Security (DHS). 2006. *National Intelligence Estimate on Trends in Global Terrorism*. Washington, D.C.
- D'Souza, D.D. 2002. *What's So Great About America?* New York: Regnery Publishing.
- Ervin, C.E., 2006. *Open Target: Where America is Vulnerable to Attack*. New York: Palgrave Macmillan.
- Falkenrath, R.A., R.D. Newman, and B.A. Thayer. 1998. *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*. Cambridge, Mass.: MIT Press.
- Friedman, T.L. 2003. *Longitudes and Latitudes: The World in the Age of Terrorism*. New York: Anchor Books.
- Hewitt, C. 2003. *Understanding Terrorism in America: From the Klan to Al Qaeda*. London and New York: Routledge.
- Lewis, B. 2003. *The Crisis of Islam: Holy War and Unholy Terror*. New York: Random House.
- Manningham-Buller, E. 2006. In Her Own Words. *Homeland Defense Jour.*, 4(12)38.
- Mayor, A. 2003. *Greek Fire, Poison Arrows, and Scorpion Bombs: Biological and Chemical Warfare in the Ancient World*. Swansea, Wales: Classical Press of Wales.
- 9/11 Commission. 2004. *Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton & Co.
- Phares, W. 2005. *Future Jihad: Terrorist Strategies Against America*. New York: Palgrave Macmillan.
- Pipes, D. 2003. *Militant Islam Reaches America*. New York: W.W. Norton & Co.
- Prados, J. 2002. *America Confronts Terrorism*. Chicago: Ivan R. Dee.
- Riedel, B. 2007. Al Qaeda Strikes Back. *Foreign Affairs*, 86(3):24.
- Shane, S. 2009. Troubled Life of an Anthrax Suspect. *New York Times*, January 4.
- Stern, J. 2000. *The Ultimate Terrorists*. Cambridge, Mass.: Harvard University Press.
- Thompson, B.G. 2007. On Radicalization. *Homeland Defense Jour.*, 5(5):80.
- Time Magazine*. 2007. Can We Spot the Threat? *Time Magazine*, July 16.
- Time Magazine*. 2009. Terrified or Terrorist? *Time Magazine*, November 23.
- Wright, L. 2006. *The Looming Tower: Al-Qaeda and the Road to 9/11*. New York: Alfred A. Knopf.
- Zuckerman, M.B. 2006. The Threat From Within. *U.S. News and World Report*, December 15.

THE THREAT TO DRINKING WATER SYSTEMS

There are approximately 53,000 community drinking water systems in the United States. Another 106,000 noncommunity systems serve schools, rest stops, fairgrounds, campgrounds, etc. The size of these water systems varies greatly. The largest include more than 400 community water systems that serve more than 100,000 people each. These are primarily surface water systems and provide water to nearly 45 percent of the American population. The smallest include 30,000 groundwater systems that serve fewer than 500 consumers. To what extent are these water systems a target for terrorism and other intentional acts?

A common belief has been that an attack on a water utility is not likely because it would not provide the same sensational media video footage as an attack on an airplane, train, subway, or iconic building. Perhaps this is true. Another piece of conventional wisdom holds that an intentional contamination attack on a drinking water system is too sophisticated and would require too much contaminant to be successful. Unfortunately, this is not true.

Because drinking water is a basic necessity, an attack on a water system, either through intentional contamination or a physical attack of a critical facility, would likely have a profound impact on consumers' confidence in the safety of their water. The effect on public confidence would include not only the attacked utility, but other utilities throughout the country as well. And, the impact would be magnified with greater numbers of injuries, illnesses, or deaths. Such an attack would be successful terrorism because it could create intense fear as well as significant social and economic disruption.

The President's Commission on Critical Infrastructure Protection (1996) identified three crucial attributes for public water supplies.

- There must be adequate quantities of water.
- Water must be delivered at adequate pressure.
- Water must be safe to use.

Incidents that affect any of these three characteristics can significantly affect the community. The first two attributes can be directly influenced by physical damage. The third attribute can be affected by physical events as well as accidental or intentional introduction of microbes, biotoxins, chemicals, or radioactive materials.

The idea that drinking water utilities could be the target of sabotage or terrorism has been acknowledged by the US Justice Department over the years. Just prior to the outbreak of World War II, former FBI Director J. Edgar Hoover (1941) wrote the following statement in an article published in the *Journal American Water Works Association* (JAWWA) entitled "Water Supply Facilities and National Defense":

"It has long been recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace. Obviously, it is essential that our water supply facilities be afforded the utmost protection."

Years later, following the terrorist attacks of 2001, FBI Director Robert Mueller (2003) made a similar statement:

"Poisoning food and water supplies may be an attractive tactic in the future. Although technologically challenging, a successful attempt might cause thousands of casualties, sow fear among the US population, and undermine public confidence in the food and water supply."

The water industry was aware of its vulnerability to terrorist actions prior to the attacks of Sept. 2001. Porter De Nileon (2001) described a number of hypothetical scenarios and potential perpetrators in a JAWWA article published just months prior to 9/11. The article also described a number of measures that were already being developed to help protect the water sector from intentional attacks, including vulnerability assessments (VAs) and the Water Information Sharing and Analysis Center (ISAC).

The possibility of an intentional contamination event directed toward water supplies was also acknowledged by the National Research Council (NRC) in its report on the role of science and technology in countering terrorism (NRC 2002):

"Within the nation's infrastructure the US water supply is *probably not* the most likely target for producing mass casualties, because the combination of high dilution and water treatment provides protection against many threats. However, forced entry of a highly toxic agent into the system after water treatment could have serious consequences.... What water utilities and drinking water professionals are not prepared for is bioterrorism. Testing

and treatment for certain biological agents, their toxins, and other exotic contaminants have not been developed."

In reality, the probability of any specific drinking water system becoming the target of a terrorist attack is minuscule. However, the possibility of a water system somewhere becoming the target of a terrorist attack is real, and the consequences could be significant. Furthermore, the chances of a particular drinking water utility becoming the target of a disgruntled employee or simple vandalism that must be investigated to ensure that it isn't terrorism are very real. For these reasons, utilities in the current environment must pay some attention to defense against and response to malevolent acts.

WHY DRINKING WATER SYSTEMS COULD BE A TARGET

Drinking water might be considered a potential candidate for a terrorist act for several reasons. Drinking water is a basic necessity, like air. Everyone, even bottled water consumers, must use the public water supply for cooking, bathing, washing dishes, and other basic activities.

Because water is ingested through drinking and cooking, inhaled as an aerosol in showers, and comes into dermal contact with people through domestic and occupational exposure, there is significant potential for human contamination or infection if toxic chemicals or pathogens are present in the water. Consequently, there is a potential for casualties, perhaps in large numbers.

A successful attack on a water supply anywhere in the US would have a significant psychological impact on people throughout the nation and lead to a loss of confidence in the overall safety of domestic drinking water. This could cause a major disruption in everyday life for millions of people. A similar situation occurred in autumn 2001, when many people in this country feared handling and opening mail during the mailborne anthrax attacks.

Municipal water is important not just for consumption, but also for sanitation, public safety (fire protection), and economic purposes (e.g., factories, restaurants). Drinking water systems have several features in common with wastewater systems that make both of them potential targets for terrorism. Both are typically spread over a large geographic area and contain many components that are relatively easy to access (e.g., treatment plants, booster pumping stations, miles of distribution or collection mains). This makes both types of systems difficult to protect.

Both drinking water and wastewater systems are becoming more automated, which means fewer people are physically present at utility sites keeping an eye on things. The increasing automation, by definition, also means that the systems are more susceptible to cyber attack.

Both drinking water and wastewater systems are generally perceived to be government entities, even if they are private or investor-owned. Therefore, they could serve as political targets.

SCENARIOS OF CONCERN

Physical Assault

A physical assault on one or more components of a drinking water system is considered to be one of the most likely scenarios of concern for this industry. Such an attack could involve the use of an improvised explosive device (IED), a vehicle-borne improvised explosive device (VBIED), or an improvised incendiary device (IID). These devices are considered to be the most likely weapons in a water system attack because the materials to make them are easier to acquire and require less technical expertise to assemble and utilize than sophisticated chemical agents or biological pathogens.

On the other hand, a physical attack may not create the widespread public fear that an intentional contamination event would because the health of the entire community may be threatened by contaminants in the public water supply. Physical destruction of water facilities could deny service to individuals, businesses, and industries, creating a potentially devastating impact on fire protection, medical care, industrial production, and other services. The economic effect on the community would be significant if critical water or wastewater services were destroyed. A disruption in the supply of water, when coordinated with arson, would compound the effect. Furthermore, because much of the equipment in drinking water and wastewater systems, such as pumps and power sources, are custom designed, it could require months to replace them if they were destroyed (President's Commission on Critical Infrastructure Protection 1996).

In its report on the role of science and technology in countering terrorism, the NRC (2002) pointed out that major cities such as Boston, New York, Los Angeles, and San Francisco are served by aqueducts which, if lost from service, would have major cascading effects on the community. The report recommends that more attention be given to the interconnectedness of water supply systems and water transfers.

Some of the most commonly used IEDs have been homemade concoctions assembled from relatively easy-to-acquire materials. A number of intentional explosions have been carried out using triacetone triperoxide (TATP), which is made from acetone and hydrogen peroxide. This mixture is extremely reactive and can be detonated by an electrical spark or from common devices such as cell phones or flash cameras. The explosive has reportedly been nicknamed the “Mother of Satan” by terrorist organizations and has been used as a detonator explosive or a primary explosive in al-Qaida bomb plots and by Palestinian suicide bombers.

The mixture was also used in the London subway and bus bombings of 2005 and was allegedly intended to be used in the thwarted multiple bombings of commercial airliners flying from England to the United States in the summer of 2006. Acetone is an easily obtain solvent, but the hydrogen peroxide sold in pharmacies is only 3 percent strength and is too dilute to be used as an explosive. The most effective form of hydrogen peroxide, 70 percent, is

capable of generating a powerful explosion but is difficult to obtain. However, 30 percent peroxide is commercially available from chemical supply houses and is powerful enough to set off a fire or small explosion. The details for manufacturing TATP have been reported in the popular press (Cowell 2005, Chang and Broad 2006).

VBIEDs can carry much greater explosive power than a hand-delivered IED. Since 1970, terrorists of one stripe or another have deployed at least 756 vehicle bombs around the world (*Time Magazine* 2007). The most frequent users have included the IRA, the Basque Separatist group ETA, and al-Qaida. The destruction of the Alfred P. Murrah Federal Building by Timothy McVeigh is the classic example of the use of a VBIED in the United States. The mechanisms employed with a VBIED are typically low-tech and range from simple fertilizer–oil concoctions (Oklahoma City) to gasoline containers accompanied by propane tanks that create a fuel–air explosive bomb designed to produce a huge fireball by igniting aerated liquid gasoline.

A number of physical attacks on water systems have been documented. In 1999, a bomb blast in Lusaka, Zambia destroyed the main water pipeline, cutting off water for the city of 3 million (*Financial Times Global Water Report* 1999).

In September 2003, four incendiary devices were found inside a water-bottling plant's pumping station in Michigan. The plastic bottles containing a flammable liquid were safely removed without injury to personnel or damage to the facility. The Earth Liberation Front (ELF), an American domestic terrorist group, claimed responsibility for the attempted arson while accusing the water company of stealing well water for profit. ELF's written acknowledgement of responsibility stated: "Clean water is one of the most fundamental necessities and no one can be allowed to privatize it, commodify it, and try and sell it back to us" (Associated Press 2003a).

In Iraq (2003), insurgents destroyed a major water pipeline in Baghdad. The attack occurred around 7:00 am in the morning when a blue Volkswagen stopped on an overpass near the Nidaa mosque and an explosive was fired at the 72-in. diameter water main in the northern section of Baghdad (Tierney and Worth 2003).

In Nepal (2006), Maoist insurgents detonated explosives in two water reservoir tanks and damaged distribution lines, disrupting the drinking water supply for 20,000 people.

In Colombo, Sri Lanka (2006), powerful explosives were used to damage the main water distribution pipeline to the capital. Parts of the city were left without drinking water. The explosions occurred hours after the government imposed tough laws to deal with Tamil Tiger separatists who are fighting to create a separate homeland for Sri Lanka's ethnic Tamil minority (Associated Press 2006).

Accidental or Intentional Release of Hazardous Treatment Chemicals

Many drinking water and wastewater systems use chlorine gas for disinfection at the treatment works and in the distribution system. As evidenced by its widespread use as a weapon during World War I, chlorine gas released to the environment can be a lethal weapon.

The public health impact of chlorine gas release was also tragically illustrated in 2005 in rural Graniteville, S.C., when an accidental derailment of a Norfolk Southern railroad train resulted in the rupture of a 90-ton tank car of chlorine gas. Although only about 60 percent of the car's chlorine escaped, 10 people were killed and 630 were injured.

In early 2007, a bomb hidden beneath a tanker carrying chlorine gas was detonated in Taji, Iraq. Nine people were killed and more than 150 coughing and wheezing villagers flooded the hospital after noxious plumes covered homes and schools north of Baghdad (Associated Press 2007). This bombing was followed by a number of chlorine gas attacks in Iraq, signaling a new tactic by militants to spread greater panic with chemical weapons. While the Iraqi and US fatalities incurred in the 2007 attacks have been attributed to the explosives rather than the chlorine gas, it is likely that the explosives were not appropriately configured for the most effective release of the gas. This is a failing that could be potentially corrected by attackers in the future (Welter 2009).

The chlorine attacks in the Middle East raised fears over the possibility of copycat incidents in the United States. The storage of hazardous treatment chemicals at drinking water and wastewater utilities, and the shipment of those chemicals by rail and truck through populated areas, represent potential weapons that could be exploited by individuals or groups with malevolent intentions.

A large number of drinking water plants also store ammonia for use in the chloramination process. Accidental or intentional release of gaseous ammonia also poses a risk for utility employees and the public.

Cyber Attack

Throughout the world, supervisory control and data acquisition systems (SCADA) control a variety of critical facilities and infrastructures including nuclear power plants, chemical plants, electric utilities, natural gas utilities, and drinking water and wastewater systems. SCADA systems turn pump switches on and off, and control equipment. However, these systems are vulnerable to attacks ranging from those perpetuated by individual computer hackers seeking attention and bragging rights, to disgruntled employees and ex-employees, to domestic and international terrorists attempting to damage facilities and injure or kill people.

The potential for SCADA system interference to affect utility operations is demonstrated by a situation that resulted from accidental computer errors. In August 2003, computer glitches in Ohio caused inaccurate readings along

First Energy's electrical power lines. Cascading effects among Northeastern utilities resulted in the shutdown of more than 500 generating units in the United States and Canada. The subsequent blackout cut power to approximately 50 million people, shut down transportation and communications networks, interfered with drinking water and wastewater operations in a number of cities, and resulted in an estimated \$6 billion in economic damage (Keefe 2006). Admittedly, an intentional or unintentional interference in a water utility SCADA system would not have such far-reaching consequences because water utilities are not interconnected to the same extent as electrical utilities. However, the impact on a community could be significant.

Cascading Effects From Interdependencies

Drinking water utilities are dependent on other critical infrastructures such as electrical utilities that provide power to pump water, telecommunications, and transportation systems that deliver treatment chemicals. A water utility can be indirectly affected by an accident or malevolent act if the event successfully impacts an industry or infrastructure that water utilities rely on. An attack or accidental failure of a dam could destroy reservoirs, cause massive flooding, and contaminate drinking water supplies. An accident or attack at oil facilities or chemical plants could cause a significant contamination of source water or disrupt the delivery of supplies.

A poignant example of such a cascading effect, caused by an unintentional event was again failure of the electrical power grid in the northeastern United States in August 2003. The loss of electrical power interfered with the ability of several major cities, including Cleveland, Ohio, and Detroit, Mich., to pump finished drinking water to their customers for more than a day. The Cleveland blackout disabled the water authority's four main pumping stations, which provide drinking water to 1.5 million customers. The subsequent depressurization of the water system in both cities required boil water advisories several more days following restoration of water service. While this episode resulted from an accidental failure in the power grid, similar scenarios could be caused by an attack on the electrical power or transportation infrastructures (Luthy 2002).

Contamination

Intentional or accidental contamination of drinking water supplies is another significant concern because such an event could potentially affect a great number of people in a relatively short amount of time. A contamination incident could remain undetected until people have already become ill and show up in hospital emergency rooms. In the case of waterborne pathogens with a long incubation period, illnesses may not occur until several days following the introduction of the contaminant. By that time, the contaminant slug may have already passed through the distribution system, and a contaminated water sample may be very difficult to obtain to confirm the event analytically.

The President's Critical Infrastructure Assurance Office (1998) addressed the possibility of intentional contamination:

"The water supplied to U.S. communities is potentially vulnerable to terrorist attacks by insertion of biological agents, chemical agents, or toxins.... The possibility of attack is of considerable concern...these agents could be a threat if they were inserted at critical points in the system; theoretically, they could cause a large number of casualties."

Khan et al. (2001), from the US Centers for Disease Control and Prevention (CDC), concluded that while the general focus of those involved with antiterrorism has been on intentional aerosol delivery of contaminants, there is no easier way for a terrorist to disseminate a chemical or biological agent than through the intentional contamination of food or water supplies. They wrote: "A review of naturally occurring food and waterborne outbreaks exposes this vulnerability and reaffirms that, depending on the site of contamination, a significant number of people could be infected or injured over a wide geographic area."

Rose (2002) calculated that as little as 1 gram of feces containing 1 million infective units, adequately mixed in 1 million gallons of water, could create a risk of infection among consumers. In the case of rotavirus, the risk is 1 in 10 people consuming the water. In the case of *Cryptosporidium*, *Giardia*, and *Shigella*, the risks of infection are 1 in 1,000, 5 in 1,000, and 2 in 1,000, respectively. These estimates are based on dose-response data and the assumption that consumers ingested 1 liter of contaminated water. It is important to emphasize that while these estimates predict only sporadic cases of disease rather than a major outbreak, even a small number of illnesses attributed to an intentional act could create widespread fear. Additionally, the volume of contaminant required—one or a few grams of heavily infected feces—is easily carried in a test tube or small jar.

Many specialists argue that terrorists would likely deliver chemical or microbial agents in an airborne attack because the overall impact of the attack might be greater. However, perpetrators lacking the necessary equipment for effective aerosolization of agents could consider a drinking water contamination scenario because the attack might be technically easier to execute. As pointed out by Burrows and Renner (1999), while most biological warfare agents are intended for aerosol application and may be less effective as potable water threats, many are capable of inflicting heavy casualties when ingested.

The possible delayed detection of a contamination event lies in stark contrast to other scenarios, such as a physical attack or a release of hazardous treatment chemicals, which would become apparent almost immediately. As related by Byer and Carlson (2005), almost three weeks passed before the source of contamination was identified during the unintentional 1993 Milwaukee waterborne cryptosporidiosis outbreak that killed 100 people and sickened more than 400,000. The likelihood that an intentional contamination event would go undetected is underscored by the current limitations in online water-quality monitoring capabilities.

A successful contamination event could result in a number of negative impacts. The most important is illness and death among individuals who had consumed the contaminated water or, depending on the nature of the contaminant, had inhaled aerosols or come into dermal contact with the water. Dangerous aerosolization of volatile compounds, pathogens, or radionuclides could result from showering, flushing toilets, extinguishing fires, and perhaps even boiling water. Depending on the nature and amount of contaminant introduced, and the method of injection into the water system, intentional contamination of water could result in significant morbidity and mortality.

With or without significant numbers of injuries or deaths, an intentional contamination of the public water supply could produce fear and diminish public confidence in the ability of the government to protect its citizens. Depending on the difficulty associated with decontamination of the compromised water system, such an attack could result in a loss in the utility's ability to provide reliable drinking water for days, weeks, or longer. Such a loss could produce significant social and economic disruption. Corso and colleagues (2003) estimated that the total cost of outbreak-associated illness resulting from the accidental Milwaukee waterborne cryptosporidiosis event was \$96.2 million—\$31.7 million in medical costs and \$64.6 million in productivity losses.

POTENTIAL SITES FOR CONTAMINATION

Source Waters and Treatment Plants

While it is theoretically possible to contaminate the source water for a public water system, the large volume of water in a river, lake, or underground aquifer presents a major dilution barrier. Additionally, the presence of treatment facilities downstream of the source water provides an additional barrier because conventional treatment processes such as clarification, filtration, and disinfection would be expected to remove significant portions of most added contaminants (DeLeon and Stewart 2000). In this regard, groundwater systems may be somewhat more susceptible than surface water systems because groundwater systems typically employ a less rigorous treatment process or utilize no treatment at all.

While technically difficult to contaminate a source water and impact downstream potable water supplies, it is not impossible. On Nov. 13, 2005, an explosion occurred at a petrochemical plant in Jilin City in Northern China, releasing 10 tons of benzene and nitrobenzene into the Songhua River. The 50-mile-long slick of contaminants had a significant effect on water supplies and became an international incident when it eventually flowed into Russia. Drinking water service was shut off for four days to 4 million consumers in Harbin, the capital city of China's Heilongjiang province located 200 miles downstream from where the explosion and chemical release had occurred. The spill also denied water service to many consumers in smaller towns along

the river. Fortunately, the spill did not result in reported injuries or deaths but it did cause a panic, and hoarding of food and water, among consumers who were deprived of public drinking water (Yardley 2005).

A similar incident occurred in the United States some years earlier, affecting the Monongahela and Ohio rivers. In January 1988, a 48-ft-high storage tank collapsed near Pittsburgh, Pa., releasing 750,000 gallons of diesel fuel into the Monongahela River. This was one of the largest inland waterway spills ever to occur in this country. The spill significantly affected the drinking water supplies of a number of communities along the Monongahela and Ohio Rivers for several days (*Pittsburgh Press* 1988).

Both the Chinese and Pennsylvania spills were accidental. However, a deliberate release of chemicals affecting source waters for drinking water systems could result from an intentional explosion at an industrial site. Many of these sites have traditionally been located along waterways for transportation and waste-disposal convenience.

Additionally, many railroad right-of-ways parallel rivers and lakes. Millions of tons of dangerous industrial chemicals are transported on these rail lines, and their close proximity to the waterways makes rail accidents and subsequent spills a threat to raw water quality. Railroad accidents have occurred over the years, releasing contaminants into waterways and disrupting drinking water systems.

While these incidents were accidental, they illustrate the potential for an intentional physical attack on rail to deliberately contaminate rivers and lakes that serve as raw water sources for public water supplies. The contents of most railcars are clearly indicated in large lettering on the sides of the cars—convenient for potential perpetrators.

Several years ago, the US DHS explored the possibility of eliminating the chemical content information from the sides of railcars for security reasons. However, concerns over risks to emergency workers responding to rail emergencies were judged to be a greater practical issue than terrorism. Therefore, labeling of railcars continues to be the industry practice. However, additional US Department of Transportation (DOT) regulations are being developed to address security for transportation of hazardous chemicals.

Intentional contamination events in natural waters have been documented. In July 2000, workers at the Cellatex chemical plant in northern France dumped 5,000 liters of sulfuric acid into a tributary of the Meuse River when they were denied workers' benefits. A French analyst commented that in this instance, "the environment and public health were made hostage in order to exert pressure, an unheard-of situation until now." (*Christian Science Monitor* 2000).

It is also theoretically possible to contaminate a treatment plant. The widespread assumption is that dilution factors and treatment processes again make this difficult. However, not all public water supplies in this country incorporate full conventional treatment. A handful of major US cities do not filter the surface water that is their primary source, and a number of

groundwater systems do not disinfect the water or maintain a chlorine residual in their distribution system.

Accidental contamination events have occurred in treatment plants. In April 2007, an accidental overfeed of sodium hydroxide occurred overnight at a small drinking water treatment plant in Spencer, Mass. While there were no fatalities, a total of 93 people, from a population of 12,000, were treated at area hospitals for minor skin or esophageal irritations (Abel and Naughton 2007).

Distribution Systems

It is commonly accepted that the components of a public water supply most vulnerable to intentional or accidental contamination are the utility's distribution system and the plumbing network within individual buildings. In fact, this was the consensus of a drinking water expert panel convened by the Government Accountability Office (GAO) to assess the greatest vulnerabilities of US water supplies (GAO 2003). The idea that the distribution system is especially vulnerable is not new, and was discussed in the literature more than 50 years ago (Berger and Stevenson 1955). As noted by Byer and Carlson (2005), the distribution system has been identified as a major vulnerability for intentional contamination because of its accessibility to those it serves and its large geographic span. Because of the size of the population that some water distribution systems serve, a number of casualties could occur over a wide geographic area.

A municipal distribution system can include standpipes, reservoirs, tanks, and hundreds or thousands of miles of transmission mains that are virtually impossible to protect. Associated with this extensive distribution network are booster pumping stations and chlorination stations, as well as hundreds or thousands of fire hydrants and service connections. All of these are potential nodes for accidental or intentional introduction of contaminants.

Reservoirs and Storage Tanks

The conventional wisdom is that finished water storage tanks and reservoirs are not credible sites for a contamination event because the large volumes of water stored in these structures would dilute contaminants. This may be true for reservoirs containing millions of gallons of water. However, most reservoirs and storage tanks have a capacity of less than 1 million gallons. Even if a reservoir or tank contains massive volumes of water, the dilution factor can be overcome by contaminants that are extremely toxic at low dosages, or by accidental or intentional introduction of a contaminant near the effluent of the storage structure. It is, therefore, imprudent to automatically dismiss contamination threats to tanks or reservoirs as technically unfeasible.

An accidental situation that led to a fatal waterborne disease outbreak in Gideon, a town of 1,100 people in southeastern Missouri, supports the feasibility of an accidental or intentional contamination event in a drinking water storage facility affecting public health (Hrudey and Hrudey 2004). The source of the Gideons's drinking water is municipal wells, and the

groundwater is not treated or disinfected prior to distribution. The drinking water distribution network included two municipal storage tanks (one holding 50,000 gal of water, and the other holding 100,000 gal), as well as a private water storage tank of 100,000 gal capacity.

In early November 1993, the Gideon water system was systematically flushed in response to taste and odor complaints from residents. Then, in late November and early December, community residents started coming down with salmonellosis. By the time the outbreak was over, a total of 650 persons were estimated to have become ill, 15 were hospitalized, and 7 people had died. Investigators found that the backflow valve between the private distribution system and the municipal system had been open at the time of the epidemic. The 100,000-gal storage tank on the private system had an unscreened overflow pipe and a 5-inch diameter hole at the top, large enough for birds to enter. Samples of sediment from this tank, collected in January 1994, yielded the same strain of *Salmonella typhimurium* indicated in the disease outbreak. Pigeons had been commonly seen roosting on the tank roof, and bird feathers were subsequently found floating on top of the water in the tank.

The investigators concluded that bird droppings containing the *Salmonella* bacterium could have entered both the private and municipal storage tank and were most likely the source of contamination. The most plausible scenario for the outbreak was that extremely low temperatures on the evening of November 9 caused a thermally-induced turnover in the storage tanks that mixed contaminated upper-level water into the water being introduced into the community, leading to the taste and odor complaints. The resulting flushing program drew more of the contaminated stored water into the town distribution system. The relatively sudden discharge likely stirred up sediments and bacteria from the bottom of the tanks and introduced them into the distribution network.

The possibility of contaminating a finished water reservoir and affecting the health of a large community has been hypothesized. The World Health Organization (WHO) described a hypothetical contamination scenario for a city of 50,000 with a daily water use of 400 liters per person per day (WHO 1970). In this scenario, each person drinks 0.5 liters of water per day, and the lethal dose of the contaminant is 1 µg. The total dose required to contaminate 20 million liters of water in a storage tank or reservoir is 40 grams. Allowing for a factor of 6 to compensate for unequal distribution and dilution, the total amount of poison required would be 240 grams. Certainly consumers closer to the injection point would be at greater risk than those located farther away. However, the WHO scenario suggests a significant public health effect from a relatively small amount of contaminant.

While the effectiveness of a contamination event in a finished water storage structure is potentially hampered by significant dilution factors, this is much less of a problem if contaminants are added directly into the distribution piping system. As pointed out by Bernosky (2005), the volume of

water in 1,000 feet of 8-in. diameter pipe is only 2,610 gal. The volumes in 1,000 feet of 4-in. and 2-in. diameter pipe are only 652 and 163 gal, respectively. Furthermore, contaminants introduced directly into the distribution pipe network, as opposed to storage vessels, would reside in the system for shorter times, thus diminishing the effects of disinfectants and natural decomposition.

Fire Hydrants

Each of the hundreds or thousands of fire hydrants in a distribution system represents a point where contaminants could be injected using pumps or pumper trucks to overcome the system pressure. The potential for contaminant introduction via hydrants is well-demonstrated by the numerous reported cases of accidental distribution system contamination. These include instances where pesticides have been introduced into drinking water distribution mains by exterminators who had connected their delivery apparatus to hydrants using faulty backflow prevention devices. It is also demonstrated by incidents such as that which occurred in Charlotte, N.C. in 1997, when more than 60 gallons of fire-fighting foam, under pressure from a fire pumper hooked to a hydrant for cleaning, unintentionally backed into the hydrant and into neighborhood pipes and taps. This event prompted Charlotte officials to order thousands of residents not to shower or drink tap water for several days (Krouse 2001).

Service Connections

Each of the hundreds or thousands of individual service connections in a municipal network represents a node where contaminants could be backflowed into the distribution system using relatively inexpensive, small scale, portable pumps. The assertion that intentional backflows can affect public health is reinforced by the number of illnesses caused by accidental backflows. Between 1981 and 1998, accidental backflows were documented to have caused 57 waterborne disease outbreaks involving 9,734 illnesses (USEPA 2002). While this is a significant number, it represents only a percentage of the actual incidents and illnesses that have occurred because accidental backflow events are often underrecognized and underreported.

An accidental but fatal waterborne epidemic occurred in Cabool, Mo. that can be directly attributed to contamination in the distribution system (Hrudey and Hrudey 2004). In December 1989 and January 1990, 243 cases of severe gastroenteritis were observed in Cabool's population of 2,100 people. Eighty-two cases were characterized by bloody diarrhea, 32 people were hospitalized, 2 developed hemolytic uremic syndrome, and 4 died. Occurrence of the illness was strongly associated with consumption of Cabool tap water, and the causative agent was identified as the bacterium *Escherichia coli* O157:H7. The source of Cabool's drinking water was municipal wells, and the water was distributed without treatment or disinfection.

Investigators concluded that the contamination resulted from sewage overflows from an aging sewage collection system occurring at about the

same time as two major water main breaks and repairs. Apparently, the potable water distribution system was contaminated with raw sewage. This instance of accidental contamination of the distribution system underscores the possibility of intentional contamination of the distribution system leading to significant public health impacts.

The potential for intentional contamination of a drinking water distribution system has been described in the popular media. An article in the *Wall Street Journal* (2001) discussed this vulnerability in detail stating that “one sociopath who understands hydraulics and has access to a drum of toxic chemicals could inflict serious damage pretty quickly.” The article goes on to explain that a perpetrator, using a device as simple as a vacuum sweeper or bicycle pump, could backflow concentrated amounts of a toxic substance into the public water distribution system from the service connection in a home or business. Following publication of this article, there was a significant amount of discussion among individuals in the drinking water industry concerning the wisdom of describing this scenario in such detail in the press.

Allman and Carlson (2005) used commercially available distribution system modeling software to better understand how a drinking water distribution system could be affected by the intentional introduction of chemical contaminants. Four toxic chemicals were selected and water quality models of various scenarios were used to determine the influence of injection methodology, location, and the chemical itself on the effectiveness of the contamination event. The results of the modeling exercises demonstrated that significant contamination of a drinking water system could be accomplished through backflow into network water supply lines.

Individual Buildings

Contaminants can also be accidentally or intentionally injected directly into the potable water systems of large buildings using either internal plumbing lines or building potable water storage reservoirs. Affected facilities could include hospitals, hotels, office buildings, and government buildings. Building water systems are thought to be particularly vulnerable because access to the water system is usually not well protected. In fact, some large buildings have potable water storage tanks in plain view on the roof. The water quality within such potable water systems is almost never routinely monitored. Additionally, because building water supplies offer almost immediate contact with large numbers of people, there is little protection afforded by dilution, or the negligible chlorine residuals typically remaining after municipal distribution system water enters a large building plumbing network. Furthermore, in the case of hospitals, many of the people who would be exposed are weakened patients who are susceptible to opportunistic pathogens.

The potential for damage from accidental or intentional contamination was demonstrated by an accidental event that occurred in Chicago in 1933. In that incident, raw sewage entered the potable water system of a hotel through an inadvertent cross connection between sewage and water lines

within the building. The parasite *Entamoeba histolytica*, the causative agent of amoebic dysentery, was present in the sewage. As a result, 1,409 people became ill with amebiasis and 98 people died (Bundesen et al. 1936).

An intentional contamination of a building water system was reported in Edinburgh, Scotland, in 1990 (Ramsay and Marsh 1990). In this incident, nine people living in the same apartment complex were diagnosed with giardiasis, an infectious gastrointestinal disease caused by the parasite *Giardia lamblia*. The complex was served with drinking water from two linked rooftop tanks. The investigation conducted subsequent to the clinical diagnosis revealed that one of the tanks contained high coliform bacteria counts and fecal deposits below the tank's inspection hatch. The tank had apparently been intentionally contaminated with fecal material containing *Giardia*.

A foiled plot to contaminate the internal plumbing system of a Jerusalem hospital was reported in the Israeli press in 2002. According to a charge sheet filed in the Erez Junction military court, an 18-year-old Islamic Jihad activist was arrested by Shin Bet, the Israeli security service, before he was able to add a toxic contaminant to the hospital's internal drinking water reservoirs. The contaminant consisted of a combination of baking soda and an unnamed liquid poison (*Ha'aretz* 2002).

CONTAMINANTS

Various contaminants in water could poison or infect individuals via a variety of exposure routes including ingestion, inhalation, and dermal contact. The ideal intentional contaminant would have the following characteristics:

- Low infectious or toxic dose required
- Chlorine resistant
- Stable in water
- Easy for a perpetrator to acquire or manufacture
- Stores well, before use, for long periods of time
- Difficult for consumers to detect in the water by appearance, odor, or taste
- Difficult to detect and identify using routine grab or online analytical methods
- Produces severe disease and results in systemic complications leading to death

The common perception is that a contamination event would have to deliver a dosage of pathogen equivalent to the infectious dose 50 percent (ID_{50}) to cause harm in the consumer population. The ID_{50} is the dosage of pathogen that the population of average sized adults would have to ingest, inhale, or come into dermal contact with to result in a 50 percent infection rate of the exposed individuals. An equivalent belief concerning toxic substances is that a toxicant would have to be delivered to the consuming population at the lethal dose 50 percent (LD_{50}) level to be effective. The LD_{50} is the dosage of poison that the population of average-sized adults would have

to ingest, inhale, or come into dermal contact with to result in the death of 50 percent of the exposed population. In reality, illness or death among far fewer than 50 percent of the exposed population would cause significant fear and disruption in the population. This was evidenced by the anthrax attacks on the US mail system in October 2001. While these attacks resulted in only five deaths and a small number of illnesses in a geographically limited area in the United States, the incident caused concern and disruption for millions of people across the nation.

Several open-literature reports on biological, chemical, and radiological substances potentially useable for intentional contamination of drinking water were published prior to 9/11 (Burrows and Renner 1999, Deininger 2000, Clark and Deininger 2000). The infectivity and toxicity concentrations for specific contaminants listed in these works vary quite a bit in some cases. An AwwaRF (now the Water Research Foundation) study examined hundreds of threats, disrupted plots, and even some successful intentional contamination events directed toward public water supplies in the United States and overseas during the past several decades (Welter et al. 2003). Table 2-1 lists contaminants that were either threatened or actually used in these incidents.

Descriptions follow of several contaminants that have appeared in open literature discussions of contaminants that perpetrators may attempt to use for intentional contamination of water. The fact that these contaminants are discussed in this chapter does not suggest these particular contaminants would actually be effective in this application. The contaminants are merely included as possible examples.

Fortunately, as pointed out by the WHO, it is neither possible nor necessary for officials to plan for an attack on water using every conceivable specific contaminant (WHO 2004). Rather, planning and preparation to counter the effects of general groups of contaminants should provide the capabilities to deal with a wide variety of possibilities.

Table 2-1. Contaminants used or threatened in attacks on drinking water

| | | | |
|-----------------|--------------|-------------|------------------------|
| Agent Orange | Chlordane | Herbicides | Perchloethylene |
| Ammonia | Cyanide | LSD | Pesticides |
| Anthrax | Fecal matter | Lye | Plutonium trichloride |
| Arsenic | Food dye | Mercury | Potassium permanganate |
| Bioweapon | Fluoride | Naphthalene | Ricin |
| Botulinum toxin | Heating oil | Nerve gas | Sewage |
| Cholera | | | Toxic waste |

Biotoxins

Biotoxins are substances produced naturally by living organisms. While their presence in the environment is sporadic and usually in low concentration, some of the microbes and higher level organisms that produce these toxins can be cultivated. For certain agents, directions for cultivation appear on the Internet and in the underground literature. Limited technical expertise would be required to produce some of these substances.

A report published by the US Army Combined Arms Support Command (Burrows and Renner 1998) listed the following biotoxins as at least “possible” candidates for use as intentional contaminants for drinking water: botulinum, T-2 mycotoxin, aflatoxin, ricin, staph enterotoxins, microcystins, anatoxin A, tetrodotoxin, and saxitoxin.

Botulinum toxins are the most virulent of all of the biotoxins, and are some of the most toxic substances known. Botulinum toxins are produced naturally by the bacterium *Clostridium botulinum* and exist in seven neurotoxic forms. While botulinum toxins have been weaponized by a number of countries for aerosol application, they are more toxic when ingested than when inhaled (Eitzen et al. 1998). Botulinum toxins have traditionally been associated with cases of food poisoning resulting from improper canning techniques. In 1971, a resident of Bedford, N.Y. died of botulinum poisoning after eating vichyssoise manufactured by the Bon Vivant Company (Newman 2005). More than a million cans of possibly underprocessed soup were recalled, forcing the company into bankruptcy.

Open literature sources on the toxicity of this substance include LD₅₀ estimates of 0.4 µg per person (0.006 µg/kg) based on 18 case reports of botulism, 16 of which were fatal (Burrows and Renner 1999). An estimate of the no observed adverse effect limit (NOAEL) for consumers ingesting 2 L of contaminated water is 0.0004 µg/L (Rose 2002). With such a low toxicity threshold, botulinum toxin has the reputation that one gram of the toxin could kill 20 million people if it could be effectively dispersed and ingested. The toxin works by producing a protein that blocks the release of acetylcholine, a neurotransmitter that stimulates muscles to contract. Symptoms may be experienced within 24 to 36 hr. A progressive paralysis from head to toe follows. The victim remains mentally alert for the duration of the illness, and death results from an inability to breathe. Ironically, botulinum toxin, delivered in dilute form in the drug Botox, is used in medical applications ranging from the softening of wrinkles to treatment for the spastic muscular contractions of multiple sclerosis and cerebral palsy.

Burrows and Renner (1999) reported that botulinum toxins are more than 99.7 percent inactivated by 3 mg/L free chlorine in 20 min, and 84 percent inactivated by 0.4 mg/L free chlorine in 20 min. A US Army report indicated that botulinum toxins are stable in water and should be considered to be a drinking water threat (US Army Center for Health Promotion and Preventive Medicine 1998).

In 1980, a cell of the Red Army Faction was discovered in Paris with cultured *C. botulinum*. In 1984, two Canadians were arrested by the FBI when they tried to order *C. botulinum* from the American Type Culture Collection (ATCC), a biological supply house in Maryland (Falkenrath et al. 1998). While no attempts to intentionally contaminate drinking water with botulinum toxin have been reported, this toxin usually appears in open literature listings of potential intentional contaminants of water because of its substantial toxicity.

Ricin, derived from the bean of the castor plant, is another commonly known biotoxin. Ricin achieved notoriety as a tool of assassination in 1978 when Bulgarian journalist and dissident Georgi Markov was murdered in London when his attacker jabbed him in the leg with an umbrella modified to fire a pellet containing ricin (Mullins 1992). If ingested, ricin causes gastrointestinal hemorrhage with organ necrosis (Eitzen et al. 1998). Open literature sources indicate an oral LD₅₀ for mice of 20 mg/kg of ricin (Burrows and Renner 1999).

Castor beans are easily obtained. Basic but effective recipes for extracting ricin from the beans are available on the Internet. Limited technical background and equipment is required for production of at least crude preparations.

Rose (2002) estimated a NOAEL of 15 µg/L ricin for an individual ingesting 2 L of water. Burrows and Renner (1999) reported that ricin is more than 99.4 percent inactivated after 20 min contact with free chlorine at 100 mg/L, but is essentially unaffected at 10 mg/L. A US Army report indicated that ricin should be considered a potential threat for intentional drinking water contamination (US Army Center for Health Promotion and Preventive Medicine, 1998).

In 1993, Canadian border police confiscated 130 g of ricin from Thomas Lewis Lavy, an Arkansas resident with reported links to survivalist groups, as he tried to enter Canada from Alaska (Falkenrath et al. 1998). In the summer of 1995, an oncologist from Kansas City, Mo., attempted three times to poison her husband with ricin that she had extracted from castor beans (Rizzo 1996).

In 2003, a vial containing ricin was discovered in a Greenville, S.C., postal facility. An accompanying note stated that the city's water supply would be contaminated with ricin unless changes were made in federal regulations pertaining to the hours that truckers can drive without rest. No indication of ricin contamination of the water supply was reported (Miller 2003).

Infectious Microbes

A number of pathogenic microorganisms (bacteria, viruses, and protozoa) may be used for intentional contamination events. The capacity of these microbes to cause disease and death via the waterborne route has been demonstrated by waterborne disease outbreaks that have occurred accidentally. An additional concern is that highly trained and well-equipped perpetrators

potentially could increase the stability of a pathogen, or reduce its sensitivity to disinfection, via sophisticated techniques such as bio-engineering or encapsulation.

A report prepared by the US Combined Arms Support Command (Burrows and Renner 1998) listed the bacterial agents of the following diseases as at least possible candidates for intentional contamination of drinking water: anthrax, brucellosis, tularemia, shigellosis, cholera, salmonellosis, and plague. The same report listed Q fever and psittacosis as intentional rickettsial diseases, and cryptosporidiosis as an intentional waterborne protozoal disease. Additionally, the report described *variola* (smallpox) and hepatitis A as viruses that could potentially be used to intentionally contaminate water.

Biological agents are often considered to be more of a concern than chemical agents because large amounts of a pathogen can be grown from a small initial culture. In the case of certain pathogens, the illness may be subsequently transmitted from person to person. Additionally, the dosage of pathogen needed to induce illness can be a small amount, much smaller by weight than that required for a chemical contaminant.

Anthrax, a disease of hooved animals that is readily transmitted to humans, is caused by a spore-forming bacterium, *Bacillus anthracis*. The three recognized forms of the disease in humans are inhalational, cutaneous, and gastrointestinal. Cases of gastrointestinal anthrax have been documented from ingestion of contaminated meat. Ingested anthrax has an incubation period of 2 to 7 days and produces abdominal pain, fever, vomiting, bloody diarrhea, and shock.

Anthrax is one of the most commonly threatened contaminants in bioterrorism threats. Fortunately, the vast majority of threats and “white-powder” incidents have been hoaxes or false alarms. The significant exception was the series of US mailborne anthrax attacks that occurred in the autumn of 2001 (Jernigan et al. 2001). The primary concern regarding anthrax as a weapon of bioterrorism is its potential use in aerosol form. The US Office of Technology Assessment calculated that 100 kg of anthrax spores spread over Washington D.C. could kill from 1 million to 3 million people under the right weather conditions (Office of Technology Assessment 1993). The WHO estimated that the release of 50 kg of anthrax from an aircraft upwind of a city of 500,000 people would result in 95,000 deaths and 125,000 injuries (WHO 1970).

An accidental release of anthrax spores resulting from malfunctioning air filters occurred at a Soviet military microbiology facility in Sverdlovsk, Russia, in 1979. At least 77 cases of inhalational anthrax and 66 deaths occurred among people living or working within a distance of 4 km downwind of the release site. This was the largest documented epidemic of inhalational anthrax in history (Rich 1992).

Anthrax has been suggested as a potential intentional contaminant of drinking water in a number of open literature articles. Although no cases of waterborne anthrax have been documented in humans, cases of waterborne

infection have been reported for animals (Watson and Keir 1994). Anthrax was reportedly used by the Japanese Army to contaminate food and water supplies in Chinese cities during World War II (Christopher et al. 1997). Theoretically, if anthrax spores were added to drinking water, people could be exposed via all three routes: inhalation, cutaneous contact, and ingestion. Burrows and Renner (1999) have reported that *B. anthracis* spores can remain viable in pond water for periods of up to two years.

Rose and colleagues (2005) performed a series of disinfection studies on *B. anthracis* (Ames strain) in water, and found the spores to be fairly resistant to inactivation with free available chlorine. At a water temperature of 25 °C, they calculated contact time (CT) values of 79 for 2-log inactivation and 102 for 3-log inactivation of spores. In practical terms, this would mean that anthrax spores would need to be exposed to 1.0 mg/L free available chlorine for 79 min to kill 99 percent of the spores present, and for 102 min to kill 99.9 percent of the spores. These CT values are substantially higher than those typically reported for inactivation of coliform bacteria, the bacterial group usually used to indicate the sanitary quality of water. The results suggest that anthrax spores would probably not be readily inactivated by the free chlorine residuals typically found in municipal drinking water systems. Protection would be even poorer if the system residual consisted of the weaker disinfectant chloramine rather than free chlorine.

Cryptosporidiosis is a gastrointestinal infection resulting from ingestion of oocysts of the protozoans *Cryptosporidium hominis* or *Cryptosporidium parvum*. The symptoms of cryptosporidiosis include profuse diarrhea, nausea, and stomach cramps. The incubation period is 4 to 14 days and for otherwise healthy individuals, the symptoms may last for 10 to 15 days. In immunocompromised patients, the infection may be life-threatening because their immune systems are not capable of fighting the infection and there is not yet a definitive medical treatment for this illness. The infective dose is quite low and may require ingestion of just a single oocyst in the case of an immunocompromised person. *Cryptosporidium* is of particular concern from a drinking water point of view because the oocysts (environmental form) are almost totally resistant to chlorine and can survive in water for months.

Cryptosporidium has been suggested in the open literature as a potential candidate for intentional contamination of drinking water supplies because it has been associated with a number of accidental waterborne outbreaks. The largest waterborne epidemic occurred in Milwaukee, Wis., in 1993 and resulted in approximately 400,000 illnesses and 50 to 100 deaths (MacKenzie et al. 1994).

Bubonic, septicemic, and pneumonic plague are caused by the bacterium *Yersinia pestis*. Symptoms for all three diseases include high fever and toxemia within 5 days of infection. Plague is a disease of rodents but is transmissible to humans. Pneumonic plague can be spread by coughing. *Y. pestis* survives in water for periods of up to 16 days (Burrows and Renner 1999) and is considered a contamination threat in water (US Army Center

for Health Promotion and Preventive Medicine, 1998). During World War II, the Japanese military intentionally contaminated food and water supplies of Chinese cities with plague bacteria (Christopher et al. 1997). *Y. pestis* has been found to be readily susceptible to inactivation with the concentrations of free chlorine typically found in municipal drinking water distribution systems (Rose et al. 2005).

In 1995, Larry Wayne Harris, a resident of Ohio and a member of the white supremacist group Aryan Nations, was arrested after purchasing three vials of freeze-dried *Y. pestis* from the ATCC (Falkenrath et al. 1998). Although there is no proof that Harris planned to use the bacterium to infect humans, he was convicted of wire fraud because he had lied about the laboratory that he was representing when he ordered the cultures. At the time of this incident it was not illegal to possess plague and other potentially lethal microbes. However, as a result of the Harris case, the US Congress passed a law, now implemented in regulations issued by the federal CDC, restricting transport of select agents, such as the plague bacterium, to registered laboratories.

Salmonella spp. has been implicated in a number of accidental and intentional foodborne and waterborne disease outbreaks. One of the best documented waterborne episodes, previously described, occurred in Gideon, Mo. The Japanese intentionally contaminated food and water supplies with this bacterium in a number of Chinese cities during World War II (Christopher et al. 1997). From 1964 to 1966, several outbreaks of typhoid fever and dysentery in Japanese hospitals were traced to food and beverages purposefully contaminated by a research microbiologist, who later also infected family members and neighbors. Four people died and more than 100 became ill. The purpose of the deliberate contaminations may have been to obtain clinical samples for a doctoral thesis (*Science* 1966). An intentional *Salmonella* contamination of food in restaurants was carried out by a domestic religious cult in Oregon in 1984. Plans had also been made to contaminate the town water supply. This incident, which resulted in 750 individuals becoming ill, is described in more detail later in this chapter.

Salmonellosis occurs in two forms. Acute gastroenteritis is caused by *S. typhimurium*, whereas typhoid fever is caused by *Salmonella typhi*. The symptoms of acute gastroenteritis include vomiting and diarrhea, while the symptoms for typhoid fever are more general. Both forms of salmonellosis are transmittable in water. *Salmonella* bacteria have been reported to survive in water for periods of up to eight days and are susceptible to doses of chlorine typically found in municipal drinking water.

Observations of a number of outbreaks of salmonellosis suggest that the infective dose is less than 1,000 organisms (Blaser and Newman 1982). Outbreaks in which higher doses of salmonellae were ingested involved very high rates of attack and shorter incubation periods.

Shigellosis is dysentery caused by the ingestion of various *Shigella* species, in particular the bacterium *Shigella dysenteriae*. Shigellosis is transmittable

through food and water but is controlled by the typical doses of chlorine present in municipal drinking water systems in the United States. *Shigella* is reported to be stable in water for periods of 2 to 3 days (Burrows and Renner 1998). The clinical symptoms of shigellosis include diarrhea, abdominal pain, and bloody stools after an incubation period of approximately 48 hr. The infective dose by ingestion is estimated to be 10,000 organisms (Rose 2002).

Shigella bacteria were intentionally added to food and water supplies of Chinese cities by the Japanese during World War II (Christopher et al. 1997). In 1996, hospital employees in Dallas, Texas, became ill when muffins and donuts in the staff break room were intentionally contaminated with *S. dysenteriae* Type 2. Severe acute diarrheal illness was reported in 12 of 45 hospital laboratory staff. The intentional contamination was attributed to a disgruntled hospital laboratory employee who obtained cultures of the bacterium from the hospital lab (Kolavic, et al. 1997).

A US Army report indicated that **hepatitis A** should be considered to be a potential intentional contaminant for drinking water (US Army Center for Health Promotion and Preventive Medicine 1998). The report further indicated that the virus is inactivated by 0.4 mg/L free chlorine within a 30 min period and the infectious dose may be as low as 30 viral units. Hepatitis A has been responsible for numerous documented, and undoubtedly many undocumented, outbreaks of both waterborne and foodborne disease. The infection caused via these routes can be fatal.

Industrial Chemicals

There is probably more concern about the use of industrial chemicals as an intentional contaminant than for most other contaminant categories because these chemicals are so widely accessible. Fortunately, many industrial chemicals are only sparingly soluble in water, and many impart a disagreeable odor or taste to the water that would prevent consumption.

Cyanide appears in most open literature summaries of possible contaminants for use in drinking water. Whelton and colleagues (2003) published a literature review concerning the potential use of cyanide as an intentional contaminant for drinking water. Zyklon B, a crystallized version of hydrogen cyanide, was used in Nazi death camps during World War II to kill millions of people. The Zyklon B pellets, normally used as an insecticide, were exposed to air, permitting the release of hydrogen cyanide which killed its victims within a matter of minutes.

In 1978, more than 900 members of the People's Temple, followers of cult leader Jim Jones, committed mass suicide in Jonestown, Guyana, by drinking cyanide-laced Kool-Aid (Downie 1978). In 1982, seven people in the United States died after ingesting Tylenol capsules intentionally laced with cyanide. At a New Year's Eve celebration in 1994, nine Russian soldiers and six civilians in Dushanbe, Tajikistan, died after drinking cyanide-laced champagne. The champagne, poisoned by a Tajik opposition group, was on sale next to a military compound housing members of a Russian-led peacekeeping force.

Another 53 people were hospitalized, including 11 in intensive care (Reuters 1995).

A more recent threat of the use of hydrogen cyanide as a terrorist weapon was discussed in the book *The One Percent Doctrine* (Suskind 2006a) and in follow-up magazine articles (Suskind 2006b). These media accounts reported the discovery by Saudi and American counterterrorism agents of computer instructions written by a terrorism suspect in Bahrain for construction of a device designed to facilitate the release of cyanide gas in a closed space such as a theater or subway car.

The device, referred to as *mubtakkar* (meaning *invention* in Arabic), consists of a canister with two interior containers: sodium cyanide in one, and hydrochloric acid in the other. The containers are separated by a seal and a fuse. The fuse can be activated remotely by a cell phone to break the seal, which is a method similar to that commonly used to trigger bombs. Breaking the seal allows the creation and release of hydrogen cyanide gas. According to the popular accounts, the discovery of instructions for this device in February 2003 created quite a stir among US government officials.

Also, in 2002, four Moroccan men were arrested in Rome for possession of 9 lb of powdered potassium ferrocyanide, detailed maps of the US Embassy and the water distribution system of the city of Rome, and counterfeit immigration papers. The men were suspected of plotting an attack on the water supply of the embassy (Boudreux 2002). Fortunately, these individuals were ineffective terrorists, as they were caught before the attack was conducted, and poor toxicologists, as ferrocyanide, which is commonly used to make wine and ink dye, is one of the less toxic salts of cyanide.

Chemically, cyanide compounds are found in two forms: simple and complex. Simple cyanic forms, such as hydrogen cyanide and cyanogen chloride, are more toxic than complex forms, such as the metallic salts involving iron, copper, or silver. When simple cyanide salts such as potassium cyanide or sodium cyanide are added to water, they dissociate, producing cyanide ions, CN^- . Once dissolved in water, cyanide ions combine with hydrogen, especially at pH values less than 9.2, to form hydrogen cyanide. Common cyanide compounds such as sodium cyanide and potassium cyanide produce a mild almond-like odor in moist air. Cyanide compounds are readily available on the worldwide open and black markets because they are used industrially in electroplating, metallurgy, plastics manufacturing, and some mining processes (Hickman 1999).

Physiologically, when cyanide ions are inhaled or ingested, they bind with the enzyme cytochrome oxidase. This binding prevents the body from utilizing oxygen and can result in death. Ingestion of drinking water containing cyanide or inhalation of aerosols of water containing cyanide (such as from a shower) are potential routes of exposure. The US Environmental Protection Agency (USEPA) has set a maximum contaminant level (MCL) for cyanide of 0.2 mg/L. The MCL assumes a lifetime exposure with an average ingestion of 2 L of water per day. This chronic toxicity value was determined

using hydrogen cyanide toxicity data. The acute toxicity levels reported in the literature vary quite a bit. Manahan (1992) reported that death can result from ingestion of a 60 to 90 mg oral dose of cyanide. The US Army has proposed, and the NRC has approved, a cyanide drinking water limit of 6 mg/L for troops consuming 5 L of water per day for a 7-day period (NRC 2004).

Pesticides

A number of pesticides, such as the organophosphate pesticides and carbamates, are cholinesterase inhibitors. They cause central nervous system paralysis that leads to respiratory failure or cardiac arrest, potentially leading to death. The physiological mechanism for organophosphate pesticide toxicity is essentially the same as for the weaponized nerve agents soman, sarin, tabun, and VX, which are described in greater detail in the section on weaponized chemicals.

Pesticides have been used as contaminants in several documented cases of intentional drinking water contamination. In 1980, one or more individuals injected the pesticide chlordane directly into a pressurized drinking water transmission line in Pittsburgh, Pa., injuring a number of people and causing widespread disruption of water service for an extended period of time. In 2003, a perpetrator in China poured a pesticide solution into a finished water reservoir, injuring scores of people. Both of these incidents are described in greater detail later in this chapter.

Weaponized Chemicals

Weaponized chemicals are chemical compounds that have been synthesized for use in warfare. The categories of weaponized chemicals include: choking agents that damage lung tissue (e.g., phosgene); vesicants that burn eyes, lungs, and skin (e.g., mustard gas); and nerve agents that disable a crucial nervous system enzyme, acetylcholinesterase (e.g., tabun, sarin, soman, and VX). Weaponized chemicals have been developed and stockpiled by a number of countries over the years. Their use reached devastating proportions during World War I when chlorine, phosgene, and sulfur mustard gases were responsible for more than 1 million injuries and 100,000 fatalities.

Weaponized chemicals have been designed primarily for airborne delivery and for injury to victims via inhalation and dermal contact. Use of weaponized chemicals as an intentional contaminant in water is considered by most specialists as a less effective application. Some of the weaponized chemicals, such as the nerve agents, are relatively unstable in water and tend to spontaneously hydrolyze. However, for some of the agents this reaction requires a number of hours for completion. Nerve agents appear in many of the open literature lists of chemicals that could potentially be used to attempt to contaminate drinking water.

Nerve agents achieved notoriety as a terrorist weapon in 1995 when the Japanese cult, Aum Shinrikyo, attacked the Tokyo subway system with sarin gas (Falkenrath et al. 1998). On the morning of Mar. 20, 1995, cult members boarded subway trains at five stations around Tokyo. Each terrorist carried

two sealed pouches of dilute, low grade, sarin nerve gas. As the trains converged near the center of the city, the five men placed the bags on the floors of the trains, punctured them using sharpened umbrella tips, and fled. The liquid sarin leaked onto the floor and began to evaporate. The passengers displayed a variety of symptoms including sweating, runny noses, coughing, difficulty breathing, weakness, vomiting, and seizures. In all, 12 people died and more than 5,000 were injured.

Almost certainly, more victims would have died had the attackers synthesized a better quality of sarin, and used a more efficient dispersal device. The group had reportedly carried out another sarin attack 9 months earlier, in which they released 20 kg of the agent in the vicinity of the lodgings of three judges in the town of Matsumoto, Japan. This attack killed 4 people and injured 150.

These attacks were especially significant because they represented the first time that a nonstate-sponsored group was able to manufacture and successfully use a weaponized chemical in a terrorist act. The group had created a secret nerve gas production facility in the Japanese countryside and managed to produce tens of kilograms of sarin between 1993 and 1995. Interestingly, this same group had attempted attacks several years earlier in Tokyo using aerosolized anthrax and botulinum toxin. One of the attacks was aimed at the Japanese parliament, one at the wedding of the crown prince, and one was carried out from a rooftop in the city. Fortunately, these attacks failed to produce casualties.

The effectiveness of weaponized chemical agents as intentional contaminants in drinking water is questionable, at least in the open literature. A US military report on the toxicity of ingested weaponized chemicals lists an acute concentration for the nerve agents tabun, sarin, soman, and VX at 50 µg/L (ppb) (Garland 1991). An acute concentration in this context represents a concentration that would cause death or debilitation after ingestion of 0.5 L of contaminated water. The US Army has proposed, and the NRC has approved, a limit for nerve agents in drinking water of 70 µg/L for tabun, 13.8 µg/L for sarin, 6.0 µg/L for soman, and 7.5 µg/L for VX. This limit applies to troops ingesting 5 L of water per day over a 7-day period (NRC 2004).

Nerve agents in the bodies of living organisms act physiologically like the organophosphate pesticides in that they bind the enzyme acetylcholinesterase and inactivate it, thereby permitting the accumulation of large amounts of acetylcholine at neural synapses. Acetylcholine is a neurotransmitter that is released by nerves at neuromuscular junctions resulting in muscular excitation. Acetylcholinesterase is deliberately released by the body following muscular contraction to control the levels of the neurotransmitter acetylcholine. Accumulation of acetylcholine at neuromuscular junctions causes overstimulation of muscles resulting in convulsions and ultimately death.

There have been reports that nerve agents were used in an intentional attack on water supplies in Romania in 1989. At that time, the people were overthrowing the communist dictator Nicolae Ceausescu. It has been alleged

that members of the state secret police contaminated one or more drinking water supply tanks in the city of Sibiu with nerve agent, resulting in a number of people becoming ill.

Radionuclides

Radioactive materials are chemicals with unstable atoms that naturally release energy (radiation) in the form of alpha particles, beta particles, or gamma rays. Radionuclides are unstable atoms of an element that release radiation. Radiation can have significant impacts on human health depending on the type and amount of radioactive material, the proximity of the source of radiation, and the length of exposure time. Inhalation or ingestion of alpha or beta particles can pose a serious health risk. Similarly, external exposure to beta particles, and especially to gamma rays that can penetrate the body, is of serious health concern. Radioactive materials may be solid (metal, powder, salt), liquid (dissolved or suspended), or gaseous (gases, vapors, mists, or airborne dust). Some radioactive materials are water soluble while others are not.

Strontrium-90 releases only beta radiation. Americium-241 releases alpha and gamma radiation. Cobalt-60, molybdenum-99, iodine-131, cesium-137, and iridium-192 produce both beta and gamma radiation. And radium-226, uranium, and plutonium release alpha, beta, and gamma radiation. These radionuclides are potentially accessible to individuals with nefarious intentions because many of these substances are used in medical, industrial, or defense applications.

WHAT HAS ALREADY OCCURRED AT DRINKING WATER UTILITIES

Fortunately, no actual attacks have been carried out by transnational terrorists against drinking water supplies in the United States. However, over the years, in this country and others a number of intentional contamination events and a number of threats have occurred involving foreign and domestic groups, or disgruntled insiders. A large number of cases of vandalism also underscore the vulnerability of drinking water systems.

The following is a summary of some of the threats and incidents of intentional contamination of water, and in some cases food, which have been documented in the open literature. A few reports of other incidents of terrorism have also been included to add historical perspective. Additional cases of intentional contamination of water and food are described in other sections of this chapter and book.

Note that information on some of these cases has been obtained from several open literature reviews including, among others, Purver 1995; Christopher et al. 1997; Falkenrath et al. 1998; Kroll 2006; and Gleick 2008. Another report on previous water-related incidents and threats was compiled by the Awwa Research Foundation (now the Water Research Foundation). Specific information from that particular report (Welter et al. 2003) has not

been included in this handbook because the report has been categorized as proprietary and confidential by the publisher. Copies of this sensitive report are available to water utilities by request through the American Water Works Association (AWWA).

Assyria, 6th century BC—Assyrians poisoned the wells of their enemies with rye ergot (Eitzen and Takafuji 1997).

Athens, 430 BC—During the Peloponnesian War, Athenians accused the Spartans of poisoning the cisterns of the Piraeus, the source of most of Athens' water (Strategy Page 2006).

Ancient Rome—Nero eliminated his enemies with cherry laurel water. Cyanide is the chief toxic ingredient in this substance (Sidell et al. 1997).

Kaffa, 1346—The Tartar army catapulted the bodies of dead plague victims over the walls of the besieged city of Kaffa, in what is now Feodosia, Ukraine. An epidemic of plague followed within the city. Subsequently, ships carrying plague-infected refugees and rats sailed to Constantinople, Genoa, Venice, and other Mediterranean ports, possibly contributing to the great plague pandemic of 1348 (Derbes 1966).

Pittsburgh, 1763—During the Pontiac rebellion in 1763, the British Army provided blankets from the smallpox hospital at Fort Pitt to Delaware Indians loyal to the French. Subsequently, an outbreak of smallpox occurred among the Indians (Christopher et al. 1997).

American Civil War, 1864—Confederate soldiers shot and left farm animals to rot in ponds during Sherman's march to the sea, thereby depriving the Union Army of drinking water (Sidell et al. 1997).

World War I, 1914 to 1918—The German military developed and utilized biological agents to infect livestock and contaminate animal feed. In 1915, a German-American doctor in the United States, with the support of the Imperial German government, produced a quantity of *B. anthracis* (anthrax) and *Burkholderia (pseudomonas) mallei* (glanders) that was used to infect 3,000 horses, mules, and cattle being sent to the Allies in Europe (Christopher et al. 1997).

World War II, 1939 to 1945—The Japanese military used biological agents in the Soviet Union, Mongolia, and China. Japan's Imperial Unit 731, a biological warfare research facility under the direction of Dr. Ishiro Ishii, tested biological weapons on 3,000 prisoners of war. As many as 1,000 of these prisoners died from infections caused by anthrax, botulism, brucellosis, cholera, and plague. Japan also attacked at least 11 Chinese cities with biological agents. This included attacks on water and food supplies with *B. anthracis*, *Vibrio cholerae*, *Shigella* spp., *Salmonellae* spp., and *Y. pestis* (Christopher et al. 1997). In Ning Bo, China, birthplace of Chiang Kai-shek, contamination of drinking water involved dumping of pathogens into water reservoirs, ponds, and individual residential wells. Allegedly more than 1,000 persons became ill, and more than 500 people died (Harris 1994). The actual impact on public health is difficult to verify. In 1949, one former participant in the Japanese biowarfare program estimated that the Japanese facilities

could produce, on a monthly basis, 300 kg of plague bacteria, 500 to 600 kg of anthrax bacteria, 800 to 900 kg of typhoid/paratyphoid bacteria, or as much as 1,000 kg of cholera bacteria.

World War II, 1939 to 1945—Nazi Germany reportedly landed a sabotage team in the United States with a mission to attack a drinking water system. The mission failed (Grigg 2003).

World War II, 1939 to 1945—In 1945, the desperate, retreating German Army polluted a large drinking water reservoir in northwestern Bohemia with raw sewage (Christopher et al. 1997).

Post World War II, 1946—One of the most lethal terrorist attacks of the last century involved arsenic poisoning of SS soldiers interned in a US prisoner-of-war camp outside Nuremberg, Germany in April 1946. A Jewish group intent on vengeance, Nakam, infiltrated the bakery that supplied bread to the camp and spread an arsenic-based poison on the loaves. It was estimated that hundreds of prisoners died and thousands became ill (Khan et al. 2001).

Post World War II, 1946 to 1989—A number of nations operated biological weapons programs. The United States ended its weapons program in 1969. England and Canada ended their programs shortly thereafter. In 1972, 140 nations signed the Biological and Toxin Weapons Convention. However, the Soviet Union continued to develop and stockpile biological weapons through the late 1980s. At least 10 other nations also expanded their efforts during this same period. There is concern that former researchers and weapons from the Soviet program may have ended up in the hands of other nations and terrorist groups (Osterholm 2001).

Chicago, 1972—Members of the Order of the Rising Sun, an American fascist organization dedicated to creating a new master race, were found to be in possession of 30 to 40 kg of *S. typhi* culture (which causes typhoid fever). The organization allegedly planned to introduce the bacteria into the water supplies of Chicago, St. Louis, and other cities (Purver 1995; Falkenrath et al. 1998). One of the two individuals charged with conspiracy to commit murder was a college student who had developed the bacterial culture in a school laboratory.

Pittsburgh, 1980—A perpetrator injected the pesticide chlordane into an 18-in.-diameter drinking water transmission main feeding a neighborhood in Pittsburgh. Fortunately, the chlordane was dissolved in a kerosene base, a common practice used by exterminators at that time. Because of the strong kerosene odor, few people actually ingested the contaminated tap water. Even so, 150 people reported becoming ill. While no one was ever arrested, the culprit was believed to be an insider who had knowledge of the location of a pitometer pit used to inject the contaminant and who may have been part of a labor dispute occurring at the water company at that time. This is believed to be the most significant case of intentional contamination of drinking water ever to have occurred in the United States (Moser 2005).

The incident is discussed in greater detail in the recovery chapter of this book (chapter 18) because the remediation effort has been well documented.

Oregon, 1984—A total of 751 people came down with *Salmonella* gastroenteritis in The Dalles, Oregon, a small town of approximately 10,500 residents (*The Oregonian* 1985; Fitzgerald 1986; Torok et al. 1997). Although there were no fatalities, 45 of the victims were hospitalized. Intense epidemiological investigations by several health departments and the US Centers for Disease Control and Prevention implicated food consumption at restaurants in the town. However, it was not until more than a year after the outbreak that a criminal investigation and a suspect's confession confirmed suspicions that the source of the epidemic was intentional contamination of food. This episode illustrates the difficulty of differentiating biological attacks from naturally occurring epidemics.

A religious sect, followers of an Indian guru named Bhagwan Shree Rajneesh, had purchased a ranch in Wasco County where The Dalles is located. Disputes over land use at the religious commune led followers to believe that the November election would be important for the future development of their commune. In an effort to reduce voter turnout and influence the election, several members of the cult intentionally contaminated salad bars in 10 restaurants in the town with the bacterium *S. typhimurium*. Liquid cultures of *S. typhimurium* were prepared from a standard strain of the bacterium that had been purchased from a commercial supplier of biological products prior to the outbreak. The criminal investigation indicated that the liquid culture was poured, in some cases on more than one occasion, onto the restaurant salad bars. In some restaurants, the bacteria was also added to coffee creamers. Additionally, produce in at least one supermarket was contaminated. In another event involving this same group, three county commissioners visiting the religious compound were deliberately infected, apparently with *Salmonella* in contaminated glasses of drinking water. Two of the commissioners became ill and one almost died.

Upon questioning, the perpetrators revealed that plans had been made to contaminate the city water supply. Some trial contamination attempts were allegedly carried out that involved dumping sewage and dead rodents into a distribution system storage tank for the town's drinking water supply.

Arkansas, 1985—The FBI discovered that a white supremacist group in the Ozark Mountains known as "The Covenant, The Sword, and the Arm of the Lord" had acquired a drum containing 30 gal of potassium cyanide. Their stated intent was to poison water supplies in New York, Chicago, and Washington, D.C. (Tucker 2000).

New York City, 1985—During the controversial trial of subway shooter Bernard Goetz, an anonymous threatening letter was sent to the New York City mayor's office. The letter indicated that if the defendant was not released, the drinking water supply of New York City would be contaminated with "substantial quantities" of plutonium. Subsequent analyses performed by the US Department of Energy revealed radiation associated with plutonium at levels

of 20 femtocuries in several samples of drinking water, as compared with a normal background of less than 1 femtocurie. Although a person would have had to drink several million liters of the contaminated water to acquire a lethal dose, estimated at 100 microcuries, the finding suggested that portions of the public water supply had been intentionally contaminated with a radionuclide (*Time Magazine* 1985). A femtcurie is nine orders of magnitude less than a microcurie.

Duquesne, Pa., 1986—Two treatment plant operators were arrested for intentionally dumping 100 lb of a drinking water treatment chemical, potassium permanganate, into the clearwell of their small town's drinking water plant. While no one was injured, the town's drinking water turned purple in color, causing a great deal of consternation among residents. The reported motive for the disgruntled employees' actions was to underscore potential vulnerabilities that could result from recent utility staff reductions (Ownbey et al. 1988).

Philippines, 1987—A pesticide was used to intentionally contaminate drinking water provided in plastic containers to police recruits in Mindanao. The media reported 19 fatalities and 140 illnesses.

Romania, 1989—During the overthrow of the communist regime, Romanian state secret police allegedly poisoned public water supply tanks in the city of Sibiu with a nerve agent. A number of people became ill and some were hospitalized.

Istanbul, 1992—Kurdish terrorists attempted to poison the water supply of a Turkish Air Force compound with potassium cyanide. A cyanide concentration of 50 mg per liter was detected in the water stored in the tanks serving the military base. The plot was discovered before anyone was poisoned. The PKK claimed responsibility for the attack (Chelyshev 1992).

Cambodia, 1996—Khmer Rouge guerillas contaminated village water supplies with pesticide. Seven civilians and eight soldiers reportedly died.

Kosovo, 1998—Yugoslav federal forces or their allies poisoned wells throughout Kosovo. They dumped bodies of Kosovar Albanians, animal carcasses, and hazardous materials (e.g., paint, oil, gasoline) into 70 percent of area wells, deliberately making people sick and denying them use of the wells (Smith 1998).

Angola, 1999—One hundred bodies were found in four drinking water wells in Central Angola (*International Herald Tribune* 1999).

Canton, Ohio, 2002—A former water department employee was charged with poisoning a pair of municipal wells with the organic compound trichloroethylene. During a six-day crisis, thousands of homeowners with private wells were advised not to drink or bathe in their water pending testing of wells and streams by the Ohio Environmental Protection Agency (www.miwater.org/awwa/Whats_New_Archives).

Afghanistan, 2002—US military personnel recovered documents from caves in Afghanistan indicating that al-Qaida had assessed American drinking water distribution networks, pump stations, and other assets as possible targets for sabotage.

Paris, 2002—Al-Qaida operatives were arrested with plans to attack the water supply network in the Eiffel Tower neighborhood of Paris (Kroll 2006).

Jordan, 2003—Iraqi agents reportedly plotted to poison a water tank that served US troops in Khao, Jordan. They were arrested by Jordanian authorities before they could carry out the attack (Feuer 2003).

China, 2003—In an effort to promote sales, a home water purification device salesman dumped approximately 500 mL of an unnamed pesticide into a drinking water reservoir in Henan Province. The reservoir supplies 9,000 homes. No deaths were reported but 64 people were sickened and 42 of these individuals were hospitalized (BBC 2003).

Saudi Arabia, 2003—Al-Qaida threatened US water systems in a call to a Saudi Arabian magazine. The threat included the statement that al-Qaida does not “rule out...the poisoning of drinking water in American and Western cities” (Associated Press 2003b, Waterman 2003).

Italy, 2003—An unknown assailant and possibly one or more copycats injected detergent, bleach, and acetone into plastic-bottled water on store shelves. Using a syringe, the perpetrators injected the contaminants just below the cap where the puncture hole would be difficult to detect. Twelve people were hospitalized (www.cnn.com/2003/WORLD/europe/12/09/italy.water.rent/index.html).

Iraq, 2007—Several terrorist attacks were carried out involving improvised explosive devices combined with chlorine tanks on trucks, resulting in numerous injuries and fatalities. The source of the chlorine used in the attacks was chlorine gas cylinders diverted from their use at water treatment facilities (Kazim 2007).

California, 2007—Four separate instances of theft or tampering with chlorine gas containers were reported at water treatment plants in southern California from February to April. The successful thefts involved 150-lb cylinders, but one incident involved the attempted theft of a 1-ton container (Welter 2009).

Canada, 2007—A Toronto man, previously accused of sending three letter bombs, was charged with eight more counts of attempted murder after allegedly tampering with bottled water, which had been injected with an unspecified chemical. Cases of the complimentary bottled water were sent to two Toronto agencies that the suspect had a relationship with (*Toronto Star* 2007).

Pakistan, 2008—Pakistani police arrested five Sunni militants who planned to use cyanide powder to poison water in Karachi during the Shiite Muslim festival of Ashura. Police reported that “the aim was to cause widespread human losses.” Police recovered 500 g of cyanide that the extremists planned to mix with water distributed at kiosks established for the festival (*Wall Street Journal* 2008).

Pakistan, 2009—The Water and Sanitation Agency of Pakistan was directed to stop supplying water to the city of Multan from storage tanks

after receiving information that the Pakistani Tehreek-e-Taliban had obtained large quantities of poison to contaminate the city's water supply. The water authority was instructed to pump water directly through tube wells. (*Daily Times*, 2009).

REFERENCES

- Abel, D., and M. Naughton. 2007. Spencer Water Supply Contaminated: 93 Treated at Hospitals after Plant Malfunction. *The Boston Globe*, April 26.
- Allman, T., and K. Carlson. 2005. Modeling Intentional Distribution System Contamination and Detection. *Jour. AWWA*, 97(1):58.
- Associated Press. 2003a. Incendiary Devices Placed at Michigan Water Plant. Associated Press, September 25. New York.
- Associated Press. 2003b. Water Targeted, Magazine Reports. Associated Press, May 29. New York.
- Associated Press. 2006. Explosion at Water Line Affects Potable Water Supply to Sri Lankan Capital. Associated Press, December 7. New York.
- Associated Press. 2007. Gas Tanker Blast Kills Nine in Iraq. Associated Press, February 21. New York.
- Berger, B.B., and A.H. Stevenson. 1955. Feasibility of Biological Warfare Against Public Water Supplies. *Jour. AWWA*, 47(2):101.
- Bernosky, J. 2005. Distribution System Security. *Distribution System Water Quality Challenges in the 21st Century: A Strategic Guide*. Denver, Colo.: American Water Works Association.
- Blaser, M.J., and L.S. Newman. 1982. A Review of Human Salmonellosis: Infective Dose. *Rev. Infect. Dis.*, 4(6):1096.
- Boudreaux, R. 2002. Italy Nabs 4 Terror Suspects Plotting Poison Attack. *Los Angeles Times*, February 20.
- British Broadcasting Company (BBC). 2003. China Salesman "Poisoned Water." BBC News, October 6. London.
- Bundesen, H.N., J.I. Connolly, I.D. Rawlings, A.E. Gorman, G.W. McCoy, and A.V. Hardy. 1936. Epidemic Amebic Dysentery. *Nat. Inst. Health Bull.*, No. 166.
- Burrows, W.D., and S.E. Renner. 1998. *Biological Warfare Agents as Potable Water Threats*. U.S. Army Combined Arms Support Command: Fort Lee, Va.
- Burrows, W.D., and S.E. Renner. 1999. Biological Warfare Agents as Threats to Potable Water. *Environ. Hlth. Perspectives*, 107(12):975.
- Byer, D. and K.H. Carlson. 2005. Real-Time Detection of Intentional Chemical Contamination in the Distribution System. *Jour. AWWA*, 97(7):130.
- Chang, K., and W.J. Broad. 2006. It's Not Hard to Use Fluids to Cause an Explosion on a Plane, Chemists Say. *New York Times*, August 11.
- Chelyshev, A. 1992. Terrorists Poison Water in Turkish Army Cantonment. Telegraph Agency of the Soviet Union (TASS), March 29. Moscow.
- Christian Science Monitor*. 2000. Ecoterrorism as Negotiating Tactic. *Christian Science Monitor*, July 1.
- Christopher, G.W., T.J. Cieslak, J.A. Pavin, and J. Eitzen. 1997. Biological Warfare: A Historical Perspective. *JAMA*, 278(5):112.
- Clark, R.M., and R.A. Deininger. 2000. Protecting the Nation's Critical Infrastructure: The Vulnerability of U.S. Water Supply Systems. *Jour. Contingencies and Crisis Mangmt.*, 8(2):73.
- Corso, P.S., M.H. Kramer, K.A. Blair, D.G. Addiss, J.P. Davis, and A.C. Haddix. Cost of Illness in the 1993 Waterborne *Cryptosporidium* Outbreak, Milwaukee, Wisconsin. *Emerg. Infect. Diseases*, 9:4.
- Cowell, A. 2005. Police Name 2 of 4 Men Linked to Bomb Attempts. *New York Times*, July 26.
- Daily Times*. 2009. Multan Suspends Water Supply From Tanks Amid Poisoning Fears. *Daily Times* (Pakistan), November 12.
- Deininger, R.A. 2000. The Threat of Chemical and Biological Agents to Public Water Supply Systems. Report prepared for Science Applications International Corporation (SAIC), McLean, Va.
- DeLeon, R. and M. Stewart. 2000. Evaluation of Vulnerability to Microbial Threats. *Proc. 2000 AWWA WQTC*. Denver, Colo.: AWWA.

- Derbes, V.J. 1966. De Mussis and the Great Plague of 1348: A Forgotten Episode of Bacteriological War. *JAMA*, 196:59.
- Downie, L. 1978. Jonestown Story Grew Uglier with Each Chapter. *Washington Post*, November 26.
- Eitzen, E., J. Pavlin, T. Cieslak, G. Christopher, and R. Culpepper. 1998. *Medical Management of Biological Casualties Handbook*, 3rd ed. Ft. Detrick, Md.: U.S. Army Medical Research Institute of Infectious Diseases.
- Eitzen, E.M. and E.T. Takafuji. 1997. Historical Overview of Biological Warfare. *Textbook of Military Medicine, Medical Aspects of Chemical and Biological Warfare*. Washington, D.C. Office of the Surgeon General, Department of the Army.
- Falkenrath, R.A., R.D. Newman, and B.A. Thayer. 1998. *America's Achilles' Heel; Nuclear, Biological and Chemical Terrorism and Covert Attack*. Cambridge, Mass.: MIT Press.
- Feuer, A.. 2003. Iraqi Agents Held in Plot to Poison Water Supply. *New York Times*, April 1.
- Financial Times Global Water Report (FTGWR)*. 1999. Zambia: Water Cutoff. *FTGWR*, March 19.
- Fitzgerald, F. 1986. *Cities on a Hill: A Journey through Contemporary American Cultures*. New York: Simon and Schuster.
- Garland, J. 1991. *Water Vulnerability Assessments*. AL-TR-1991-0049. Louisville, Ky.: Armstrong Laboratory.
- Gleick, P.H. 2008. Water Conflict Chronology. *Pacific Institute for Studies in Development, Environment, and Security (Database on Water and Conflict)*. Oakland, Calif.
- Government Accountability Office (GAO). 2003. *Drinking Water Security: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*. Report No. GAO-04-29. Washington, D.C.: GAO
- Grigg, N.S. 2003. Water Utility Security: Multiple Hazards and Multiple Barriers. *Jour. Infrastruct. Syst.*, 9(2):81.
- Ha'aretz. 2002. English Edition. September 21.
- Harris, S.H. 1994. *Factories of Death, Japanese Biological Warfare and the American Cover-up*. New York: Routledge.
- Hickman, D.C. 1999. A Chemical and Biological Warfare Threat: USAF Water Systems at Risk. *The Counterproliferation Papers*. Air War College, Maxwell Air Force Base, Ala. www.au.af.mil/au/awc/awcgate/cpc-pubs/hickman.htm.
- Hoover, J.E. 1941. Water Supply Facilities and National Defense. *Jour. AWWA*, 33 (11):1861.
- Hrudey, S.E., and E.J. Hrudey. 2004. *Safe Drinking Water: Lessons from Recent Outbreaks in Affluent Nations*. London: IWA Publishing.
- International Herald Tribune*. 1999. 100 Bodies Found in Well. *International Herald Tribune*, August 14–15.
- Jernigan, J.A. et al. 2001. Bioterrorism-Related Inhalation Anthrax: The First 10 Cases Reported in the U.S. *Emerg. Infect. Diseases*, 7(6):933.
- Kazim, J. 2007. Iraqi Officials Quoted on Probe into Sources of Chlorine Used by Terrorists. April 2, Al-Hayat Website, London, UK. www.redorbit.com/news/science/889353/iraqiOfficials_quoted_on_probe_into_sources_of_chlorine_used/index.html.
- Keefe, R. 2006. Security Lacking in Networks Controlling Critical Infrastructure. *Austin American Statesman*, Oct. 2.
- Khan, A., D. Swerdlow, and D. Juranek. 2001. Precautions Against Biological and Chemical Terrorism Directed at Food and Water Supplies. *Public Health Rep.*, 116:3.
- Kolavic, S.A. et al. 1997. An Outbreak of *Shigella* Dysentery Type 2 Among Laboratory Workers Due to Intentional Food Contamination. *JAMA*, 278(5):396.
- Kroll, D.J. 2006. *Securing Our Water Supply: Protecting a Vulnerable Resource*. Tulsa, Okla.: PennWell.
- Krouse, M. 2001. Backflow Incident Sparks Improvements. *Opflow*, 27(2):1.
- Luthy, R.G. 2002. Bioterrorism and Water Security. *Environ. Sci. & Technol.*, 36, 123A.
- MacKenzie, W.R. et al. 1994. A Massive Outbreak in Milwaukee of *Cryptosporidium* Infection Transmitted through the Public Water Supply. *New England Jour. Med.*, 331(3):161.
- Manahan, S.E. 1992. *Toxicological Chemistry*, (2nd ed.). Boca Raton, Fla.: Lewis Publishers, CRC Press.
- Miller, J. 2003. Poison Found At Post Office; No Tie is Seen to Terrorism. *New York Times*, October 23.

- Moser, G. 2005. Purposeful Contamination of Distribution System with Chlordane Affecting 10,000 People. *Proc. 2005 AWWA Water Security Congress*, Oklahoma City, Denver, Colo.: AWWA.
- Mueller, R. 2003. Testimony before the Senate Select Committee on Intelligence Hearing on Worldwide Threats to the Intelligence Community, February 11. Washington, D.C.
- Mullins, W.C. 1992. An Overview and Analysis of Nuclear, Biological, and Chemical Terrorism: The Weapons, Strategies and Solutions to a Growing Problem. *Amer. Jour. Criminal Justice*, 16(2):95.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academies Press.
- NRC. 2001. *Guidelines for Chemical Warfare Agents in Military Field Drinking Water* (1995). Washington, DC.: National Academies Press.
- Newman, C. 2005. Poison, 12 Toxic Tales. *Nat. Geog.*, 207(5):2.
- Office of Technology Assessment (OTA), US Congress. 1993. *Proliferation of Weapons of Mass Destruction: Assessing the Risks*. OTA-ISC-559. Washington, D.C.: US Government Printing Office.
- The Oregonian*. 1985. Portland, Ore. September 21.
- Osterholm, M.T. 2001. Bioterrorism: a Real Modern Threat. *Emerging Infections* 5. Washington, D.C.: ASM Press.
- Ownbey, P.J., F.D. Schaumburg, and P.C. Klingeman. 1988. Ensuring the Security of Public Water Supplies. *Jour. AWWA*, 80(2):30. Denver, Colo.
- Pittsburgh Press*. 1988. Spill Threatens Water Supply of 150,000. *Pittsburgh Press*, January 5.
- Porter De Nileon, G. 2001. The Who, What, Why, and How of Counterterrorism Issues. *Jour. AWWA*, 93(5):78.
- Presidents Commission on Critical Infrastructure Protection. 1996. *Critical Foundations: Protecting America's Infrastructure*. Washington, D.C. www.pccip.gov.
- President's Critical Infrastructure Assurance Office. 1998. *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*. Washington, D.C. http://cioa.gov/roadmap-e.pdf.
- Purver, R. 1995. *Chemical and Biological Terrorism: The Threat According to the Open Literature*. Canadian Security Intelligence Service (unclassified). Toronto, Ont., Canada.
- Ramsay, C.N., and J. Marsh. 1990. Giardiasis Due to Deliberate Contamination of Water Supply. *Lancet*, 336, 880.
- Reuters. 1995. Champagne au Cuanure: 15 Morts et 53 Hospitalise, Selon un Nouveau Bilan. Reuters North American Wire, January 2.
- Rich, V. 1992. Anthrax in the Urals. *Lancet*, 339, 419.
- Rizzo, T. 1996. Green Gets Life Sentence. *Kansas City Star*, May 31.
- Rose, J.B. 2002. Water Quality Security. *Envir. Sci. & Technol.*, 36, 247A.
- Rose, L.J., E.W. Rice, B. Jensen, R. Murga, A. Peterson, R.M. Donlan, and M.J. Arduino. 2005. Chlorine Inactivation of Bacterial Bioterrorism Agents. *Appl. Environ. Microbiol.*, 71(1):566.
- Science. 1966. Deliberate Spreading of Typhoid in Japan. *Science*, 2, 11.
- Sidell, F.R., E.T. Takafuji, and D.R. Franz. 1997. *Medical Aspects of Chemical and Biological Warfare*. Washington, D.C.: Borden Institute.
- Smith, R.J. 1998. Poisoned Wells Plague Towns All Over Kosovo. *Washington Post*, December 9.
- Strategy Page. 2006. www.stategypage.com/articles/biotoxin_files/BIOTOXININWARFARE.asp
- Suskind, R. 2006a. *The One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11*. New York: Simon and Schuster.
- Suskind, R. 2006b. Al-Qaeda Cell Planned to Attack Subway with Poison Gas, Says New Book. *Time Magazine*, June 20.
- Tierney, J., and R.F. Worth. 2003. Attacks in Iraq May be Signals of New Tactics. *New York Times*. August 18.
- Time Magazine*. 1985. New York City's Plutonium Scare. *Time Magazine*, August 5.
- Time Magazine*. 2007. Can We Spot the Threat? *Time Magazine*, July 16.
- Torok, T.J. et al. 1997. A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars. *JAMA*, 278(5):389.
- Toronto Star*. 2007. Man Faces Attempted Murder Charge Over Water. *The Toronto Star*, November 6.
- Tucker, J.B. 2000. *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. Cambridge, Mass.: MIT Press.

- US Army Center for Health Promotion and Preventive Medicine. 1998. Biological Warfare Agents as Potable Water Threats. Medical Issues Information paper no. IP-31-017. Aberdeen Proving Ground, Md.
- US Environmental Protection Agency (USEPA). 2002. Potential Contamination Due to Cross-Connections and Backflow and the Associated Health Risks: An Issues Paper. Washington, D.C. www.epa.gov/ogwdw/tcr/pdf/ccrwhite.pdf.
- Wall Street Journal*. 2001. Water Utility Officials Fear Backflow from Terrorists. *Wall Street Journal*, December 27.
- Wall Street Journal*. 2008. Pakistan Arrests 5 Suspected of Planning Cyanide Attack. *Wall Street Journal*, January 19.
- Waterman, S. 2003. Al-Qaida Threat to US Water Supply. *United Press International*, May 28.
- Watson, A., and D. Keir. 1994. Information on Which to Base Assessments of Risk from Environments Contaminated with Anthrax Spores. *Epidemiol. Infect.*, 113, 479.
- Welter, G.J. 2009. One Perspective on Chlorine Security. *Jour. AWWA*, 101(1):36.
- Welter, G.J., G.B. Best, and K.L. Moran. 2003. *Actual and Threatened Security Events at Water Utilities*. Denver, Colo.: Awwa Research Foundation.
- Whelton, A.J., J.L. Jensen, T.E. Richards, and R.M. Valdivia. 2003. The Cyanic Threat to Potable Water. *Proc. 2003 AWWA Annual Conf.* Denver, Colo.: AWWA.
- World Health Organization (WHO). 1970. *Health Aspects of Chemical and Biological Weapons*. Geneva, Switzerland: WHO.
- WHO. 2004. *Public Health Response to Biological and Chemical Weapons: WHO Guidance*. Geneva, Switzerland: WHO. www.who.int/csr/delibepidemics/biochemguide/en/index.html.
- Yardley, J. 2005. Rural Water Worries Persist After Chinese Chemical Spill. *New York Times*, November 27.

THE THREAT TO WASTEWATER SYSTEMS

WHY WASTEWATER SYSTEMS MIGHT BE TARGETED

The wastewater industry plays a critical role in protection of public health and the environment. Wastewater systems collect, treat, and safely dispose of sanitary waste, industrial waste, and stormwater runoff. With water becoming a scarcer commodity, especially in arid regions and areas of high population growth, wastewater utilities are reclaiming more and more wastewater that in the past was simply considered a nuisance material to be disposed of in the cheapest manner possible.

Most people would generally agree that drinking water systems are potentially a target of terrorism. The idea that a wastewater system might also be the target of an intentional malevolent act is less commonly accepted. However, the following observations support this possibility:

- Wastewater systems are a major part of a country's infrastructure. There are 16,000 public wastewater systems in the United States, serving communities ranging from housing developments to the largest cities.
- Interruption in the ability to effectively remove and treat sanitary waste would significantly affect public health and the environment. Loss of wastewater collection and treatment facilities could also result in restrictions on commercial and industrial activities. These impacts would cause a major disruption in daily life for the affected population.

- Wastewater systems have many components and are widespread geographically, making them difficult to protect. Many facilities, such as lift stations, are unmanned. Additionally, with manholes and stormwater catch basins located every several hundred feet throughout urban areas, the collection network is very susceptible to intrusion.
- Like drinking water utilities, wastewater utilities, whether municipally or investor owned, are perceived as being associated with the government. This could make wastewater facilities a political target.

As mentioned in the previous chapter on drinking water utilities, the probability of a specific wastewater system becoming the target of an act of terrorism is quite remote. However, the possibility of a wastewater system somewhere becoming the direct or indirect target of terrorism is real. Additionally, as in the case of drinking water systems, wastewater utilities can certainly become the target of a disgruntled employee. They could also be the target of simple vandalism, which in today's climate must be investigated to ensure that the incident is not terrorism. And, of course, wastewater systems are vulnerable to emergencies resulting from natural or accidental causes.

One of the reasons less attention has been directed toward protecting wastewater systems than drinking water systems is likely because damage to a wastewater systems represents more of an environmental threat (i.e., release of untreated sewage) than a direct threat to public safety. However, as indicated in the following discussion of possible scenarios, intentional or accidental incidents affecting wastewater utilities can endanger public health and safety.

SCENARIOS OF CONCERN

A number of scenarios can be identified for malicious acts directed toward wastewater systems.

A car bomb, truck bomb, or an incendiary device could be used to damage wastewater facilities such as the treatment plant or lift stations. Alternatively, a weapon could be fired at a facility from a distance. The goal would be to destroy physical assets, cause economic damage, undermine public confidence in the ability of the government to protect the community, and perhaps negatively impact public health.

Flammable or explosive substances could be introduced into the collection system through a manhole, inlet, or even a building drain or cleanout. The level of sophistication for this scenario could be as simple as the theft of a gasoline tanker truck and injection of its contents into a catch basin. Such an incident would not only damage wastewater infrastructure but also other underground utilities, such as gas, electric, and drinking water.

Incendiary or explosive devices could be placed in the sewage system, essentially turning the system into a pipe bomb to attack targets such as high profile buildings, stadiums, and public events. Explosions in sewers can cause the collapse of roads, sidewalks, and adjacent structures and injure or kill people nearby. Several events, some accidental and some intentional,

are described in a later section dealing with incidents and threats that have already occurred in wastewater systems.

Toxic substances could be added to the wastewater collection system or treatment plant. One scenario includes the use of delivery vehicles, including septic tankers, to introduce toxic chemicals or hazardous waste directly into treatment facilities. The safety of utility employees or individuals in the surrounding community may be jeopardized if harmful vapors or aerosols are released. Toxins could also damage microorganisms used in the treatment process, shutting down treatment. If not removed by treatment, the toxins could potentially pass through the plant and negatively impact the environment and downstream users of receiving waters.

Approximately 40 percent of almost 300 wastewater treatment plants that responded to a survey conducted by the Water Environment Federation (WEF) (2004) indicated that they were currently using chlorine gas for disinfection of treated effluents. Intentional or accidental release of chlorine gas from 150 lb bottles, 1-ton cylinders, 55-ton railroad cars, or 90-ton railroad cars at a facility, or en route to a facility, could be lethal for publicly owned treatment works (POTW) employees and residents in the surrounding area. Theft of commonly used 150-lb bottles of gaseous chlorine and subsequent release in a mall or other crowded site could also produce disastrous results. Other dangerous treatment chemicals available in some wastewater plants include ammonia and sulfur dioxide. Anecdotally, at the time of the Pentagon attacks on 9/11, a string of railroad cars filled with gaseous chlorine intended for the Blue Plains Wastewater Treatment Works sat idle on a rail spur across the Potomac River (NRC 2002). Had these cars, rather than the Pentagon, been struck by the hijacked plane, it is conceivable that the number of casualties in downtown Washington, D.C. may have been even greater than those that occurred among workers in the Pentagon.

Many wastewater utilities utilize SCADA systems to operate collection and treatment facilities. Vandals or terrorists hacking into these systems could cause overflows or interrupt treatment processes, creating back-ups. Another potential cyber target is administrative functions. The loss of information systems for customer billing and service presents a potentially costly vulnerability.

Sewer lines vary from 4 inches to 20 feet in diameter. Large diameter sanitary, storm, or combined sewers are easily accessible by manholes, inlets, and overflow structures and could serve as conduits that could enable an adversary to pass undetected beneath city streets. Collection systems may provide unrestricted access to government buildings, financial centers, public gatherings, and other high-profile targets.

Wastewater utilities, like drinking water utilities, have critical interdependencies with other infrastructures. An accidental power failure or an attack on the electrical grid, which supplies power to the treatment plant and pumping stations, could put a wastewater system out of commission for an extended period of time. Disruption of transportation networks that supply

treatment chemicals to wastewater plants would also impede wastewater operations. During the August 2003 electricity blackout in the northeastern United States, wastewater treatment plants in Cleveland, Detroit, New York, and other locations that lacked adequate backup generation systems lost power and discharged millions of gallons of untreated sewage to receiving waters (Congressional Research Service 2005).

Finally, wastewater utilities could inadvertently be significantly affected by events involving other facilities in the community. If the public drinking water supply is accidentally or intentionally contaminated, the contaminated water ultimately ends up in the wastewater system through normal use or remedial flushing of the drinking water system. Additionally, during the cleanup of an intentional contamination of a government building or other facility, wastewater systems may be asked to accept decontamination residue, or chemical, biological, or radiological contaminants may be washed into wastewater or stormwater systems by emergency response personnel. In reality, becoming the indirect target of a terrorist attack may be the most likely terrorism scenario of concern for wastewater systems.

CONTAMINATION ENDPOINTS OF CONCERN

Several endpoints of concern could result from intentional or accidental, contamination events in wastewater systems. The primary concern is that a contamination incident could threaten the health or safety of utility workers or the public. This could be the case if flammable, explosive, toxic, or infectious substances found their way into the sanitary or stormwater collection network, or the treatment plant.

Another potential problem is that contaminants introduced into the wastewater system could pass through the treatment plant and negatively affect the aquatic environment or downstream users such as drinking water plants located on receiving bodies of water. Still another possibility is that toxic contaminants could damage the microbial flora that is a key component of secondary treatment and thereby impair the ability of the POTW to effectively treat wastes. Re-establishment of effective secondary treatment could require weeks or months. Finally, there is a concern that flammable or explosive agents could seriously damage the wastewater infrastructure, or tough-to-remove radionuclides, bacterial spores, or other recalcitrant contaminants could make components of the infrastructure difficult or impossible to decontaminate. In this case, remediation or replacement of portions of the system would be extremely expensive.

DOCUMENTED INCIDENTS IN WASTEWATER SYSTEMS

As in drinking water utilities, wastewater utilities have experienced their share of vandalism over the years. While no reports of terrorist acts directed

toward wastewater systems appear in the literature, the potential damage that could be caused by such incidents is amply demonstrated by reports of several accidents and several intentional acts that have occurred over the past several decades.

Louisville, Ky., 1977—A classic example of damage from the injection of a toxic substance into a wastewater system occurred in Louisville. Workers at the Morris Forman Wastewater Treatment Plant reported a strong chemical odor that was making them ill. The US Army sent teams wearing protective gear into the sewers to find the source of the chemicals. The FBI also joined the search. After more than a week of investigation it was determined that the odor was coming from a mixture of hexachloropentadiene and octachlorocyclopentene, two highly toxic compounds used in the manufacture of pesticides. The chemicals had been illegally discharged into a manhole in the sewage collection system by a local chemical disposal company improperly disposing industrial waste. The contaminated POTW had to be shut down for several months, and during that period, all the raw sewage (100 mgd) was bypassed directly to the Ohio River. The sewer line carrying the waste to the treatment plant required an additional two years for remediation. During this period, raw sewage from the line was shunted around the treatment plant and into the river. The disposal company president and two employees were found guilty of polluting a waterway and the president was sentenced to two years in prison. In 1983, the companies responsible for sending the waste to the disposal company agreed to pay the Metropolitan Sewer District \$1.9 million for the medical expenses of employees and the costs of cleaning up the sewers and the treatment plant (www.msdlouky.org/aboutmsd/history20.htm).

Louisville, Ky., 1981—An accidental introduction of explosive materials into a sewage collection system also occurred in Louisville. In February 1981, two women going to work at a hospital were driving under an overpass on Hill Street when a huge explosion hurled their car into the air and onto its side. At the same time, officers in a police helicopter heading toward the downtown area observed a series of explosions “like a bombing run” erupting along the streets of Louisville and through the University of Louisville campus. More than 2 miles of street were pockmarked with craters where manholes had been. Several blocks of Hill Street fell into the collapsed 12-foot-diameter sewer line (Figure 3-1). Fortunately, no one was seriously hurt, but homes and businesses were extensively damaged and a number of people had to be evacuated. Louisville was in the national headlines for several days.

The cause of the explosion was traced to a soybean processing plant southeast of the university campus, where thousands of gallons of the highly flammable solvent hexane had accidentally spilled into the sewer system. The hexane fumes were apparently ignited by a spark from the car that the women drove under the overpass. It took 20 months to repair the sewer lines, and another several months to repair the streets. While the chemical release was accidental, the responsible company pled guilty to four counts of violating environmental laws and paid a fine of \$62,500. The company also agreed to



Courtesy of *The Courier Journal*, Louisville, Ky.

Figure 3-1. Hill Street, Louisville, Ky., 1981

pay the Metropolitan Sewer District more than \$18 million in damages. Many millions more were paid to other government agencies and private individuals who had suffered damages (www.msdlouky.org/aboutmsd/history20.htm).

Akron, Ohio, 1977—An intentional, malevolent injection of a flammable substance into the collection system resulted in a series of sewer explosions in this city. A police investigation revealed that at least 3,000 gal of petroleum naptha and isopropyl alcohol had been dumped into the sewer during the night by vandals at a strikebound rubber company. Officials theorized that when the material entered the sewer it was too rich to ignite, but as it flowed further into the system it became diluted to explosive range and finally ignited 3.5 miles from the point of injection. Approximately 1 mile of sewer line was damaged. Damage estimates exceeded \$10 million.

Queensland, Australia, 2000—An intentional cyber attack occurred at a wastewater utility soon after a contractor completed a major upgrade of a plant SCADA system. A former employee of the contractor was upset over not having been hired directly by the utility following completion of the contract. With his insider knowledge of the computer system, and using a wireless connection and a stolen computer, the frustrated job applicant was able to hack into the utility's SCADA system 46 times during a 10-week period. On some



Courtesy of *The Disaster Recovery Journal*

Figure 3-2. Guadalajara, Mexico, 1992

of these occasions the hacker was able to shut down pumps. During one incident, the perpetrator caused the overflow of thousands of gallons of raw sewage into a river, into a park, and onto the grounds of a hotel. The attack resulted in a cleanup costing \$26,000 US. The perpetrator was subsequently arrested, sent to prison for two years, and ordered to reimburse the expense associated with the cleanup efforts (Kroll 2006).

Louisiana, 2003—One or more individuals attempted to steal anhydrous ammonia from a wastewater treatment facility. Anhydrous ammonia is a component in the manufacture of illegal drugs such as methamphetamines. The attempted theft resulted in a serious ammonia leak at the plant.

Guadalajara, Mexico, 1992—A particularly tragic accident occurred in Mexico's second largest city in April 1992. There were nine separate explosions over a four-hour period in the sanitary sewage collection system. The cause of the explosions was gasoline leaking from the state-run Pemex underground pipeline into the sanitary sewer collection lines. Residents in the Reforma district of the city had complained for three days about a strong, gasoline-like odor wafting up from the sewer drains. Officials could not find a leak, did not order an evacuation, and called off their investigation several hours before the explosions began.

The explosions killed 206 people and injured 1,460; damaged 1,148 buildings; destroyed 250 businesses and 500 vehicles; left 15,000 people homeless; and forced the evacuation of 25,000 people for fear of additional explosions. Seven miles of sewer pipe exploded, some of which was 18 feet in diameter. The event gouged a 20-foot-deep trench along sewer mains in a 20-block area in the downtown section of the city (Figure 3-2). A number of victims were apparently buried alive. Numerous vehicles were buried or toppled into the ditches. Damage costs were estimated at \$75 million US. Investigators eventually concluded that the ultimate cause of the sewer explosions was the faulty installation of a water pipe several years earlier, which leaked water onto a gasoline line lying underneath. The subsequent corrosion of the gasoline pipeline, in turn, caused leakage of gasoline into the sewers

(Eisner 1992, *Time Magazine* 1992, Dugal 1999, Suburban Emergency Management Project 1996).

Conroe, Texas, 1994—The owner of a gas station-convenience store learned that his 8,000-gallon underground gasoline storage tank was cracked and groundwater was infiltrating the tank. Rather than dispose of the diluted gasoline properly, the business owner rented a small pump and intentionally discharged a mixture of approximately 5,000 gallons of gasoline and 500 gallons of water onto the street in front of his store. The gasoline-water mixture entered both the sanitary and stormwater collection systems and essentially formed the equivalent of a 3-mile-long pipe bomb. Fortunately, there was no explosion. However, several schools were evacuated the next day as a precaution. The gasoline in the stormwater collection system flowed into a creek. Utility officials were able divert the gasoline from the sanitary sewer collection system to a lagoon to protect the wastewater treatment plant. The perpetrator was prosecuted for violations of the federal Clean Water Act (CWA) (McKay 1994).

Hagerstown, Maryland, 2002—Chemicals from an unknown source entered the wastewater treatment plant and destroyed the facility's biological treatment process. The incident resulted in the discharge of million of gallons of partially treated sewage into a major tributary of the Potomac River, less than 100 miles upstream of a drinking water supply intake for the Washington D.C. area (GAO 2006).

Visalia, California, 2006—A small-scale incident in this town illustrates the potential effect of contaminants in the sewer system on individual buildings located above the sewer system. A downtown medical building was shut down for a day when benzene fumes filled the building. Investigators believed that the fumes rose from the sewer system through a vent pipe leading to the medical center's roof and were sucked into the building's heating system. The source of the benzene in the sewer system was not conclusively determined but was attributed to probable illegal chemical dumping. Officials evacuated the building because of concerns over an inhalation risk for occupants (*Visalia Times-Delta* 2006).

Philadelphia, Pa., 2006—A nationally known pharmaceutical company accidentally discharged 25 gal of potassium thiocyanate, a chemical used in production of vaccines and antibiotics, into the Upper Gwynedd Township sewage collection system. A day after the release, employees at the POTW noticed fluctuations in the chlorine levels in treated wastewater discharged to the river. The spill led to a sizable fish kill downstream of the wastewater plant effluent. It was believed that the potassium thiocyanate combined with chlorine injected at the POTW to form cyanogen chloride, a compound highly toxic to fish. The discharge also resulted in the temporary closure of one of the City of Philadelphia Water Department's river intakes (Bauers 2006).

CONCLUSIONS

These accidental and intentional incidents involving wastewater systems underscore the vulnerability of the systems to accidental and malevolent acts. The instances involving injections of toxic, flammable, and explosive substances into sewer systems illustrate the potential risk to public safety, public health, and the wastewater infrastructure, and indicate the large amounts of time and money needed to repair the damage.

REFERENCES

- Bauers, S. 2006. Merck Faces Fish-Kill Probe. *Philadelphia Inquirer*, June 23.
- Congressional Research Service (CRS). 2005. *Terrorism and Security Issues Facing the Water Infrastructure Sector*. CRS Report for Congress. The Library of Congress, April 25. Washington, D.C.
- Dugal, J. 1999. Guadalajara Gas Explosion Disaster. *Disaster Recovery Jour.*, 5(3).
- Eisner, P. 1992. Mexico Reels from Explosion. *Newsday*, 112(22):2.
- Government Accountability Office (GAO). 2006. *Securing Wastewater Facilities: Utilities Have Made Important Upgrades but Further Improvements to Key System Components May be Limited by Costs and Other Constraints*. GAO-06-390. Washington, D.C.
- Kroll, D. 2006. *Securing Our Water Supply: Protecting a Vulnerable Resource*. Tulsa, Okla.: PennWell.
- McKay, P. 1994. Huge Gasoline Spill a Mystery in Conroe. *Houston Chronicle*, January 27, 1994.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academies Press.
- Suburban Emergency Management Project. 2006. The Guadalajara 1992 Sewer Gas Explosion Disaster. *SEMP Biot #356*. www.semp.us/biots/biot_356.html.
- Time Magazine*. May 4 and May 11, 1992.
- Visalia Times-Delta*. 2006. Chemical Fumes Close Clinic. *Visalia Times-Delta*, December 6.
- Water Environment Federation (WEF). 2004. Disinfection Process Survey Summary. *Water Environ. & Technol.*, 16.
- WEF. Security website. Washington, D.C. www.wef.org.

LEGISLATIVE AND REGULATORY ASPECTS OF WATER SECURITY AND EMERGENCY PREPAREDNESS

Water security and emergency preparedness begin at the utility level. Vulnerability Assessments (VAs), emergency response plans (ERPs), and continuity of operations plans (COOPs) are site specific. Emergency response and recovery from accidents, natural disasters, and intentional acts begins with the local community and local government. When local resources are overwhelmed, state and federal assistance come into play.

While the ultimate responsibility for preparing for and dealing with emergencies lies at the local level, a number of federal regulations and directives have been issued, especially since 9/11, that address the protection of drinking water and wastewater systems in the United States. The following is a summary of the key federal documents, including some federal reports, dealing with this subject.

Safe Drinking Water Act

The Safe Drinking Water Act (SDWA) is the primary federal law that assures the quality of the nation's drinking water and regulates the public water supply and its sources. The act was first published in 1974 and was significantly amended in 1986 and 1996. A specific security section, which will be discussed later in this chapter, was added in 2002. Under the SDWA, USEPA is authorized to set standards for drinking water quality. USEPA is also authorized to oversee the states, tribes, and water suppliers that implement these standards.

Federal Water Pollution Control Act (CWA 1972)

The Clean Water Act (CWA) includes regulatory and nonregulatory tools to reduce pollutant discharges into US waterways, finance wastewater treatment facilities, and manage polluted runoff. The CWA authorizes USEPA to implement pollution control programs and to set wastewater standards for industry.

President's Commission on Critical Infrastructure (1996)

In response to attacks within the United States and overseas by domestic and foreign terrorists, the President's Commission on Critical Infrastructure was formed in 1996 to evaluate the vulnerability of US infrastructure (President's Commission on Critical Infrastructure Protection 1996). The Commission evaluated the vulnerability of the following infrastructure categories to internal and external terrorism:

- Information and communication
- Physical distribution
- Banking and finance
- Energy and vital human services

Community water supply systems were included under vital human services. The commission concluded that there is a credible threat to the nation's water supply systems from certain known biological agents.

Presidential Decision Directive 63 (1998)

The Clinton Administration's Policy on Critical Infrastructure Protection, issued as Presidential Decision Directive 63 (PDD 63) in 1998, initiated the nation's security efforts by identifying eight critical infrastructures as those physical and cyber-based systems essential to the minimum operations of the economy and government (NSC 1998). Water, including both drinking water and wastewater, appeared in this initial list of critical infrastructures. PDD 63 established the National Infrastructure Protection Center (NIPC) and identified USEPA as the lead federal agency for the water sector, but anticipated a public–private partnership as a necessary requirement for protecting critical infrastructures. One of the objectives of PDD 63 was to prepare critical infrastructures for Y2K. Y2K was a commonly understood abbreviation that represented concerns about major difficulties that might occur as a result of the transition from the 20th to the 21st century and the millennium change. Some of the concerns focused on the possibility of information system confusion during this significant calendar change, while other fears centered on terrorist acts that might be planned to exploit the symbolism of the event.

Bioterrorism Act (2002)

The Bioterrorism Act is the short name for the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107-188). Title IV of the act amended the SDWA and required managers of drinking water systems serving more than 3,300 people to conduct formal VAs to determine

their systems' susceptibilities to terrorist attack and other intentional acts. The assessments are intended to identify threats and develop mitigation measures to reduce risk. The mandate was scheduled to be completed on a timetable according to customer base. Utilities serving more than 100,000 people were required to submit their completed VAs to USEPA by Mar. 31, 2003. Utilities serving 50,000 to 100,000 people and those serving 3,300 to 50,000 people were required to submit assessments by Dec. 31, 2003, and June 30, 2004, respectively.

The Bioterrorism Act stops short of mandating utilities to implement the security improvements outlined in their VAs. Additionally, under the Bioterrorism Act these same utilities were required to update their ERPs to incorporate their response activities for emergencies arising from intentional acts. While the actual ERPs do not have to be sent to USEPA, utilities were required to submit written certification of ERP update completion within six months of submission of their VA. More than 8,000 drinking water utilities completed VAs and revised their ERPs according to the regulatory timetable (Roberson and Morley 2005).

The Bioterrorism Act contains requirements for USEPA to provide information to utilities on potential threats, as well as strategies for responding to incidents. The act also requires USEPA to conduct research on areas relevant to water security. Additionally, under this amendment to the SDWA, USEPA is authorized to take actions to protect public health in the event of threatened or potential terrorist or intentional acts designed to adversely affect the provision or safety of drinking water. This authority may be exercised by the agency if appropriate state and local organizations have not acted to protect public health.

The Bioterrorism Act also increases the penalties for tampering with a public drinking water system to a maximum of \$1,000,000 and a prison sentence of up to 20 years. Attempts or threats to tamper with a water supply are punishable by fines of \$100,000 and a prison sentence of up to 5 years. For these penalties to apply, the tampering must include the intent to harm persons.

Although legislative initiatives have been introduced to require wastewater utilities to conduct VAs, there is currently no mandate for wastewater systems to conduct assessments or update their ERPs. However, many wastewater systems have initiated these steps on their own.

Homeland Security Act (2002)

The Homeland Security Act (HSA) of 2002 established the DHS, a cabinet-level department within the executive branch. This department was created to improve coordination among the nation's security forces and provide a single point of responsibility. Creation of the DHS brought 23 federal agencies (including the US Coast Guard, US Secret Service, and the Federal Emergency Management Agency) with a total workforce of 180,000 people, under one umbrella. The HSA requires that DHS secure the people, infrastructures,

property, resources, and systems in the United States from acts of terrorism. Among other tasks, DHS is charged with conducting a national scientific research and development program to support this mission. More specifically, the act directs the DHS secretary to assess the vulnerabilities of critical infrastructures and key resources (CI/KR), such as water, and identify protective priorities and measures.

Safety Act (2002)

The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (commonly known as the Safety Act) was enacted as part of the 2002 HSA. It promotes development of effective anti-terrorism technologies that can be deployed by the US government and private entities to protect vulnerable infrastructure targets. Upon designation for protection under the Safety Act by DHS, the manufacturers, vendors, and users of qualified technologies are afforded liability protection from lawsuits, with some limitations, should their product fail to detect and prevent an act of terrorism.

Patriot Act (2001)

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (commonly known as the Patriot Act) codified critical infrastructures. The act defines critical infrastructures as “those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economy, national public health or safety, or a combination of those matters.” Thirteen critical infrastructure sectors designated by the Patriot Act are listed in Table 4-1.

Critical Infrastructure Information Act (2002)

The Critical Infrastructure Information Act is designed to protect critical infrastructure information that is voluntarily submitted to DHS. This legislation doesn’t strictly apply to drinking water utilities because these utilities have already been required to submit a copy of their VAs to USEPA under the Bioterrorism Act and that law mandates that USEPA protect the information in the VAs from unauthorized disclosure.

Making the Nation Safer (Federal Report 2002)

In June 2002, the National Research Council (NRC) issued a report to Congress entitled “Making the Nation Safer: The Role of Science and Technology in Countering Terrorism” (NRC 2002). The report outlined a range of activities to improve the use of existing technologies and undertake research and development with the goal of improving the nation’s preparedness against terrorism.

Table 4-1. Critical infrastructure sectors as defined by the Patriot Act

| | |
|---|-------------------------|
| Agriculture | Banking and finance |
| Chemical industry and hazardous materials | Defense industrial base |
| Emergency services | Energy |
| Food | Government |
| Information and telecommunications | Postal and shipping |
| Public health | Transportation |
| Water* | |

* Water sector includes both drinking water and wastewater.

The report contained the following recommendations (among others) concerning water:

- Determine the persistence of pathogens, chemical contaminants, and other toxic materials in public water supplies in the presence of chlorine.
- Increase research into the use of sensors to monitor the safety of drinking water and to detect toxic agents in chemical or biological attacks.
- Reduce the potential hazards of transporting large quantities of industrial chemicals.
- Identify technologies for removal of chemical contaminants from water.
- Utilize encryption techniques, improved firewalls, and cyber detection technologies to improve the security of SCADA systems.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVES

Homeland Security Presidential Directives (HSPDs) are issued by the federal executive branch to various federal agencies to establish national homeland security policy. The first such directive, HSPD 1, was issued on Oct. 1, 2001. Directives differ from federal legislation in that they don't carry the force of law and don't mandate specific action on the part of the water sector, as the Bioterrorism Act did for drinking water. The directives typically instruct federal agencies to develop a plan or conduct a study. Several HSPDs, described as follows, are relevant to the drinking water and wastewater industries.

HSPD 5—Management of Domestic Incidents

Over the years, a number of issues have surfaced repeatedly during management of large-scale emergency responses, including:

- A single incident may affect multiple infrastructures and community services
- The scale of an incident may exceed the capacity of the response agencies

- Response entities have different organizational structures
- Coordinated planning between agencies is often lacking
- Communications between agencies is sometimes inadequate and incompatible
- Different response organizations use different terminology

HSPD 5, Management of Domestic Incidents, issued in 2003, addresses these problems. The purpose of this directive is to develop a comprehensive national approach for emergency management that includes the prevention, preparedness, response, and recovery phases of the incident. The goal is to ensure that all levels of government and the private sector work together during the response to an emergency. A more specific objective is to integrate the crisis and consequence phases of emergency response that previously had been dealt with separately.

HSPD 5 also mandates that the DHS secretary develop two important initiatives: the National Incident Management System (NIMS), and the National Response Plan (NRP), now known as the National Response Framework (NRF). These initiatives are discussed in detail in chapter 14 of this handbook, Emergency Management of Drinking Water and Wastewater Incidents.

HSPD 7—Critical Infrastructure Identification, Prioritization, and Protection

In December 2003, President George W. Bush issued HSPD 7, Critical Infrastructure Identification, Prioritization, and Protection, which established a national policy for federal departments and agencies to identify and prioritize critical infrastructures and key resources of the United States in order to protect them from terrorist attacks. DHS was assigned responsibility for coordinating the national effort to enhance the protection of critical infrastructures and key resources. Under HSPD 7, DHS was charged with preparing a National Infrastructure Protection Plan (NIPP) and the various critical infrastructure sectors were charged with preparing sector-specific plans (SSPs). This directive superseded PDD 63, which was issued in 1998 and initially identified eight critical infrastructures. Like PDD 63, HSPD 7 also designates USEPA as the sector-specific agency (SSA) to address the security needs of the drinking water and wastewater critical infrastructure. The intent is for USEPA to collaborate with federal, state, and local government agencies, as well as industry organizations such as AWWA and WEF, to facilitate VAs and foster risk management strategies.

HSPD 8—National Preparedness

Also issued in 2003, HSPD 8, National Preparedness, establishes policies to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments. The directive defines preparedness as “the existence of plans, procedures,

policies, training, and equipment necessary at the federal, state, and local levels to maximize the ability to prevent, respond to, and recover from major events.” A key priority of HSPD 8 is to expand regional collaboration through mutual aid agreements and assistance compacts. For the water industry, this collaboration is formalized through the WARN Program (Water and Waste-water Agency Response Network). More information on the program can be found at www.nationalwarn.org.

HSPD 9—Defense of United States Agriculture and Food

HSPD 9, Defense of United States Agriculture and Food, was released in 2004 and establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. Drinking water is included under the provisions of the directive. HSPD 9 requires USEPA to ensure water quality through surveillance and monitoring initiatives. Specifically, this directive charges USEPA to develop a robust, comprehensive surveillance and monitoring program to provide early warning in the event of a terrorist attack using biological, chemical, or radiological contaminants. HSPD 9 also directs USEPA to develop a nationwide laboratory network to support the routine monitoring and response requirements of the surveillance program.

USEPA’s primary effort to respond to the monitoring mandate is the Water Security Initiative (WSI). This initiative is a demonstration project intended to design, deploy, and evaluate model contamination warning systems (CWSs) for drinking water security. The goal is to demonstrate the concept in a few public water supplies so that drinking water utilities across the nation can establish their own CWSs. This initiative is discussed in greater detail in chapter 12 of this handbook, Contamination Warning Systems.

USEPA’s effort to develop a nationwide laboratory network is the Laboratory Alliance Program, which is described in chapter 15, Analytical Response to Water Contamination Threats.

HSPD 10—Biodefense for the 21st Century

Another 2004 directive, HSPD 10, Biodefense for the 21st Century provides a comprehensive framework for the nation’s biodefense. This classified directive establishes roles and responsibilities and integrates the efforts of various community, national security, medical, public health, intelligence, diplomatic, and law enforcement organizations, including USEPA, into a focused national effort against biological weapons threats. Four key themes of HSPD 10 are

- threat awareness
- prevention and protection
- surveillance and detection
- response and recovery

An unclassified summary of HSPD 10 is available for public dissemination.

National Infrastructure Protection Plan (2006)

The US infrastructure includes thousands of essential facilities, plants, transportation networks, and information systems. The majority of the infrastructure is owned and operated by private industry or state and local governments. Protecting the nation's critical infrastructures and key resources from destructive natural events or deliberate attack is essential to the nation's security, public health, safety, and economic vitality.

The NIPP, which was mandated by HSPD 7 (issued in 2006 and updated in 2007–2008), is a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government, nongovernmental agencies, and private industry. The goal is to integrate critical infrastructure security efforts among all of the governmental and nongovernmental stakeholders. The NIPP addresses risk management using an all-hazards approach. Resilience is a key objective of this plan. In this context, resilience is defined as "the capability of an asset, system, or network to maintain its function during, or recover from, a terrorist attack or other incident."

The NIPP identifies 14 critical infrastructures and 4 key resources (CI/KR). Each of these has been assigned a federal Sector-Specific Agency (SSA) responsible for working with DHS and infrastructure security partners to implement the partnership model. The sectors and SSAs are listed in Table 4-2.

While the NIPP addresses US infrastructure as a whole, Sector-Specific Plans (SSPs) have been developed for each of the critical infrastructures and key resources. The Water SSP is discussed in chapter 5 of this handbook.

Chemical Facility Anti-Terrorism Standards (2007)

DHS published the interim final rule for Chemical Facility Anti-Terrorism Standards (CFATS) in April 2007 (DHS 2007a). This rule establishes risk-based performance standards for the security of chemicals at industrial sites and other facilities that could be hazardous if released to the environment or stolen. Facilities that possess chemicals of interest (COI) above certain thresholds are required to prepare security vulnerability assessments and to develop and implement site security plans (SSPs). DHS subsequently published the COI list and the release and theft thresholds in November 2007 (DHS 2007b).

Water and wastewater utilities are currently exempt from CFATS. However, pressure is mounting to remove this exemption, with DHS Secretary Chertoff testifying that this exemption is a "gap" in the regulatory framework. Chlorine gas is the primary COI for the water sector, with a release threshold of 2,000 pounds and a theft threshold of 500 pounds.

CONCLUSIONS

While a number of federal regulations and directives dealing with protection of US water systems and emergency preparedness have been issued since September 2001, relatively few direct mandates have been issued to the drinking water industry, and none have been issued to the wastewater industry. Most directives have been aimed at organizing federal resources to assist the water industry in protecting itself. To date, the only federal mandates have been a one-time requirement for drinking water systems serving more than 3,300 people to conduct a VA, and a one-time requirement for these same utilities to prepare or update an ERP to deal with emergencies arising from intentional acts. The general expectation among many water industry practitioners is that this absence of actual security mandates may continue unless a significant malevolent event directed against a drinking water or wastewater utility occurs.

Table 4-2. Critical infrastructure, key resources, and sector-specific agencies

| Critical Infrastructure and Key Resources Sector | Sector-Specific Agency |
|--|--|
| Agriculture and food * | Department of Agriculture, Department of Health and Human Services |
| Banking and finance * | Department of the Treasury |
| Chemical * | Department of Homeland Security |
| Commercial facilities † | Department of Homeland Security |
| Nuclear reactors, material, and waste † | Department of Homeland Security |
| Dams † | Department of Homeland Security |
| Defense industrial base * | Department of Defense |
| Water * | US Environmental Protection Agency |
| Emergency services * | Department of Homeland Security |
| Energy * | Department of Energy |
| Government facilities † | Department of Homeland Security |
| Information technology * | Department of Homeland Security |
| National monuments and icons * | Department of the Interior |
| Postal and shipping * | Department of Homeland Security |
| Public health and healthcare * | Department of Health and Human Services |
| Critical manufacturing * | Department of Homeland Security |
| Communications * | Department of Homeland Security |
| Transportation systems * | Department of Homeland Security |

Source: US DHS

NOTES: The Water sector includes both drinking water and wastewater. The NIPP is available online at www.dhs.gov/nipp.

* Indicates a critical infrastructure.

† Indicates a key resource.

REFERENCES

- American Society of Civil Engineers (ASCE), American Water Works Association (AWWA), and Water Environment Federation (WEF). 2004a. *Interim Voluntary Security Guidance for Water Utilities*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- ASCE, AWWA, and WEF. 2004b. *Interim Voluntary Security Guidance for Wastewater/Storm Water Utilities*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- ASCE, AWWA, and WEF. 2004c. *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- ASCE, AWWA, and WEF. 2006a. *Guidelines for the Physical Security of Water Utilities*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- ASCE, AWWA, and WEF. 2006b. *Guidelines for the Physical Security of Wastewater/Stormwater Utilities*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- Department of Homeland Security (DHS). 2007a. Chemical Facility Anti-Terrorism Standards: Interim Final Rule. *Fed. Reg.*, 72:67:17687.
- DHS. 2007b. Appendix to Chemical Facility Anti-Terrorism Standards: Final Rule. *Fed. Reg.*, 72:223:65397.
- Linville, T. J. and K.A. Thompson. 2006. Protecting the Security of Our Nation's Water Systems: Challenges and Successes. *Jour. AWWA*, 98(3):234.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academies Press.
- National Security Council (NSC). 1998. White Paper Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (May 22). Washington, D.C.: National Academies Press.
- President's Commission on Critical Infrastructure Protection. 1996. *Critical Foundations: Protecting America's Infrastructure*. Washington, D.C. www.pccip.gov.
- Roberson, J.A., and K.M. Morley. 2005. We Need to Get Strategic on Water Security. *Jour. AWWA*, 97(10):42.

THE WATER SECTOR-SPECIFIC PLAN AND ACTIVE AND EFFECTIVE SECURITY PROGRAMS

The drinking water and wastewater industries, collectively known as the water sector, in conjunction with the USEPA and a number of industry associations, has produced several general guidance documents to assist the water sector in developing security programs. These documents are described in this chapter along with a program of national performance measures that have been developed to track risk-reduction progress in the sector.

SECTOR-SPECIFIC PLANS

While the NIPP (DHS 2006) discussed in chapter 4 of this book, addresses all 18 critical infrastructures and key resources (sectors), an SSP is also being prepared for each of the individual sectors. An SSP addresses the unique characteristics of each critical infrastructure and key resource and applies the NIPP risk management structure to each sector. The SSPs provide guidance to help prepare each sector to prevent, detect, respond to, and recover from terrorist attacks, other intentional acts, natural disasters, and accidents. The SSPs also outline the responsibilities of the SSAs. In the case of drinking water and wastewater, the SSA is the USEPA.

USEPA, partnering with a Water Sector Coordinating Council (WSCC) and a Water Sector Government Coordinating Council (WSGCC), developed the SSP for drinking water and wastewater. The WSCC is a committee consisting of 16 utility representatives. Two representatives are recommended by each of 8 water and wastewater organizations, which include AWWA,

the Association of Metropolitan Water Agencies (AMWA), National Association of Clean Water Agencies (NACWA), National Rural Water Association (NRWA), WEF, Water Environment Research Foundation (WERF), Water Research Foundation, and the National Association of Water Companies. The WSGCC is composed of representatives from various levels of government including federal, state, local, and tribal. Federal agencies represented include USEPA, DHS, Defense Department, Department of the Interior, and Department of Health and Human Services, among others.

All SSPs address processes for

- Identifying assets within the sector
- Identifying and assessing vulnerabilities, and prioritizing infrastructure within the sector
- Developing sector-specific protective programs
- Developing metrics to measure the effectiveness of security improvements within the sector

The Water SSP was published in 2007 (DHS and USEPA 2007). It contains goals and objectives that drive the development of protective programs and measure success. The following lists the four goals of the Water SSP, and their supporting objectives.

Goal 1: Sustain protection of public health and the environment.

Objective 1: Encourage integration of security concepts into daily business operations at utilities to foster a security culture.

Objective 2: Evaluate and develop security-related surveillance, monitoring, warning, and response capabilities to recognize risks introduced into water-sector systems that affect public health and economic viability.

Objective 3: Develop a nationwide laboratory network for water-quality security that integrates federal and state laboratory resources and uses standard diagnostic protocols and procedures, or develop a supporting laboratory network capable of analyzing security threats to water quality.

Goal 2: Recognize and reduce risks in the water sector.

Objective 1: Improve the identification of vulnerabilities based on knowledge and best available information, with the intent of increasing the sector's overall security posture.

Objective 2: Improve identification of potential threats through water-sector partners' (water utilities, national associations, and federal, state, and local governments) knowledge base and communications with the intent of increasing the sector's overall security posture.

Objective 3: Identify and refine public health and economic impact consequences of manmade or natural incidents to improve utility risk assessments and to enhance the sector's overall security posture.

Goal 3: Maintain a resilient infrastructure.

-
- Objective 1: Emphasize continuity of drinking water and wastewater services as it pertains to water-sector utility emergency preparedness, response, and recovery planning.
 - Objective 2: Explore and expand the implementation of mutual aid agreements and compacts in the water sector. The sector has significantly enhanced its resilience through agreements among utilities and states; increasing the number and scope of these will further enhance resiliency in the sector.
 - Objective 3: Identify and implement key response and recovery strategies. Response and recovery from an incident in the sector will be crucial to maintaining public health and public confidence.
 - Objective 4: Increase understanding of how the water sector is interdependent with other critical infrastructure sectors. Sectors such as public health and emergency services are largely dependent on the water sector for their continuity of operations, while the water sector is dependent on sectors such as chemical and electricity for the continuity of its operations.

Goal 4: Increase communication, outreach, and public confidence.

- Objective 1: Communicate with the public about the level of security and resilience in the water sector and provide outreach to ensure the public's ability to be prepared and respond to a natural disaster or manmade incident.
- Objective 2: Enhance communications and coordination among utilities and federal, state, and local officials and agencies to provide information about threats and other hazards.
- Objective 3: Improve relationships among all water sector security partners through a strong public–private partnership characterized by trusted relationships.

The WSCC is working to implement these goals and objectives.

TEN FEATURES OF ACTIVE AND EFFECTIVE SECURITY PROGRAMS

In the fall of 2003, the National Drinking Water Advisory Council (NDWAC) established a Water Security Working Group (WSWG) to make recommendations on water security issues. The WSWG included stakeholders from a variety of perspectives in the drinking water and wastewater industries including large and small utilities, USEPA, CDC, states, DHS, and community interest groups, among others. The WSWG was an expanded and more formalized group than the ad hoc advisory committee that had been formed in early 2001 to implement PDD 63, discussed in chapter 4, and the Water Protection Task Force that was established in October 2001, which is discussed in chapter 6.

The purpose of the group was to encourage development of voluntary water security programs. In 2005, NDWAC released a report (NDWAC 2005) identifying 14 features that drinking water and wastewater utilities could implement to achieve a more active and effective security program for their individual organizations. The features were associated with the four overarching pillars of security: prevention, detection, response, and recovery. The committee emphasized that one size does not fit all and that there will be variability in security approaches among utilities based on utility specific circumstances. It was hoped that many utilities may be able to adopt some of these features with minimal, if any, capital investment.

In 2007, another advisory group, a workgroup of the Critical Infrastructure Partnership Advisory Council (CIPAC), updated the original 14 features of an active and effective security program (CIPAC 2007). CIPAC was convened by the Water Sector Coordinating Council (WSCC) and the Government Coordinating Council (GCC) and consists of representatives from utilities, industry organizations, and federal and state government agencies. Their goal was to streamline the existing features, capture the water sector's post Hurricane Katrina emphasis on *all hazards* preparedness, and align the features with the goals of the Water SSP, which was not completed at the time that the original 14 features were drafted.

The new 10 features, aligned with each of the four SSP goals, are as follows.

SSP Goal 1: Sustain protection of public health and the environment.

Feature 1: Encourage awareness and integration of a comprehensive protective posture into daily business operations to foster a protective culture throughout the organization and ensure continuity of utility services.

Feature 2: Annually identify protective program priorities and resources needed support priorities with utility-specific measures; and self-assess using these measures to understand and document program progress.

Feature 3: Employ protocols for detection of contamination while recognizing limitations in current contaminant detection, monitoring, and public-health surveillance methods.

SSP Goal 2: Recognize and reduce risks in the water sector.

Feature 4: Assess risks and periodically review (and update) VAs to reflect changes in potential threats, vulnerabilities, and consequences.

Feature 5: Establish physical and procedural controls to restrict access only to authorized individuals and to detect unauthorized physical and cyber intrusions.

Feature 6: Incorporate protective program considerations into procurement, repair, maintenance, and replacement of physical infrastructure decisions.

SSP Goal 3: Maintain a resilient infrastructure.

Feature 7: Prepare emergency response, recovery, and business continuity plans; test and review plans regularly, update plans as necessary to ensure NIMS compliance and to reflect changes in potential threats, vulnerabilities, consequences, physical infrastructure, utility operations critical interdependencies, and response protocols in partner organizations.

Feature 8: Forge reliable and collaborative partnerships with first responders, managers of critical interdependent infrastructure, other utilities, and response organizations to maintain a resilient infrastructure.

SSP Goal 4: Increase communication, outreach, and public confidence.

Feature 9: Develop and implement strategies for regular, ongoing communication about protective programs with employees, customers, and the general public to increase overall awareness and preparedness for response to an incident.

Feature 10: Monitor incidents and available threat-level information; escalate procedures in response to relevant threats and incidents.

The 10 features describe basic elements that utility owners and operators can consider when establishing a protective program appropriate for their specific utility.

SECURITY PERFORMANCE MEASUREMENT

In 2007, the same CIPAC workgroup that revised the original 14 measures of a successful security program to 10 measures developed a national performance measurement system to monitor progress in improving security in the water sector. CIPAC recommended measurements that correspond to the goals and objectives outlined in the Water SSP previously described.

The metrics program was implemented in 2008. The water sector was the first of the 18 critical infrastructure and key resources sectors to establish metrics for assessing security and preparedness (Morley 2009). Annual reporting by utilities is voluntary. The reports will help utilities demonstrate the improvements they've made in security enhancements and risk reduction to the USEPA and the DHS, and should identify gaps where federal government efforts could be focused in the future. The government efforts may include development of additional security tools and provision of additional training.

Reporting consists of a survey that is completed by utilities and other key players. Utilities of all sizes are encouraged to participate. The questions asked consist of one subset that is to be used for national reporting purposes. To preserve the anonymity of individual utilities, this subset is collected by a third party, the Information Sharing Analysis Center (ISAC), and is reported to USEPA as aggregate data. Progress data submitted by individual utilities is protected from public disclosure under an amendment to the Freedom of

Information Act (FOIA). Another group of questions, primarily concerning risk reduction, is available for use by the utilities themselves as a self-assessment tool. Still another subset of questions is directed to key players such as federal agencies, state agencies, and water utility associations to gauge the effectiveness of their efforts in improving the emergency preparedness of utilities.

The metrics are aligned with specific goals of the Water SSP. For example, Goal #2 of the SSP is: Recognize and reduce risks in the water sector. One relevant measure of efforts toward achieving that goal is the percentage of utilities that annually review their VAs. The corresponding question asked of utilities in the survey is: Does your utility review its VA annually (Y/N)? Another example, Goal #4 of the Water SSP is: Increase communication, outreach, and public confidence. A measurement of efforts toward meeting that goal is a determination of the number and percentage of utilities that have developed plans to handle communications during an emergency. The corresponding question asked of utilities is: Does your utility have a crisis communication plan (Y/N)?

CONCLUSIONS

The Water SSP and 10 features of an active and effective security program are expected to provide useful guidance to utilities, industry organizations, and government agencies working to improve the security and preparedness of drinking water and wastewater utilities against a variety of risks. The national measurement system is intended to give these stakeholders a method for gauging their progress in this area.

REFERENCES

- Critical Infrastructure Partnership Advisory Council (CIPAC). 2007. *Features of an Active and Effective Program for Water and Wastewater Utilities*. Washington, D.C. www.epa.gov/safewater/watersecurity/pubs/brochure_watersecurity_featuresofanactiveandeffective.pdf.
- Department of Homeland Security (DHS). 2006. National Infrastructure Protection Plan (amended 2007–2008). Washington, D.C. www.dhs.gov/nipp.
- DHS and US Environmental Protection Agency (USEPA). 2007. Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan. Washington, D.C. www.dhs.gov/xlibrary/assets/nipp-ssp-water.pdf.
- Morley, K.M. 2009. An Evolving Culture of Security and Preparedness in the Water Sector. *Jour. AWWA*, 101(1):32.
- National Drinking Water Advisory Council (NDWAC). 2005. Recommendations of the National Drinking Water Advisory Council to the US Environmental Protection Agency on Water Security Practices, Incentives, and Measures. Washington, D.C. www.epa.gov/safewater/ndwac/pdfs/wswg-report_final_july2005.pdf.

REPORTS AND TOOLS TO IMPROVE SECURITY AND EMERGENCY PREPAREDNESS

The United States government rapidly undertook a number of steps after 9/11 to address new security concerns. On Oct. 5, 2001, USEPA established a Water Protection Task Force to coordinate national water security efforts. On Oct. 8, 2001, President Bush created the White House Office of Homeland Security. On Oct. 16, 2001, the Critical Infrastructure Protection Board was formed to coordinate physical and cyber security for the various key infrastructures in this country. In March 2003, the DHS was established by merging 22 federal agencies under one umbrella organization. This was the largest reorganization in the federal government since the Department of Defense was instituted in 1947.

In September 2003, USEPA created the Water Security Division, which took over the activities initiated by the Water Protection Task Force. An advisory group of drinking water and wastewater utilities, named the Water Security Working Group, was formed by USEPA in early 2004 to advise the agency on the development of best security practices and policies for water utilities.

Some of the programs, reports, and tools developed by federal organizations such as these to assist utilities in protection efforts against malevolent acts, natural disasters, and accidents are described in this chapter.

BASELINE THREAT DOCUMENTS

One of the requirements of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) was that USEPA

provide information to utilities on threats that they may face from intentional acts. The goal was to provide drinking water and wastewater utility officials with information that would assist them in preparing VAs. To comply with this mandate, USEPA published two documents:

- *Baseline Threat Information for Vulnerability Assessment of Community Water Systems* was released in September 2002 (USEPA 2002). This report describes threats to drinking water utilities across the country.
- *Wastewater Threat Document* was released in June 2005 (Water Environment Federation 2005). This document was prepared through a grant awarded to WEF. Under the grant, WEF and its contractors, with significant input from wastewater industry stakeholders, USEPA, DHS, and FBI, summarized the threats to wastewater systems.

The threat information in these two publications is not specific for individual utilities but rather summarizes the general risks from malevolent acts that could potentially impact drinking water and wastewater systems across the nation. Specific threats are assessed when individual utilities, working with law enforcement, regulators, and other partners, conduct VAs or receive specific threat information.

Neither of these guidance documents contains classified information. However, they do contain sensitive information on the perceived threat to US utilities. Therefore, neither publication is available to the public. Rather, individual water systems must obtain these documents directly from USEPA.

USEPA WATER SECURITY WEB SITE

To better provide security information for water utilities, local and state governments, public health officials, consultants, and other emergency preparedness and response partners, USEPA established a water security Web site, www.epa.gov/safewater/watersecurity. This site provides extensive information on a variety of topics, including VAs, ERPs, pertinent legislation, and publications.

SECURITY PRODUCT GUIDE

The *Security Product Guide* is an important information tool that provides information on commercially available products that drinking water and wastewater utilities may use to reduce their vulnerability, and increase their preparedness for, a variety of natural and manmade events. The guide is organized into three areas:

- Physical security (e.g., walls, gates, manhole locks)
- Electronic or cyber security (e.g., computer firewalls)
- Monitoring tools (e.g., analytical devices that detect chemical, biological, or radiological contaminants online in source water, drinking water, or wastewater)

The *Security Product Guide* can be found on USEPA's Web site at www.epa.gov/watersecurity/guide. Note that the listing of a product in the *Security Product Guide* does not constitute an endorsement by USEPA or any other federal agency.

NATIONAL HOMELAND SECURITY RESEARCH CENTER

USEPA's Office of Research and Development established the National Homeland Security Research Center (NHSRC) in February 2003. The research center, which is headquartered in Cincinnati, Ohio, manages research designed to help stakeholders prevent, prepare for, respond to, and recover from public health and environmental emergencies arising from terrorist threats and incidents. Stakeholders include utility operators, public health officials, and emergency and follow-up responders. The center's motto is: "Advancing Our Nation's Security Through Science."

NHSRC's research and development efforts focus on five areas:

- Threat and consequence assessment
- Decontamination and consequence management
- Water infrastructure protection
- Response capability enhancement
- Technology testing and evaluation

Resources available from NHSRC include tools and methodologies to support contaminant detection and characterization, treatment and decontamination, physical security enhancement, and risk assessment and communication, as well as numerous papers and fact sheets covering a variety of related topics. These products are available to download from www.epa.gov/nhsrc.

RESPONSE PROTOCOL TOOLBOXES

In 2003–2004, USEPA released the *Drinking Water Response Protocol Toolbox: Planning for and Responding to Contamination Threats to Drinking Water Systems* (USEPA 2003–2004). This guidance document provides emergency response planning tools that are designed to help the drinking water industry respond effectively to intentional contamination threats and incidents. The *Toolbox* was created for use by drinking water utilities, laboratories, emergency responders, state drinking water regulators, technical assistance providers, and public health and law enforcement officials. While use of the *Toolbox* is not mandatory, utilities and other responders are encouraged to employ information from this resource when they are updating their ERPs. The *Toolbox* is available online in Microsoft® Word to allow users to easily cut and paste forms and text from the *Toolbox* into their own planning documents.

In 2009, USEPA released the *Wastewater Response Protocol Toolbox: Planning for and Responding to Contamination Threats and Incidents in Wastewater Systems* (USEPA 2009). This document is designed to assist wastewater utilities and other stakeholders in responding to both intentional and accidental contamination events in wastewater collection and treatment systems. As with the drinking water version, the intent is that utilities and other responders will freely utilize recommendations outlined in the Toolbox when updating their organizations' ERPs.

Both the drinking water and wastewater toolboxes are discussed in greater detail in chapter 13 of this book.

ENVIRONMENTAL LABORATORY COMPENDIUM

The USEPA Environmental Laboratory Compendium is a database of national environmental laboratories available to water utilities and state agencies. The database describes each laboratory's capabilities to analyze chemical and biological analytes as well as chemical warfare, bioterrorism, and radiochemical agents. It was developed as a tool to quickly identify laboratories with capabilities to support incident-specific response and recovery. The compendium should be useful in preparing for and responding to natural and accidental events as well as to malevolent acts. To access the database, potential users must first register with USEPA. Instructions for registration are available at www.epa.gov/compendium.

ERP GUIDELINES

These guidelines provide suggestions to utility personnel on how to organize their ERPs. The suggestions are not intended to supersede requirements that the individual states have imposed on utilities within their jurisdictions, but rather to supplement them. USEPA's ERP guidance is discussed in greater detail in chapter 13 of this handbook and can be accessed at www.epa.gov/safewater/watersecurity.

SECURITY RESEARCH PLANS AND HOMELAND SECURITY STRATEGY

In September 2002, USEPA published *Strategic Plan for Homeland Security*, which was not limited to water security concerns, but rather identified several mission critical areas on which USEPA intended to focus its homeland security planning; critical infrastructure protection; preparedness, response and recovery; communication and information; protection of USEPA personnel and infrastructure; and self evaluation. The plan can be downloaded from www.epa.gov/safewater/watersecurity/pubs/epa_homeland_security_strategic_plan.pdf.

In March 2004, USEPA issued the *Water Security Research and Technical Support Action Plan*, identifying critical research needs and providing an implementation plan for addressing those needs. Projects were included in the areas of physical and cyber infrastructure protection; contaminant identification; monitoring and analysis; treatment, decontamination, and disposal; contingency planning; infrastructure interdependencies; and risk assessment and communication. A second homeland security strategy, released in Oct. 2004, updated the initial strategy principally by identifying projected funding and resources for USEPA's strategic objectives and recognizing the evolving role of DHS (USEPA 2004).

GOVERNMENT ACCOUNTABILITY OFFICE (GAO) REPORTS

The GAO issued two reports discussing how federal funding can best be spent to improve security at drinking water and wastewater utilities. Both reports were based on opinions of subject matter experts selected by GAO. The drinking water report (GAO 2003) identified a number of specific activities deserving of federal support, particularly physical and technological upgrades, education and training for utility personnel and responders, and strengthening the relationships between water utilities and other key players including law enforcement and public health agencies. In the wastewater report (GAO 2005), the experts identified the replacement of gaseous chemicals used for disinfection with less hazardous alternatives as an important initiative worthy of federal funding. Additionally, the wastewater experts emphasized the need for improved local, state, and regional collaboration, as well as support for VAs. Both groups of experts favored giving funding priority to utilities that serve critical assets (e.g., public health institutions, government, and military bases) and to utilities serving large populations.

ENVIRONMENTAL TECHNOLOGY VERIFICATION AND TECHNOLOGY TESTING AND EVALUATION PROGRAMS

Since 2001, a number of technologies have been proposed to address homeland security needs in the water sector. A critical question for utilities determining which products to purchase is "How effective are these technologies?" USEPA's Environmental Technology Verification (ETV) and Technology Testing and Evaluation Programs (TTEP) conduct third-party performance evaluations of market-ready homeland security technologies to assist utilities in selecting technologies. The programs incorporate stakeholder guidance in determining which technologies should be tested and in designing the tests. Stakeholders include personnel from utilities and various government agencies.

ETV and TTEP are not certification programs, and USEPA does not endorse technologies through these initiatives. Rather, ETV and TTEP independently evaluate commercially available equipment and report the results of their verification studies. Technology categories of interest to water and wastewater utilities include contaminant detection, monitoring, treatment, decontamination, and computer modeling.

ETV was the initial version of this product verification initiative, and has evolved into TTEP. TTEP differs from ETV in that it actually compares technologies against each other as well as tests them against a standard set of user needs. TTEP also differs from the earlier program in that it does not require voluntary commitment of vendors. Rather, TTEP can independently purchase commercially available equipment and conduct verification tests.

The criteria used for verification of contaminant detection technology include:

- Ability to utilize the technology in the field
- Accuracy
- Frequency of false positives and negatives
- Interferences
- Level of operator skill required
- Matrix effects
- Reproducibility
- Sensitivity

Some of the analytical technologies already tested include, among others:

- Multiparameter water quality probes
- Mobile mass spectrometers
- Portable cyanide analyzers
- Rapid toxicity testing systems
- Rapid polymerase chain reaction (PCR) systems

Test results for technologies already verified can be obtained from www.epa.gov/nhsrcc.

THREAT ENSEMBLE VULNERABILITY ASSESSMENT

Developed by USEPA's NHSRC, the Threat Ensemble Vulnerability Assessment (TEVA) is a collaborative research program dedicated to developing methodologies and software tools for improving the security of drinking water systems (Murray et al. 2004). Collaborative partners include AWWA, Sandia National Laboratory, Argonne National Laboratory, and the University of Cincinnati, with technical support from Science Applications International Corporation (SAIC). TEVA uses probabilistic analysis to assess the vulnerability of a water distribution system to a large range of contamination events. Monte Carlo–type simulations are performed to generate scenarios, and statistics are analyzed to determine the feasibility of various threats, identify

vulnerable locations in the water distribution system, and help determine the optimal location for contaminant monitors. A number of drinking water utilities have shared their distribution system network hydraulic models with USEPA, and subsequently USEPA has recommended optimum placement of monitors by using these models and simulating the introduction of contaminants at various nodes throughout the distribution network.

USEPA WATER SECURITY DIVISION

USEPA formed the Water Security Task Force shortly following the terrorist attacks of 2001 in response to concerns about drinking water and wastewater utilities becoming potential targets of malevolent acts. In 2005, this temporary task force was upgraded to a permanent Water Security Division. The mission of the USEPA Water Security Division is to work with states, tribes, drinking water and wastewater utilities, and other partners in developing and maintaining security practices to enhance the water sector's ability to prevent, detect, respond to, and recover from natural or manmade emergencies (Whitler 2007). The impetus for these activities comes from HSPD 8 and NIMS. The direction of this organization has evolved from a focus on terrorism to an all-hazards approach, especially following the widespread damage of Hurricanes Katrina and Rita in 2005. The division has two branches:

- Security Assistance
- Threats, Analysis, Prevention, and Preparedness.

WATER SECURITY INITIATIVE (WSI)

The WSI is USEPA's response to the mandate in HSPD 9, *Defense of United States Agriculture and Food*, that USEPA develop robust and comprehensive surveillance and monitoring systems for drinking water similar to the BioWatch monitoring system for air. The WSI gathers information from a number of sources to indicate the presence of contaminants in a public water supply. The sources include online instrumental monitoring of water quality, grab sampling and analysis of distribution system water samples, customer complaints, enhanced physical security monitoring, and public health syndromic surveillance data. The goal of a monitoring system is to reduce the public health and economic impacts from an intentional or accidental contamination event. The initial pilot Contamination Warning System (CWS), developed as part of the WSI, was established in the Cincinnati, Ohio drinking water distribution network. Additional pilots are being established in New York, San Francisco, Philadelphia, and Dallas. The hope is that these pilots will serve as examples and provide guidance materials for other water utilities opting to develop their own CWSs.

The WSI is described in more detail in chapter 12, Contamination Warning Systems. Additional information on the WSI is available from www.epa.gov/watersecurity/pubs/fs_watersecurity_securityinitiative.pdf.

HYDRAULIC MODELS

USEPA, through its contractor SAIC, has produced several hydraulic models intended for use by utilities in planning for and responding to accidental and intentional contamination events.

IC Water (Incident Command Water) addresses concerns over contaminant discharges into natural waterways such as rivers, lakes, and reservoirs. This model, which was originally called RiverSpill, produces maps, tables, and charts that help officials determine whether drinking water intakes are in a contaminant's path, and when and in what concentration the contaminant will reach the intakes. IC Water makes use of river velocity data; substance dispersion models; and a biological, chemical, and radiological contaminant database. It also utilizes GIS to display the location of drinking water and sewage treatment plants, hazardous materials storage sites, railways, highways, airports, and other critical facilities.

PipelineNet is a consequence-assessment tool for drinking water contamination events. (Bahadur et al. 2003; Samuels et al. 2003). It is a GIS-based software tool with integrated database capability that can be used to model the flow and concentration of contaminants in a public drinking-water pipeline network. PipelineNet combines hydraulic and water quality monitoring with maps and a US Census population database. The model estimates the population and critical facilities at risk resulting from an accidental or deliberate introduction of a contaminant into a drinking water distribution system. The hydraulic tool also assists in the analysis and visualization of the consequences associated with various response actions. For example, while flushing may help remove a contaminant from the water distribution network, an unintended consequence may be reduced water flow to meet fire protection requirements.

SewerNet focuses on accidental and intentional contamination events in sanitary and stormwater collection systems. SewerNet integrates ESRI's ArcGIS and USEPA's Sewer and Water Management Model (SWMM) hydraulic model for wastewater/stormwater collection systems to perform consequence assessment analysis for facilities affected by a hazardous event. A fully integrated chemical, biological, and radiological database facilitates pollutant characterization. The SewerNet application can be used for emergency planning and emergency response, as well as for normal operations.

Because all three of these models are based on a common GIS platform, they can be integrated to trace a contaminant from the source water through the drinking water system, and subsequently through the wastewater network (Samuels et al. 2009).

Additional information on these three models can be obtained from <http://eh2o.saic.com/iwqss>.

WATER CONTAMINANT INFORMATION TOOL (WCIT)

The Water Contaminant Information Tool (WCIT) is a secure, password-protected, web-accessible database that provides information on contaminants that could pose a threat to people, the environment, or the infrastructure if intentionally or accidentally, introduced into a drinking water or wastewater system. Contaminants included in WCIT include pathogenic microorganisms, biotoxins, inorganic and organic chemicals, weaponized chemicals, and radionuclides. Many of the contaminants included in the WCIT database are not the familiar ones regulated under the SDWA or CWA. However, they are contaminants that could result in substantial adverse consequences to public health if introduced into drinking water or wastewater networks. Unlike other resources or databases, WCIT contains water-specific data rather than general information on environmental contamination.

The first version of WCIT was released in late 2005, and has been updated several times since then. The database contains up-to-date information extracted from peer-reviewed sources and research. The types of information provided for the various contaminants include: contaminant names and Chemical Abstract Service ID numbers, availability, fate and transport characteristics in water, health effects, toxicity, infectivity, basic clinical information, water quality and environmental indicators, laboratory and field analytical techniques, effectiveness of drinking water and wastewater treatment process for contaminant removal, response advice for utilities and regulatory agencies, and basic guidance on decontamination.

WCIT is designed to assist utilities and other stakeholders in planning for, and responding to, drinking water and wastewater contamination threats and incidents. As a planning tool, WCIT can be used to better understand the threat of contamination and the attributes of contaminants that make them a concern. As a response tool, WCIT provides immediate access to contaminant information that will help responders make informed decisions. As a research tool, WCIT helps identify knowledge gaps for priority contaminants, which in turn will guide future research efforts.

As of 2009, WCIT contained information on 97 contaminants, with plans for the addition of another 10 contaminants. All of the information is from open literature sources. However, once the data are compiled into the database, the information is considered sensitive. To gain access to the password-protected online database, potential users must preregister with USEPA. Access is granted to US drinking water and wastewater utilities, state regulatory agencies, drinking water and wastewater associations, public health officials, government laboratory personnel, and federal officials. Online registration is free. Additionally, WaterISAC-Pro subscribers can access this database directly through the WaterISAC website.

Additional information on WCIT, and instructions on applying for access, are available at the following web address: www.epa.gov/wcit

FBI INFRA GARD PROGRAM

The 18 critical infrastructures and key resources include physical and cyber-based systems that are essential to the operation of the US economy and government, as defined by PDD 63 (May 1998). These infrastructures and resources are listed chapter 4 of this book (Table 4.2).

InfraGard is an FBI/NIPC (National Infrastructure Protection Center) program designed to help identify and coordinate existing infrastructure protection expertise from both inside and outside the federal government. Each of the 56 FBI field offices has established a local InfraGard chapter with membership rosters that consist of representatives from private industry, academia, and the public sector. Through InfraGard, stakeholders such as water utilities gain access to specialists from law enforcement, industry, universities, and federal, state, and local government agencies.

The InfraGard program includes an encrypted, two-way email communication system to facilitate the secure sharing of information among InfraGard members. Because the water industry is included as one of the 18 critical infrastructures and key resources, drinking water and wastewater utilities are encouraged to join InfraGard. There is no cost associated with membership, and information is available at www.infragard.net or by email from infragardteam@infragard.org.

WATER INFORMATION SHARING AND ANALYSIS CENTER

WaterISAC is a highly secure, Internet-based, rapid notification system and information resource for threats to America's drinking water and wastewater utilities. It is a portal for water systems to report incidents and share sensitive intelligence among utilities and between the water sector and federal agencies. It offers subscribers access to specialized information, intelligence, data, and resources. WaterISAC analysts have access to classified intelligence and the WaterISAC team is available by email or phone 24 hours a day, 7 days a week, every day of the year. The analysts gather, assess, and quickly disseminate critical information on threats to the nation's water sector, with detailed analysis that shows how these threats could impact utilities. Many of the notifications and much of the information originates from the FBI, DHS, and USEPA, as well as other intelligence, law enforcement, and public health agencies. WaterISAC analysts even suggest mitigating security actions. In addition to serving as a secure communications network, WaterISAC functions as a library for unclassified information on security topics. Access to WaterISAC assists utilities in responding to natural disasters as well as man-made events.

The WaterISAC online operation is hosted inside a government-designated top-secret security clearance facility. The system is further protected by state-of-the-art cyber security measures that constantly monitor for unauthorized login attempts or system breaches.

WaterISAC has developed two tiers of service to meet the needs of water utilities as well as other water-sector stakeholders. WaterISAC Pro is designed exclusively for drinking water and wastewater utility systems and offers the full range of WaterISAC services to its subscribers. The upper tier service is provided for a fee, which ranges from \$200 per year for utilities serving fewer than 50,000 people to \$1,000 per year for utilities serving more than 100,000 people. WaterISAC Basic, an entry-level connection to the WaterISAC, is a free service designed for utilities, local law enforcement, municipal departments, and other agencies that need to remain connected to the water sector but do not have the same security needs as the water systems themselves. WaterISAC Basic disseminates bulletins and advisories issued by the USEPA, DHS, and other federal agencies.

WaterISAC went online in December 2002. Overseen by a board of managers comprised of drinking water and wastewater utility executives, the program is administered by the AMWA. More information on WaterISAC is available at www.WaterISAC.org or by phone at 1-866-426-4722.

THREAT-BASED SECURITY GUIDELINES

AWWA, WEF, and the American Society of Civil Engineers (ASCE), under a cooperative agreement with USEPA, formed the Water Infrastructure Standards Enhancement Committee. This committee is working on a comprehensive program to produce security guidelines for the drinking water and wastewater industries (Linville and Thompson 2006). Phase I of the effort resulted in the publication of three guidance documents: *Interim Voluntary Security Guidance for Water Utilities*; *Interim Voluntary Security Guidance for Wastewater/Storm Water Utilities*; and *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System* (ASCE, AWWA, and WEF 2004 a, b, c).

Phase II of the project generated training materials based on these three guidance documents to assist utility managers, operators, and system designers in protecting the water infrastructure. The training program is modular and includes Microsoft PowerPoint presentations, instructor notes, and quizzes.

Phase III is intended to produce voluntary, consensus security standards for the water industry. Many utilities do not want security standards, and it is not clear at this time whether rigid standards are needed in the water sector. The draft standards provide recommendations on physical security for utilities. The recommended measures are intended to be linked to the design-basis threats developed by any given utility. A design-basis threat is the most probable threat that a particular utility anticipates based on its VA and the most current information from local, state, and federal sources. The drinking water or wastewater utility is encouraged to customize the recommended measures to fit its own specific circumstances. These standards were released in December 2006 and are entitled *Guidelines for the Physical*

Security of Water Utilities, and Guidelines for the Physical Security of Wastewater/Storm Water Utilities (ASCE, AWWA, and WEF 2006 a, b).

CONCLUSIONS

As discussed in this chapter, a number of reports and tools have been released by federal agencies since 2001 to assist water utilities in decreasing their vulnerabilities and increasing their ability to respond to emergencies arising from manmade events, natural disasters, and accidents. Additional studies and tools are under development and will become available in the coming years. A good source for these resources continues to be USEPA's water security Web site, www.epa.gov/safewater/watersecurity.

REFERENCES

- American Society of Civil Engineers (ASCE), American Water Works Association (AWWA), and Water Environment Federation (WEF). 2004a. *Interim Voluntary Security Guidance for Water Utilities*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- ASCE, AWWA, and WEF. 2004b. *Interim Voluntary Security Guidance for Wastewater/ Storm Water Utilities*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- ASCE, AWWA, and WEF. 2004c. *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*. I.M. Pincus, ed. Reston, Va.: ASCE.
- ASCE, AWWA, and WEF. 2006a. *Guidelines for the Physical Security of Water Utilities*. wise@asce.org Reston, Va.: ASCE.
- ASCE, AWWA, and WEF. 2006b. *Guidelines for the Physical Security of Wastewater/Storm Water Utilities*. Reston, Va.: ASCE.
- Bahadur, R., W.B. Samuels, and J. Pikus. 2003. *Case Study for a Distribution System Emergency Response Tool*. Awwa Research Foundation Report No. 2922. Denver, Colo.: Awwa Research Foundation.
- General Accountability Office (GAO). 2003. *Drinking Water Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*. GAO-04-29, October 2003. Washington, D.C.: GAO.
- GAO. 2005. *Wastewater Facilities, Experts' Views on How Federal Funds Should Be Spent to Improve Security*. GAO-05-165, January 2005. Washington, D.C.: GAO.
- Linville, T.J., and K.A. Thompson. 2006. Protecting the Security of Our Nation's Water Systems: Challenges and Successes. *Jour. AWWA*, 98(3):234.
- Murray, R., R. Janke, and J. Uber. 2004. The Threat Ensemble Vulnerability Assessment (TEVA) Program for Drinking Water Distribution System Security. *Proc. 2004 ASCE/EWRI Congress*. Arlington, Va.: ASCE.
- Samuels, W.B., R. Bahadur, D. Amstutz, and J. Pikus. 2003. An Extended Period Simulation Hydraulic Model for Distribution System Emergency Response. *Proc. 2003 AWWA DSS*. Denver, Colo.: AWWA.
- Samuels, W.B., R. Bahadur, and R. Romani. 2009. Linking Drinking Water and Wastewater Security. *Proc. 2009 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- US Environmental Protection Agency (USEPA). 2002. *Baseline Threat Information for Vulnerability Assessment of Community Water Systems*. Washington D.C.: USEPA.
- USEPA. 2003–2004. *Drinking Water Response Protocol Toolbox: Planning for and Responding to Contamination Threats to Drinking Water Systems*. Washington D.C.: USEPA. www.epa.gov/safewater/watersecurity/pubs/guide_response_overviewpdf.
- USEPA. 2004. *Homeland Security Strategy*. Washington, D.C.: USEPA.
- USEPA. 2009. *Wastewater Response Protocol Toolbox: Planning for and Responding to Contamination Threats to Wastewater Systems*. Washington, D.C.: USEPA.
- Water Environment Federation (WEF). 2005. *Wastewater Threat Document*. Washington D.C.: WEF.
- Whitler, J. 2007. Emergency Preparedness for Drinking Water and Wastewater Systems. *Jour. AWWA*, 99(3):36.

VULNERABILITY ASSESSMENT

The Public Health Security and Bioterrorism Preparedness and Response Act (Bioterrorism Act) was signed into law (PL 107-188) in June 2002. Actually an amendment to the federal SDWA, the Bioterrorism Act required every community drinking water system serving more than 3,330 people to conduct a Vulnerability Assessment (VA), and to submit a copy of the VA to the administrator of the USEPA. The regulation also required drinking water utilities to prepare or update their ERPs to incorporate their VA results and response measures for incidents of human origin, such as terrorism and vandalism. Drinking water utilities were required to submit completed VAs to USEPA on a schedule dictated by utility size. Certification that ERPs had been updated had to be submitted to USEPA within six months of submission of the VAs.

According to USEPA statistics, approximately 4,800 water utilities fell under the mandatory requirement to conduct formal VAs and update their ERPs. These utilities serve an estimated total of 256 million people across the nation (Danneels and Finley 2004). USEPA appropriated grant funds in January 2002 (PL 107-117) to assist the largest utilities in conducting their VAs. The 449 drinking water systems serving more than 100,000 people received an average of \$115,000 per utility. Using subsequent appropriations, USEPA targeted grants to “train the trainers,” delivering technical assistance to organizations such as the Rural Community Assistance Program and WEF that assist and train personnel at thousands of medium and small utilities across the nation (Congressional Research Service Report for Congress 2005). Although it is not a requirement of the Bioterrorism Act, USEPA strongly encourages water systems to continue to review and update their VAs and ERPs on a regular basis.

The Bioterrorism Act applies to drinking water utilities but not wastewater utilities. Despite repeated efforts by some members of Congress, no comparable requirement to conduct VAs or update ERPs has yet been issued for the wastewater industry. However, wastewater systems have been encouraged by USEPA to follow the same steps voluntarily, and many utilities have done so.

VULNERABILITY ASSESSMENTS (VAs)

Vulnerability is usually defined as a characteristic of a facility or an operation that makes it susceptible to destruction or incapacitation by a threat. *Risk* is defined as “the probability that an adverse action will occur and consequences will result that negatively affect public health, the infrastructure, property, or the environment.” Risk is a function of the likelihood of an occurrence (probability) and the severity of the occurrence (criticality) (ISO 2001). Risk reduction can be achieved by either lowering the probability that an event will occur or the criticality of the event, or both.

Risk analysis procedures for infrastructure, in general, and municipal water distribution systems, in particular, have been discussed in the literature (Ezell et al. 2000a, b). Concerning water utility security, Grigg (2003) concluded that risk management in utilities is more complex than current methods can handle. More comprehensive risk and performance-based methods are needed to design more resilient and reliable systems. Specifically, risk management approaches in water utilities should involve the concepts of multiple hazards and multiple barriers.

VAs help water utilities evaluate their susceptibility to potential threats and identify actions to reduce or mitigate the risk of consequences from vandalism, insider attacks, or terrorism. The assessment of vulnerabilities includes analysis of the water source, transmission, treatment, and distribution systems. It also considers risks posed to the surrounding community related to attacks on the water system.

A VA considers the approaches and methods that could be used for a successful attack and the types of safeguards, such as physical security improvements, operational modifications, and policy changes, that would be needed to prevent the attack or lessen its impact. A VA also considers consequences of the various types of attacks so that an evaluation can be made of the extent to which resources should be expended to mount an effective defense. Consequently, more expensive protective measures can be justified to prevent an intentional contamination event that may threaten public health. Ideally, a VA is “performance-based” in that it evaluates the risk to the water system based on the performance of existing and planned measures to counteract adversarial actions.

Use of a specific VA tool is not mandated under the Bioterrorism Act. However, USEPA did specify that the following six elements be included in each completed assessment:

- Characterization of the water or wastewater system, including its mission and objectives
- Identification and prioritization of adverse consequences to avoid
- Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences
- Assessment of the likelihood of such malevolent acts from adversaries
- Evaluation of existing countermeasures
- Analysis of current risk and development of a prioritized plan for risk reduction

While USEPA only required these six tasks be included in a VA, a number of commercial tools have been developed by a variety of sources to aid in the assessment process. Some of the most widely used tools are briefly described in the following sections.

RISK ASSESSMENT METHODOLOGY FOR WATER

RAM-W stands for Risk Assessment Methodology for Water (Awwa Research Foundation 2002). This VA tool was developed by Sandia National Laboratories, with input from the Awwa Research Foundation (AwwaRF) and funding from USEPA. The tool was designed for drinking water utilities but has also been used by some wastewater utilities. The methodology was derived from techniques originally used to assess the security of extremely critical fixed assets such as nuclear weapons facilities and federal dams. The overall goal of the RAM-W assessment is to develop recommendations that lead to a cost-effective, balanced security system. Ideally, the entire analysis is driven by the threats a utility wants to protect against.

A simplified version of RAM-W for small- and medium-sized water utilities was developed a couple years after the initial version was introduced. The simplified methodology is essentially the same as that followed in the full RAM-W, without the complicated mathematical and engineering analysis. RAM-W for small- and medium-sized water utilities also presents a case study featuring a fictional small city water district to demonstrate the process.

The RAM-W approach to VA is performance based. The assessment evaluates the risk to the water system based on the effectiveness of the current security system against specific malevolent acts that are identified in the initial step of the analysis. RAM-W compares system components against each other to determine which components are the most critical. It also helps the utility prioritize security upgrades, policy changes, and operational procedure changes to mitigate identified risks.

The basic steps and questions asked in the RAM-W methodology are briefly described here.

Determine the mission and objectives of the water system. What are the highest priority services provided by the utility? These may include providing

safe water for human consumption, providing water for fire protection, and providing water for sanitary purposes. Who are the most critical customers of the utility? These can include, among others, health care facilities, the general public, firefighters, schools, and industrial sites.

Perform a systematic site characterization of the water system. Which are the most important facilities, processes, and assets of the system for accomplishing the mission (i.e., which assets need to be protected)? Where are the single points of failure—the components whose unavailability would result in a total system failure (e.g., critical intakes, reservoirs, transmission mains, pumps, wells)? What is the critical infrastructure? This includes both utility assets and non-utility assets and processes, such as electrical transmission lines and transportation systems for delivery of chemicals.

Identify and prioritize the adverse consequences that could occur. Consequences may include, among others, adverse impacts on public health, catastrophic release of onsite hazardous chemicals such as chlorine, and loss of pressurized water for fire protection. Determine which critical assets might be attacked, resulting in the undesired consequences. These could include specific pump stations, water mains, or reservoirs, as well as key control networks such as the plant SCADA system.

Identify the specific malevolent acts that could cause adverse consequences. These acts could include contamination of a portion of the distribution system, physical destruction of a critical asset, or interruption of electricity to operate pumping systems.

Assess the likelihood of these malevolent acts being carried out by defined threat sources. Who is out there that might pose a problem (defined threat source)? What, if any, is the history of malevolent acts directed against this utility? What are the identified threats in this area, such as gangs or counter-culture groups known by local law enforcement or the FBI?

Identify the design-basis threat. The design-basis threat is the specific credible threat that a utility's security system must be designed to protect against. The assessment team must determine the specific threats that a particular utility must be most concerned about. Depending on the location, size, and history of the utility, the design-basis threat could range from simple vandals to disgruntled employees to domestic or transnational terrorist groups.

Evaluate the existing security system. How effective are existing security measures and operational practices in protecting against the likely threats that were identified during the VA? The security measures and operational practices could include physical security systems, water quality monitoring systems, and security policies such as background checks of new employees.

Analyze the current risk, and develop a prioritized plan for risk reduction. Analyze the current information on utility operations, critical assets, threats, consequences, and existing security systems to determine the current level of risk. Determine whether the current risks are acceptable or whether risk reduction methods should be pursued. Evaluate strategies for

reducing vulnerabilities and risks. These may include upgrading security systems, upgrading operational procedures, and changing company policies, among others.

Additional information on RAM-W can be obtained from AWWA's website: www.awwa.org. To obtain a copy of the AwwaRF report that details the RAM-W methodology, contact AWWA Customer Service, custsvc@awwa.org. The requestor must demonstrate a need-to-know, meet other minimum requirements, and sign a nondisclosure agreement.

VULNERABILITY SELF-ASSESSMENT TOOL (VSAT)

The Vulnerability Self-Assessment Tool (VSAT) was originally developed for wastewater systems (VSAT_{wastewater}TM) by the Association of Metropolitan Sewerage Agencies (AMSA) in conjunction with several consulting firms and support from USEPA. It was subsequently modified for use in drinking water utilities (VSAT_{water}TM). A version is also available for use by utilities that operate both drinking water and wastewater facilities (VSAT_{water/wastewater}TM). VSAT is a computer software tool designed to help utility personnel assess their utility's vulnerabilities, develop priorities based on cost and feasibility of remediation, and determine potential solutions for the prioritized vulnerabilities.

VSAT guides users through the VA and risk-reduction process using an asset hierarchy and a library of threats. Assets and threats are linked and security risks are calculated from a determination of asset criticality and the probability of an incident occurring. Countermeasures are listed in a database library or can be customized for the particular utility. The impacts of various countermeasures are determined and a revised risk level is then calculated by the computer program. Finally, VSAT uses a cost-reduction analysis to help prioritize security improvements.

The following is a brief summary of the key steps in the VSAT process.

Asset characterization and identification. In this initial stage, utility managers conduct a desktop inventory of the utility's assets in each of five categories: physical plant, people, knowledge base, information technology (IT), and customers. They then assess whether, and the extent to which, a range of manmade or natural events pose a threat to these assets to ascertain a general sense of their system's vulnerabilities.

Criticality. Each vulnerability identified in the previous step is assessed to determine its criticality—the potential adverse consequences of failure should an event occur. Four levels of criticality are possible: low, moderate, high, and very high.

Existing countermeasures. After criticality is determined, specific existing measures that can be used to mitigate the vulnerabilities are identified. For example, if information-system hacking is considered a threat, existing

countermeasures such as firewalls and network monitoring can be employed to reduce the level of vulnerability.

Vulnerability rating. Next, utility managers select a vulnerability rating based on criteria that include the asset in question, the probability of threats, and the extent to which effective countermeasures are already in place. Vulnerability ratings are subjective and range from low to very high.

Risk level. Now that the two fundamental aspects of risk—consequence (criticality) and probability—have been determined, each vulnerability is evaluated using a two-dimensional matrix.

Risk acceptability. The acceptability of each level of risk is then defined. The color red on the program screen denotes relative unwillingness to accept a particular risk. Green indicates relative willingness to accept a risk.

Estimate cost of mitigation. Normally, vulnerabilities with the greatest risk receive the highest priority. Utility managers evaluate measures such as equipment, technology, structures, procedures, training, and communications activities that would effectively mitigate risks. Risks can be mitigated through either a reduction of criticality or a reduction of vulnerability.

Business continuity plan. The business continuity plan maps out the who, what, when, and how for all improvements needed to mitigate or manage identified risks. Improvement activities address the questions:

- What do we need to be prepared for in terms of manmade and natural events?
- What do we need to respond to in terms of manmade or natural events?
- What do we need to restore utility operations to normal after the response actions are complete?

Improvement activities are directed to each of the five utility assets addressed during the first step of the analysis. The highest priority vulnerabilities will be addressed first. Improvement activities can include capital investments, organizational changes, process reforms, improvements in information management, and/or enhanced communications.

The VSAT tool also has ERP modules for both drinking water and wastewater utilities. The modules contain resources for ERP tools and include direct linkages to USEPA's response protocol toolboxes. VSAT is free for utilities. Additional information concerning VSAT is available from the website: www.vsatusers.net

Tools for Small Utilities

Security Self Assessment Guide for Small and Very Small Systems. This self-assessment tool was developed by the National Rural Water Association (NRWA) and the Association of State Drinking Water Administrators (ASDWA) in consultation with USEPA. Intended to assist small system operators and local officials in reviewing their vulnerabilities and prioritizing steps to reduce risk, the tool is available in two versions: one for small systems (3,300–10,000 population served) and another for very small systems

(<3,300 people served). The tool is available electronically in both Microsoft® Word and PDF formats and can be customized for a specific utility. The program includes an emergency contact list and a phone threat identification checklist. These self-assessment tools can be downloaded from the Web site, www.vulnerabilityassessment.org.

SEMS. SEMS stands for Security and Emergency Management System. This software program was developed by NRWA, and is based on ASDWA/NRWA's above described security vulnerability self-assessment guide for small drinking water systems serving populations between 3,300 and 10,000. The program uses the same questions and prompts as the self-assessment guide, but it can also automatically generate an Emergency Response Plan based on VA answers. The SEMS CD-ROM (software program) can be purchased from NRWA.

ASSET. ASSET is an acronym for Automated Security Survey and Evaluation Tool, an assessment program developed by the New England Water Works Association (NEWWA). Intended for use by small-and medium-sized drinking water systems, ASSET is a self-guided software program designed to help drinking water systems complete a VA, as well as to improve their security and their responsiveness to a range of threats. The ASSET CD-ROM (software program) is available for purchase from NEWWA, (508) 893-7979.

Protecting Your Community's Assets: A Guide for Small Wastewater Systems. This tool was developed by the National Environmental Training Center. It is intended to assist utility operators and local officials in improving security and planning for emergency situations affecting wastewater systems serving fewer than 10,000 people.

Asset-Based Vulnerability Checklist for Wastewater Utilities. This checklist approach was developed by AMSA to provide a means for walking through a wastewater utility's assets to identify potential vulnerabilities. This abbreviated tool is well suited for small utilities with a limited number of assets.

Vulnerability Assessment Videos. USEPA and the National Environmental Training Association have produced two videos for small water systems that describe how to develop a VA through various scenarios. One video is directed to utilities serving 3,001 to 10,000 people, while the other is aimed at systems serving fewer than 3,000 customers. The videos highlight the six basic elements common to all VAs and some VA tools available to small systems. Both videos can be ordered at no cost from the National Environmental, Safety, and Health Training Association (NESHTA) Web site, www.neshta.org/PDFs/orderform.pdf.

PROTECTION OF SENSITIVE INFORMATION

Public disclosure of sensitive information contained within a VA has been a concern among water utilities since the mandate to conduct VAs was first established. According to the SDWA, information contained in the VAs

submitted to USEPA is exempt from public disclosure under the federal FOIA. In many states, however, release of this same security sensitive information by the utility is not protected by state law. Some recommendations have been published to assist utilities in addressing this issue at the state and local levels (AMWA 2002, Herrick and Blaha 2007).

RISK ANALYSIS MANAGEMENT FOR CRITICAL ASSET PROTECTION

To help compare risks among various critical infrastructures, DHS has asked each critical infrastructure sector to voluntarily implement the risk analysis management for critical asset protection (RAMCAP) methodology within their respective VA tools. RAMCAP offers a framework, provided by DHS, for analyzing and managing the risks associated with different infrastructures.

RAMCAP is a methodology to identify and quantify the various factors that may lead terrorists to select a particular target and execute a specific form of attack. For the water sector, the methodology is not limited to terrorism but involves an all-hazards approach. RAMCAP is not a VA tool. Rather, it is a framework that can be used to modify existing tools so that they provide comparable output allowing comparison of risks across critical infrastructure sectors. This comparison is useful in determining where the greatest risks are likely to occur for varying threat conditions and therefore helps identify risk reduction measures and allocate risk reduction resources. RAMCAP is being integrated into the widely used water sector VA tools, RAM-W, VSAT, and SEMS.

Additional information on RAMCAP is available at www.amwa.net/cs/water_security/ramcap_project.

REFERENCES

- Association of Metropolitan Water Agencies (AMWA). 2002. *State FOIA Laws: A Guide to Protecting Sensitive Water Security Information*. Washington, D.C.
- Awwa Research Foundation (AwwaRF). 2002. *Risk Assessment Methodology for Water Utilities (RAM-W)*. 2nd ed. Denver, Colo.
- CRS Report for Congress. 2005. *Terrorism and Security Issues Facing the Water Infrastructure Sector*. Congressional Research Service, April 25. Washington, D.C.: Library of Congress.
- Danneels, J.J. and R. Finley. 2004. Assessing the Vulnerabilities of U.S. Drinking Water Systems. *Jour. Contemp. Wat. Res. & Edu.*, 129, 8.
- Ezell, B.C., J.V. Farr, and I. Wiese. 2000a. Infrastructure Risk Analysis Model. *J. Infrastruct. Syst.*, 6(3):114.
- Ezell, B.C., J.V. Farr, and I. Wiese. 2004b. Infrastructure Risk Analysis of Municipal Water Distribution Systems. *J. Infrastruct. Syst.*, 6(3):118..
- Grigg, N.S. 2003. Water Utility Security: Multiple Hazards and Multiple Barriers. *J. Infrastruct. Syst.*, 9(2):81.
- Herrick, C., and F.J. Blaha. 2007. Information Disclosure and Security Information Protection at Water Utilities. *Jour. AWWA*, 99(11):40.
- International Organization of Standards (ISO). 2001. *Draft ISO Guide 73. Technical Management Board Working Group on Risk Management Terminology*. Geneva, Switzerland: ISO.

MITIGATION OF RISK THROUGH PHYSICAL PROTECTION SYSTEMS

Once a drinking water or wastewater utility has assessed the risks it faces from intentional acts ranging from vandalism to terrorism, and especially after a formal VA has been conducted, the next step is to determine which safeguards or mitigation measures can be put into place to protect the assets and reduce vulnerability. Mitigation measures can include physical facility improvements, operational modifications, and changes in utility policies and procedures. These mitigation measures should address deficiencies identified in the VA.

Realistically, it is not possible to eliminate risk completely. The utility must decide the level of risk that is acceptable and then determine what it will take to get to that point. All proposed mitigation measures (physical, operational, procedural) must be considered within the constraints under which the organization operates. These include financial limitations, staff resources, political restrictions, social and cultural considerations, and legal and regulatory limitations. All of these must be evaluated in a complex assessment that asks the question, “Does the degree of risk reduction exceed the cumulative costs, financial and otherwise, of the mitigation steps?” For example, triple fencing and the 24-hour presence of heavily armed guards are acceptable mitigation measures to protect a nuclear power plant. However, these same steps would be considered excessive for protection of the average drinking water or wastewater treatment plant based on fiscal, political, and even perhaps, public relations considerations.

Although triple fencing may be an excessive measure at a utility, the principle of “defense in depth” or “protection in depth” is sound and should be practiced regardless of the type of target being protected. The approach

entails using several layers of defense against a perpetrator, and not relying on a single protective barrier. This could involve a fence surrounding a facility, coupled with a camera surveillance system, and finally, securely locked windows and doors on the buildings themselves. The protection-in-depth approach not only makes it more difficult for an intruder to penetrate a facility, but also helps to ensure that the security system remains effective even if one of the defensive layers fails (e.g., a trespasser is detected by the closed circuit television (CCTV) system as he manages to successfully breach the protective fence).

Another general recommendation is that utilities should strive to obtain multiple benefits from mitigation steps that they take. Ideally the mitigation measure not only helps to protect against malevolent acts but also improves normal operations and response to unintentional emergencies such as accidents and natural disasters. One example is modifying the finished water distribution system to enhance system redundancy in the form of backup mains to feed a particular service zone. This step not only facilitates isolation of portions of the distribution system in the case of an intentional or accidental contamination incident, but also helps ensure continuity of service in the event of a water main break.

Another example is the deployment of online chlorine analyzers within the distribution system. The observation of a sudden loss of chlorine residual in a particular segment of the distribution system could suggest that a contaminant that exerts a chlorine demand has either accidentally or intentionally entered the water supply. In this instance, the chlorine monitor serves as a security device. However, the added information on distribution system chlorine residuals also helps the utility maintain the proper chlorine dosage at the chlorine booster station and thereby is useful for routine process control.

Additionally, the chlorine data assist the system operator with regulatory compliance because maintaining chlorine residual is required under drinking water regulations. This approach of deriving practical system advantages (multiple benefits) from security mitigation measures makes it easier to justify the expense of system modifications and helps ensure continued maintenance of mitigation measures during times when the threat of malevolent activity seems less likely.

Murphy and Kirmeyer (2005) proposed a “trident approach” to assist utilities in developing a security program that addresses short-term, long-term, and future facility needs while accounting for the realities of utility operation. During phase 1 of this approach, utilities take short-term actions and implement relatively inexpensive activities such as procedure and policy changes to maximize currently available security tools. Phase 2 involves long-term objectives that evaluate security, redirect resources, and institute approaches and technologies that provide a level of security adequate for today’s potential threats. Phase 3 considers future facilities and can occur concurrently with the other two phases. The goal in the final phase is to track developments in security technologies, architectural design, and construction materials and

to integrate security early on in the planning, site selection, and construction phases of future utility development.

Every consideration of risk mitigation is accompanied by the question “How will the improvements be paid for?” Following 9/11, a great deal of federal money has been directed toward reduction in vulnerability for transportation systems such as airlines, and improvements in preparedness for police, fire, and emergency medical services (EMS) responders. Very little funding from DHS has been devoted to drinking water and wastewater security improvements. Part of this may be related to the general perception that water utilities have a steady flow of money already because their operations are funded by rate payers. However, the reality is that water utilities are faced with numerous large-scale, long-term expenses, including compliance with increasingly stringent regulations and replacement of an aging infrastructure. Further complicating the security funding situation for utilities is the fact that processes for distribution of security funds vary from state to state and even county to county.

Some utilities have invested large amounts of their own money into physical security upgrades. The Birmingham (Alabama) Water Works and Sewer Board has spent \$7 million on a series of improvements including cameras, electrical security fences, access card readers, a central monitoring facility, and replacement of chlorine gas with liquid chlorine bleach as a disinfectant (Ogden 2009). Some utilities, such as the City of Atlanta (Georgia) Department of Watershed Management, have imposed a security surcharge on bills sent to residential, commercial, and industrial customers to cover additional expenses resulting from the Bioterrorism Act. Most other utilities, however, look to the federal government for assistance in paying for physical security improvements.

Some practical advice for utilities trying to obtain security grant funding is detailed in a report developed by AWWA (2007) and summarized by Spence and colleagues (2008). These recommendations include being persistent, tailoring applications, and educating decision makers concerning the security and “all hazards” needs (i.e., natural disasters, accidents) of the water sector.

With these points in mind, this chapter describes the mitigation of risk that can be achieved through enhancement of physical protection systems (PPSs). The next three chapters describe reductions in vulnerability that may be realized through operational measures; changes in policies, procedures, and training; and enhanced cyber protection.

PHYSICAL PROTECTION SYSTEMS (PPS)

The overall goal of physical security is to prevent access to facilities and assets by individuals with malevolent intent. The operational philosophy of a PPS includes four steps:

- *Deny or delay access.* If possible, completely prevent access. At a minimum, delay an adversary from accomplishing his mission long enough to permit intervention. Delay can be accomplished through the use of

physical barriers, protective devices, or operational safeguards, such as locked valves.

- *Detect an incident.* A suspicious activity or an intrusion is detected either directly by a person or indirectly through a piece of security hardware.
- *Validate the detection.* Detection is not very useful unless it can be validated to eliminate false alarms.
- *Respond.* Disrupt the activity or at least minimize damage and/or apprehend the perpetrator. For most drinking water and wastewater utilities, the primary response force is local law enforcement and the response time can be quite variable.

There are two approaches to protecting a facility using a PPS. While the differences may be subtle, they are important.

- *Deter an adversary.* Deterrence occurs by implementing measures that are perceived by potential adversaries as too difficult to defeat. It makes the facility an unattractive target, so that the adversary doesn't attempt an attack. Examples of deterrence are adequate lighting at night, posting of signs, and the use of barriers such as bars on windows. While these are measures that can help prevent theft, vandalism, or other malevolent acts, they are features that are often implemented with no additional layers of protection in the event of an actual attack. Deterrence may be effective against low-level threats such as vandalism and employee thefts. Because the effectiveness of deterrence is difficult to assess, and reliance on deterrence alone can be risky, deterrence is usually considered to be a secondary approach for PPS.
- *Defeat an adversary in the event of an attack.* The other approach for a PPS is to defeat an adversary in the event of an attack. By taking this approach to a PPS, the adversary may also be deterred. However, if he decides to proceed with the attack anyway, these PPS measures are actually strong enough to protect the assets. An adversary is defeated through *detection* and *response*.

It is important to emphasize that PPS, such as a hardened perimeter, do not guarantee security. A motivated adversary, with the proper equipment and training, can overcome any PPS. After all, despite all the security measures employed in financial institutions, banks are still robbed. The objective of a PPS is to make the task as difficult as possible.

Note, however, that while most physical protection enhancements restrict access to the facility from the outside, they do not increase the level of protection from the insider threat, which may be one of the most significant risks for drinking water and wastewater utilities. Effective physical protection devices against insiders are those that monitor or restrict an employee's or contractor's access to sensitive locations within a facility.

Another important consideration when designing PPSs is to ensure that they don't interfere with health or safety aspects of a facility's structure, such as the ability to quickly exit a building during a fire. Several excellent reference

books and training resources are available dealing with PPSs (Garcia 2001, AWWA 2006).

The following are categories of PPSs that are being employed by drinking water and wastewater utilities to decrease their vulnerability to malevolent acts.

Access Control

Access control can be used to regulate entry into a particular building and even into specific rooms or areas within a building. A number of approaches can be employed for ensuring that only authorized personnel can gain entry to various sites.

The most basic access control devices are doors and locks. Security doors are typically steel plates over a hollow cavity that can be reinforced with steel stiffeners that enhance the strength of the door and make it more resistant to blunt force. The space between the reinforcement stiffeners can be filled with materials that increase fire, bullet, or blast resistance. Hinges can be a source of vulnerability on doors, so the hinges should always be located on the interior side of a security door. To further enhance security, hinges should be welded to the door and frame rather than merely attached by screws.

Door locks can either be mechanical or electronic. Mechanical locks require keys. A critical vulnerability of key-lock systems is key control. The most substantial mechanical lock is ineffective if an adequate key control system is not in place. Obviously, keys should only be distributed to individuals who have a legitimate need for access to a particular building or room. Keys should be numbered and tracked through either a paper or computerized log system. Although not a fool-proof protection, each key should be stamped with the statement “Do Not Copy.”

Similarly, while the specific door that corresponds to the key should never be indicated on the key, keys should be imprinted with “Return To” instructions in the event of loss. Keys must always be retrieved when they are no longer needed, such as when an employee voluntarily or involuntarily leaves the company or a contractor finishes a job. Also, production and distribution of master keys should be minimized, and if a building or room is especially sensitive, the lock should be periodically rekeyed.

Electronic locks use an electric current to engage or disengage the lock. A variety of electronic locks are available, including card-reader locks, electronic combination locks, electromagnetic locks activated by a coded swipe card, and biometric locks activated by the correct fingerprint, hand geometry, voice, eye pattern (based on iris or retinal image), or signature recognition. Electronic locks can be combined with card readers to track who has entered a facility. Some higher security locks can require a combination of means to gain access (e.g., possession of a coded card and knowledge of a combination or PIN number). Electronic locks are more secure than mechanical locks because they can't be picked. Another advantage is that access rights on electronic locks can often be changed by the security administrator without

regaining possession of a key or physically changing a lock. Just as in most hotels, room-card access can be controlled electronically from a central location. Therefore, if an employee is terminated or an access card is lost, the access granted by the card can easily be suspended.

Because construction work is an almost continuous process at many water and wastewater utilities, key control for contractors is a security issue. One generally effective approach is to issue the appropriate key or access card to the construction superintendent of a particular project and make him responsible for ensuring access security for his workers. This, of course, assumes a certain degree of trust between the utility and the contractor.

Another consideration for an access control system is providing access for emergency responders to unmanned facilities or manned facilities if the operator on duty is incapacitated or otherwise unable to let them in. One approach is to install lock boxes that contain the necessary keys but are accessible only by codes or keys that fire, police, and EMS possess. The dilemma here is that the utility does not maintain direct control over the security of the first responders' pass-key. Additionally, there is the added risk that an adversary could breach the lock box and obtain access to the facility.

Windows are an access route into buildings. The most commonly used security device for windows is steel bars. Metal security screens are also used, but are lighter weight and thus not as secure as bars. Security film, which consists of a polyester coating bonded to glass surfaces to impart special resistance (e.g., bullet-proof glass), is also used to reinforce windows. Perhaps the most secure window coverings are glass blocks, but they eliminate the visibility afforded by other types of security windows.

Lighting

Lighting is one of the least expensive security measures to install. Lighting an area makes a trespasser more visible and can deter an adversary who seeks to remain undetected. Lighting makes it easier for security personnel or surveillance cameras to detect intrusion or signs of intrusion. Burning lights in a building at night can give the impression that the building is occupied, but it also may draw more attention to a critical facility or area. Still another option is motion detectors that activate lights when triggered by movement across a sensor. These can add the element of surprise and may be more acceptable in a residential neighborhood or other area where bright lights may be considered a nuisance.

Several types of lighting are available.

Incandescent bulbs are normally used indoors. They produce less light than other lights and typically have a shorter lifetime.

Mercury lights are generally used in outdoor applications. Most street lights are mercury vapor. These lights offer a good ability to distinguish between colors and therefore are helpful for making positive identification. They are also typically rated for more than 20,000 hours of life.

Metal halide lights are also used in outdoor applications. They are more

efficient electrically and provide even better color discrimination than mercury vapor. However, they normally are rated at only 6,000 hours of use.

Sodium lights are the most efficient of all of the outdoor lights, and are available in either high-pressure or low-pressure versions. The high-pressure version is more suitable for camera surveillance. The low-pressure variety produces a yellow light that is less effective for cameras.

Barriers (Perimeter Security)

Physical barriers deployed around the perimeter of an asset serve as delay systems that increase an adversary's entry and withdrawal time. For less determined and less skilled adversaries, such as vandals, physical barriers can be an effective deterrent. However, many passive barriers are not a foolproof deterrent for a determined adversary. They may delay entry by only a few seconds.

Barriers can be positioned in or around roadways, sidewalks, or buildings to control access by vehicles or pedestrians. These barriers can prevent intruders from driving a vehicle into a protected area or prevent a bomb-laden vehicle from reaching a location where detonation would be damaging. Such barriers, if in place at the time, could have prevented or lessened the impact of the 1995 truck bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Barriers are now commonly deployed around government facilities and other high-profile buildings, including some utilities.

The most commonly used barriers are discussed here.

Chains are frequently stretched across a roadway or path to prevent access by vehicles. This simple device is obviously not an absolute physical impediment because even if padlocked, a simple chain is easily cut or broken by a vehicle moving at even moderate speeds.

Jersey barriers are one of the most commonly used barriers. They are pre-cast concrete structures placed in front of a building or beside a roadway. Sometimes they are staggered within a roadway to prevent a vehicle from attaining high speeds. Jersey barriers are effective because of their mass and because they tend to become jammed under a vehicle if the vehicle attempts to ram them.

Bollards are concrete or steel post-like objects deployed approximately 4 feet apart to prevent access to an area by a vehicle.

Concrete planters can be as effective as Jersey barriers or bollards. Because they are more aesthetically pleasing, especially if they contain plants or flowers, they are often preferable in high-use areas such as the front of buildings.

Hydraulic lift barriers are employed at the entrance of, or within, a roadway to control vehicle access. The steel edge of the barrier is flush with the surface of the roadway when in the retracted position. If the barrier is activated, typically by personnel in a nearby guardhouse, the edge is elevated above the surface and physically blocks vehicles.

One-way teeth impede vehicle movement by severely damaging tires. Because the steel spikes are oriented at a sharp angle, they permit traffic to move in the desired direction, such as out of a controlled parking area. The

treadles then prevent vehicles from moving in the opposite direction through the same passage way.

Site and Building Design

Enhanced physical protection can be constructed as integral architectural features. While typically employed for high-profile, high-risk applications (e.g., nuclear facilities, government buildings, foreign embassies), protection features can be evaluated when planning for new water or wastewater facilities or substantial renovations to older buildings. These measures may include the use of specialized wall and roof materials, glass restraints and window films, blast curtains, blast-resistant coatings, blast walls, and special lighting.

Fences, Walls, and Gates

Following 9/11, and in many cases prior to that date, fences, walls, and gates have been considered essential security components of treatment plants, reservoirs, pumping stations, and other critical drinking water and wastewater facilities.

Fences are available in a variety of designs and materials. Chain-link fences are the most economical and commonly used. An advantage of chain-link fence is that it permits good visibility to the outside for personnel stationed within the fence boundary and it allows good visibility to the enclosed area for personnel patrolling the outside perimeter. Of course, this visibility may also be considered a disadvantage because it allows potential trespassers to view the protected area. The most important variable in chain-link fence is the mesh size. The smaller the mesh, the more material per unit area, and therefore the stronger the fence is. Additionally, smaller mesh is more difficult for an intruder to gain a foothold in for climbing.

While chain link fences are the most widely used, they are not as resistant to cutting or breaking as wire or iron fences. Wire fences consist of strong steel wires that run horizontally between posts and present a more difficult barrier to breach. Iron fences are still more resistant to cutting or bending than chain-link or wire. While they can also be made more attractive, they are considerably more expensive. Both wire and iron fences offer the same visibility as chain link fence.

All three types of fences can be reinforced using $\frac{3}{4}$ -inch wire cable to help prevent penetration by a high-speed vehicle. Fences can also be enhanced through the use of outriggers, barbed wire, or concertina wire. Fence posts can be anchored in concrete footings to prevent the fence from being pushed over or pulled out of soft soils.

Walls have long been used to provide boundary security. Brick or stone walls are certainly more difficult to penetrate than fences, but are also significantly more expensive. Unlike fences, walls can visually obscure the protected site from outside view. This may be advantageous in remote areas to help conceal critical assets. Walls might also be desirable in residential areas to screen facilities that neighbors may object to.

Gates provide access through walls or fences. The security of gates can be enhanced by using locking–unlocking devices ranging from simple padlocks to locks operated by PIN access codes or programmable card readers. Gate styles range from simple swinging gates to those that slide open in response to a sensor when an authorized vehicle approaches. Guardhouses provide an extra layer of screening at gates. For security considerations, a guard stationed at a gate should be positioned so the gate doesn't have to be open in order to communicate with an individual or vehicle seeking entry.

Several design features can further improve the security provided by fences, walls, and gates. For example, a perimeter fence or wall should be located at an appropriate standoff distance to provide a clear zone. Standoff distance is the distance between the outside perimeter and critical areas, such as restricted buildings, inside the perimeter. At least 6 feet of clear space on either side of a fence, wall, or gate is recommended to eliminate potential cover and concealment for intruders. Trees should not overhang fences, walls, and gates because they can provide a platform for intruders attempting to jump over the barriers. For similar reasons, fences, walls, and gates should not be located in close proximity to other potential climbing aids such as utility poles. In the case of a smaller site such as a wellhead or key valves, security can be further enhanced by fencing over the top and completely enclosing the critical area.

Intrusion Detection

Many commercially available sensors are designed to detect intrusion into either exterior or interior environments and subsequently set off an alarm. Alarms must be designed to contact someone so that a response can be implemented. Rigging an alarm system only to activate lights and whistles may provide a false sense of security. The process of detecting an unauthorized adversarial act must also include the capability of analyzing or verifying the threat. An alarm without analysis is not considered adequate detection.

The effectiveness of a physical detection system is based on

- an acceptable probability of detecting the threat,
- adequate time built into the system for assessing the threat and initiating a response, and
- low incidence of nuisance and false alarms.

Many exterior and interior detection sensor technologies are available, including

- Microwave
- Ultrasonic
- Active infrared
- Passive infrared
- Capacitance
- Sonic
- Vibration
- Fiber optics

- Video motion
- CCTV
- Balanced magnetic switches
- Proximity

Exterior Intrusion Detection Sensors

Intruders crossing a boundary or entering a protected zone can be detected by sensors placed in clear zones such as open fields, around buildings, or along fence lines. Exterior sensors must be tough enough to withstand weather conditions (heat, cold, dust, rain, wind, snow) but also sensitive enough to detect intrusion during harsh environmental conditions.

There are three types of exterior intrusion detection sensors: buried, free-standing, and fence-associated; and two categories of sensors: passive and active. Passive sensors emit no energy. Rather, they rely on the intruder to produce energy such as body heat or impact (on the ground or fence). Examples include fence vibration detectors, passive infrared sensors, buried seismic sensors, and video motion detectors. Active sensors transmit and receive energy such as microwave or active infrared. The trespasser either absorbs or reflects that energy, thereby causing a change in the amount of energy subsequently received.

Buried exterior intrusion sensors are usually placed 2 to 12 inches underground. Because buried sensors are unobtrusive, they do not act as a deterrent unless a perpetrator suspects that they are present. These sensors can be connected to an alarm, lights, or video surveillance cameras. *Pressure or seismic sensors* are passive buried sensors that don't send out active fields of energy. *Pressure sensors* are essentially containers filled with liquid and connected to a transducer. This is similar to a pressure hose at the entrance to a gas station. *Seismic sensors* are connected to conducting coils and geophones that respond to soil movement. Fiber optic cables are active buried sensors that provide an optical transmission. The cables are typically buried in a mat-like matrix. Pressure on the sensor causes disturbance of the optical transmission and triggers the alarm.

Freestanding or aboveground sensors are exterior intrusion sensors that are anchored to the ground and can act as a deterrent if located where trespassers can see them. There are two types of infrared sensors in this category. *Active infrared sensors* use infrared beams transmitted between sensors. An object breaking the beam triggers the alarm. Multiple beam systems are typically deployed. Because these sensors depend on line of sight, a number of artifacts, including fog, snow storms, dust storms, animals, and falling leaves, can trigger false alarms. *Passive infrared sensors* detect heat from living objects and trigger an alarm. These systems work best when the background temperature differs significantly from the temperature of the intruder. *Microwave intrusion detection systems* transmit microwaves from a transmitter to a receiver. As with active infrared sensors, an individual or object crossing the detection zone absorbs or reflects energy and activates the alarm. *Video motion*

detectors are still another version of aboveground sensors in that changes in the video signal trigger an alarm. These are discussed in more detail in the section on visual surveillance.

Fence-associated sensors are external sensors installed on or within fences. They are activated when fences are climbed, cut, or lifted. *Fence disturbance sensors* can detect subtle movement or vibration of a fence through the use of switches, strain-sensitive cables, electro-mechanical transducers, or fiber optic cables. *Sensor fences* are less prone to false alarms than fence disturbance sensors because they are less sensitive to minor vibrations. In these systems, taut wires (e.g., steel cables running through the fence) are anchored at their ends but have transducers or switches at their midpoints. *Electrical field–capacitance sensors* incorporate wires that carry an electrical current and run through a fence. The wires are electrically insulated from the fence. However, when the fence is approached or disturbed, the amount of electrical energy received changes and an alarm is triggered. Because this sensor is electrical in nature, nuisance alarms can be caused not only by animals and blowing debris, but also by lightning, rain, and poor electrical grounding.

Exterior intrusion sensors have a lower probability of detecting intruders and a higher false alarm rate than interior sensors because of uncontrollable factors such as wind, rain, blowing debris, animal movement, and electronic interference. Thus, in some applications, two or more sensor combinations are used to ensure an effective exterior intrusion detection screen. For example, an aboveground sensor system may be combined with a belowground sensor system.

Interior Intrusion Detection Sensors

As their name implies, interior intrusion detection sensors detect trespassers in an interior environment. Interior intrusion sensors incorporate many of the same technologies as exterior sensor systems.

Boundary penetration sensors are triggered when something intrudes on a monitored area. This can include a door opening, a window breaking, or a threshold being crossed. *Vibration-type boundary sensors* detect movement of a surface. They can be set for a specific vibration frequency such as glass breaking in a window, or concrete breaking in a wall. The actual sensors include jiggle switches or piezoelectric sensors. Depending on their sensitivity, external vibrations from trucks or electric storms could cause a false alarm. *Electromechanical sensors*, which depend on a magnetic current, are the most common of the boundary penetration sensors.

In these devices, a switch is mounted on the frame and a magnet is mounted on the corresponding door or window. Opening the door or window moves the magnet, disrupts the field, and activates an alarm. *Active infrared sensors* or *linear beam sensors* transmit beams between two sensors. The sensor detects the loss of infrared energy when an opaque object breaks the light beam. This is especially useful for monitoring a wall with multiple windows. Finally, *fiber-optic cables* can be installed in the floor or imbedded in walls

and doors. Pressure or movement disturbs the optical path and triggers the alarm. Fiber-optic sensors suffer from relatively few nuisance alarms because they are not sensitive to changes in the environment.

Interior motion detectors detect the presence of an intruder within a room. *Microwave sensors* contain a transmitter and receiver in the same unit. They detect a Doppler shift in transmitted or received energy when an object is moving toward or away from the beam. The Doppler effect occurs when frequency becomes higher as an object approaches, and lower after an object passes. The classic example of the Doppler effect is the change in the auditory pitch of a train whistle or bell heard as a train engine passes by at high speed. *Passive infrared motion detectors* sense the change in heat generated by a person crossing the line of sight. Dual technologies are commonly deployed incorporating both microwave sensors and passive infrared motion detectors in the same room. These can be designed to alarm if either sensor detects an intruder to reduce the risk of false negatives. Alternatively, the system can be set to alarm only if both sensors detect an intrusion, thereby decreasing the risk of false positives.

As with all types of PPSs, none of the interior or exterior detection sensor systems are 100 percent effective against a skilled adversary. Typical defeat measures have been anticipated for many of the technologies. For example, passive infrared intrusion systems may be circumvented by masking or insulating the intruding heat source from the infrared field of view through the use of an infrared emission-blocking cloak. Photoelectric beams may be evaded by stepping over or under the beam. Fence vibration sensors, and fences protected by strain-sensitive cables or fiber-optic systems, can be defeated by either bridging over the fence or deep tunneling under the fence. Similarly, buried exterior intrusion sensors such as in-ground fiber optic systems, balanced pressure systems, or geophone systems can be avoided by bridging over the sensor system.

Automatic Shutoffs

In certain critical facilities, if operationally feasible, intrusion alarms can be linked with an automatic shut-off function. For example, a detected intrusion into a reservoir or storage tank access hatch, well house, booster pumping station, or chemical addition building can be designed to trigger an automatic shutdown of that facility. This feature should be reserved for high-risk, critical function facilities and an effort should be made to ensure a minimum of false alarms. The shut-off function must be easily overridden should a false alarm occur.

Visual Surveillance

One of the first technologies usually considered by utility personnel trying to improve the physical security of their facilities is the installation of Closed Circuit Television (CCTV). Visual surveillance systems utilize cameras to watch single or multiple unmanned locations. The images are then transmitted to a central location for monitoring and interpretation. Surveillance systems can

be used to detect intruders or suspicious objects, validate alarms, and assess the capabilities of intruders. These systems can also provide evidence of an event for purposes of prosecution. Visual surveillance systems can be used to protect both exterior and interior areas of concern.

Important considerations for visual surveillance cameras include the field of vision (i.e., the width of an area that a camera monitors), resolution (the ability to detect small objects as measured in pixels), and whether the camera produces a color or a black-and-white image. A decision must be made as to the desired level of resolution. Specifically, do the security system designers intend for the system to have the capability to merely *detect* the presence of an intruder; *classify* the intruder as human, animal, or other object; or *identify* the specific person who is trespassing? Also important is whether the field of view is fixed or can be varied as with a pan–tilt–zoom (PTZ) camera. PTZ cameras are significantly more expensive than fixed position cameras but are particularly useful for assessing alarms.

Another consideration for a visual surveillance system is the amount of lighting required for the camera to capture an image. Obviously, this is most critical for night-time surveillance. Infrared lighting is invisible to the human eye. Commercially available infrared of a 730-nm wavelength produces a red glow at the lamp, while longer wave infrared (940-nm) is covert. Several types of low-light cameras are also available for night vision including intensified (low-light), which intensifies illumination from the scene, and thermal infrared, which requires no ambient light but rather uses differences in temperature to capture images.

After an image has been captured by a camera, it must be sent somewhere to be monitored. Image transmission can be accomplished in two ways. The system may be hardwired, in which case coaxial or fiber-optic cables physically connect cameras to viewing monitors. While hardwired transmission is generally considered to be less vulnerable to signal interception and therefore more secure, it is obviously difficult to hardwire remote locations.

The second option is wireless transmission in which the signal is transmitted over the air via microwave, optical systems, or radio waves. Depending on the specific technology, wireless transmission can require direct line of sight or retransmission via amplifiers or repeaters.

Still another factor in visual surveillance is monitoring of the images. Provision has to be made for someone to monitor the pictures being transmitted. Decisions have to be made concerning whether the images will be viewed on a rotating or split screen basis. Policies also have to be established for the response to an incident observed via CCTV. For example, does the individual monitoring the CCTV notify police if they observe something suspicious? Should the surveillance system be designed so there is an automatic shutdown of the facility if a suspicious event is detected via visual surveillance?

In reality, it is difficult to expect one person to diligently monitor one or more television screens over an eight-hour period. For this reason, the use of digital video motion detection has become increasingly popular. In this

technology, which can be applied in either an exterior or interior environment, a computer analyzes the video stream for the presence of motion within the camera's field of view. The sensor detects changes in the monitored area by comparing the current scene with a pre-recorded stable scene of the same area. The system analyzes the change between the two scenes and determines whether the difference is significant. Detection of significant motion can be used to signal an alarm and/or activate a video recording device. This level of automation always presents a possibility for false alarms caused by unstable camera mounts, animals, blowing debris, or changes in illumination from the lights on passing vehicles. Some visual sensors have been designed to reduce the possibility of nuisance alarms through pattern recognition so only objects having approximately the size and shape of humans, and traveling at the typical speed of humans, would trigger an alarm.

A final consideration in designing a visual surveillance system is to provide for archiving video images. It is useful to be able to review images captured by the cameras. Recording can be continuous or initiated only when the appropriate motion is detected by a motion detector camera. Playback options can include search features, a variety of play speeds, and the ability to freeze on a single frame.

A camera system can become a legal liability if improperly applied because of the public presumption that an area is being protected by a visual surveillance system. If a citizen is assaulted while walking around a reservoir apparently equipped with surveillance cameras, or with posted signs indicating that the site is monitored 24-hours a day, and in actuality no visual surveillance system is in place, the utility may be judged to be negligent. This dilemma has discouraged the practice of deploying fake cameras as a deterrent device.

It is also important to be aware of the interdependencies of surveillance equipment and other systems. If electrical power is lost, alarms and cameras should be supported by a backup power supply or battery pack to ensure continued coverage.

EXTERNAL ASSET PROTECTION

Drinking water and wastewater systems are difficult to protect because they contain so many assets and components that are external to the main treatment plant and are widely dispersed geographically. Many of these assets, such as the hundreds or thousands of service connections and fire hydrants in a municipal drinking water system, represent a vulnerability. Each service connection or fire hydrant represents a site where a contaminant could be pumped into the distribution system and, depending on the virulence and dosage of the contaminant, could seriously impact the safety of a number of consumers.

While it is impossible to completely protect these assets, PPSs are available that may detect tampering or at least make access to these assets more difficult.

Service Connections

Disconnecting a domestic or industrial service connection after the meter and intentionally backflushing a contaminant into the distribution system is a fairly low-tech task (*Wall Street Journal* 2001). The only practical obstacle is to provide sufficient pressure, using a commercially available, inexpensive pump, to overcome the ambient pressure in the municipal distribution system. An approach for detecting such an intrusion is the installation of automatic water meter readers capable of backflow, leak, and tamper detection. These devices are in various stages of development. The American Water Company is exploring the possibility of having this information relayed back to the utility through the automatic meter reading fixed network (Schneider 2006).

Fire Hydrants

Fire hydrants also represent a vulnerable access point where a contaminant could intentionally be introduced into the distribution system. While the introduction of a contaminant into a single hydrant is probably not capable of negatively affecting the entire municipal network, it could certainly affect a significant portion of the pressure zone into which the contaminant is introduced. A number of accidental back-siphonage incidents involving hydrants have been documented. Some of these involved backsiphonage of pesticides into the municipal water system caused by exterminators who connected their devices to hydrants, but check valves either failed or weren't used at all. Several documented cases describe instances of fire suppression foam being inadvertently pumped into the municipal water distribution system from a fire pumper trunk (States et al. 2008).

Hydrant security can be improved using several approaches.

Hydrant locks are devices that can be opened by authorized personnel such as firefighters or water utility employees who have been issued the appropriate equipment, but are much more difficult for the public to access.

Cap locks are mechanical or magnetic locks installed over the operating nut of the hydrant. The lock does not have to be removed to use the hydrant. Rather, the hydrant can be operated using a special type of wrench.

Steel straps are locks that are padlocked over the operating nut of a hydrant. The straps are locked using a padlock, and in order to operate the hydrant, the padlock must be opened and the strap removed. Firefighters and utility personnel must be issued the appropriate key for this device.

Hydrant backflow-prevention devices are another means of securing hydrants. In this case, a check valve is retrofitted to the interior of a hydrant already in place, or can be purchased in a new hydrant. Just like a backflow-prevention device on a distribution system service line, the check valve seals and prevents someone from intentionally overcoming the system pressure at the hydrant and pumping a substance backward into the distribution system. These devices can also protect against substances that are intentionally introduced into the dry barrel of a hydrant from being subsequently drawn into the distribution main by the Venturi effect. Hydrant backflow-prevention devices

not only guard against intentional backflow through a hydrant, but also protect against accidental backflows.

Finished Water Reservoir Covers

Under the Long-Term 2 Enhanced Surface Water Treatment Rule (LT2ESWTR), finalized in 2005, open finished water reservoirs across the United States either must be covered to prevent contaminants from entering the finished water, or the finished water must be treated again before being distributed to remove contaminants that may have entered the water during storage. This requirement should offer some protection against both accidental and intentional contamination of reservoirs. However, because many covers added to preexisting reservoirs are made of thin plastic materials, such as polypropylene, these barriers can easily be breached.

Manhole Covers

Manholes are located approximately every 300 feet along most wastewater collection systems lines. This presents an incredible number of access points where explosive, incendiary, or toxic substances could be intentionally injected into the wastewater system. The National Research Council (NRC) recommended installation of locking manhole covers to reduce this risk (NRC 2002). The NRC also suggested installation of barriers or gratings to prevent movement of people or vehicles within large sewers. While it may be impractical to secure the thousands of manhole covers within a municipal system, it might be feasible to fortify those manhole covers in high-risk or high-profile locations such as key government buildings and military bases. Several approaches are employed for securing manhole covers.

Tack welding has been used to secure manhole covers prior to visits by dignitaries. The objective is to prevent adversaries from placing explosive devices under the street or to prevent persons from hiding in the manholes. The down side to this practice is that the welds have to be manually removed every time maintenance is required.

Bolt-type locking devices consist of bolts that anchor the manhole cover to the frame. The bolts are designed with heads that require specialized keys or wrenches to open.

Pan locks can be used to prevent access into a manhole and prevent injection of substances into the collection system. The pan is installed with its rim resting on the manhole cover frame and is locked into place with a special lock. The manhole is placed on top of the pan and can still be easily removed.

SECURITY GUARDS AND PATROLS

During the first year or two following the events of 9/11, when public concerns over terrorism were high, many drinking water and wastewater utilities employed guards to augment their physical security measures. Some utilities subsidized their local police departments to have uniformed officers, and in some cases their official vehicles, continuously present on utility property.

Others contracted private security firms for unarmed or armed guards or security patrols. Still other utilities, especially government-related utilities, encouraged local law enforcement to increase their patrols and general vigilance. Because the hiring of off-duty police officers or contract security personnel is a relatively expensive proposition, many utilities have since discontinued this practice. A number of water systems continue to use unarmed utility personnel as gatekeepers to document the passage of people and vehicles onto utility grounds, thereby controlling access.

Concerning the use of armed guards, in some legal jurisdictions, local codes prohibit firearms in public facilities such as treatment plants. Liability issues regarding security staff and those they are intended to protect also need to be considered. Accidents involving armed guards, especially inadequately trained ones, can be extremely costly from a personal level and also from a legal liability perspective.

Some major water utilities in the United States maintain their own extensive police forces. The New York City Department of Environmental Protection (DEP) has an environmental police force of more than 200 officers. This force is more than 100 years old and is charged with protecting New York City's 1,972-square-mile watershed in upstate New York, as well as the city's extensive municipal water infrastructure (New York City DEP 2006).

All security personnel should be clearly identified with a badge and uniform, and they should be well trained and cleared using employee background checks. Training should include incident response measures such as activating an alarm, activating automatic gates or barriers, and contacting utility management or police; and behavior awareness, which would alert them to patterns that could indicate that the facility is under surveillance. Security staff should be provided with adequate communications tools and current contact information so they can report incidents to utility management and law enforcement. They should also be familiar with the relevant portions of the utility's ERP and what role they would be expected to perform in the event of an emergency. The areas to be patrolled must be clearly defined and the timing of patrol rounds should be varied to prevent potential intruders from determining when certain areas are protected.

CONCLUSIONS

PPSs can harden a target, deter vandals, and possibly delay intrusion by skilled adversaries. However, they can't be counted on to guarantee that a well-trained, motivated perpetrator will not be able to gain access to facilities. This is especially true for drinking water and wastewater facilities, which are numerous and geographically dispersed. Utilities should not rely solely on physical protection because acquisition and installation of PPS is often restricted by financial, political, and cultural factors. To more fully mitigate risk, utilities must strive to reduce their vulnerabilities to intentional acts, natural disasters, and accidents through operational measures; changes in

policies, procedures, and training; and through enhanced cyber protection. Recommendations for these mitigation measures are described in the following chapters.

REFERENCES

- American Water Works Association (AWWA). 2006. *Security Hardware*. AWWA online course (SEC003). Denver, Colo.: AWWA.
- AWWA. 2007. *Security Funding Opportunities: Lessons and Observations from Successful Water and Wastewater Utilities*. Denver, Colo.: AWWA. www.awwa.org/government.
- Crime Prevention through Environmental Design (CPTED). www.cpted-watch.com/Industrial.html.
- Garcia, M.L. 2001. *The Design and Evaluation of Physical Protection Systems*. Boston. Butterworth-Heinemann.
- Luthy, R.G. 2002. Bioterrorism and Water Security. *Environ. Sci. & Technol.*, 36, 123A.
- Murphy, B.D., and G.J. Kirmeyer. 2005. Developing a Phased Distribution System Security Enhancement Program. *Jour. AWWA*, 97(7):93.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Research Council. Washington, D.C.: National Academies Press.
- New York City Department of Environmental Protection (DEP). 2006. New York. www.nyc.gov/dep.
- Ogden, L.T. 2009. Security Infrastructure Improvements at the Birmingham Water Works Board. *Proc. 2009 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Schneider, O. 2006. New Monitors for Improved Distribution System Operations. *Proc. 2006 AWWA Water Quality Technology Conference*. Denver, Colo.: AWWA.
- Spence, S., K. Smith, and K. Morley. 2008. Finding the Funding for Security Upgrades. *Jour. AWWA*, 100(1):36.
- States, S., J. Carroll, G. Cyprych, K. Hayes, J. Kuchta, M. Little, A. Pyle, M. Stoner, C. Westbrook, and L. Casson. 2008. An Accidental Contamination Event in the Pittsburgh Drinking Water Distribution System (A Case Study). *Proc. 2008 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- U.S. Environmental Protection Agency (USEPA) Security Product Guide. Washington, D.C. www.epa.gov/safewater/security.
- Wall Street Journal*. 2001. Water Utility Officials Fear Backflow from Terrorists. *Wall Street Journal*, December 27.

MITIGATION OF RISK THROUGH OPERATIONAL MEASURES

Utilities can reduce vulnerability to terrorism and other intentional acts by employing operational security measures. These same measures will also reduce the impact of natural disasters and accidents. A strong motivation for this approach is that operational and design changes can often be made at a much lower cost than installing expensive physical security features and can provide additional benefits to the drinking water or wastewater system. Some operational mitigation measures are discussed in this chapter.

SYSTEM REDUNDANCY AND BACKUPS

Drinking water and wastewater systems designed with a high degree of redundancy in processes and in individual pieces of equipment are inherently more resilient to a variety of manmade events, accidents, and natural disasters. Single points of failure in a water system represent especially vulnerable sites and are typically a focal point in formal VAs. For example, if all of the finished drinking water leaving a treatment plant must first pass through a single clearwell in order to reach the distribution system, or if all of the sewage from a particular section of the wastewater collection system must pass through just one lift station, this is a facility whose loss could significantly jeopardize a utility's ability to provide critical services.

Whenever possible, drinking water utilities should establish alternate raw water sources and intakes. The ability to activate normally unused supply wells or a backup intake on another river or lake can be critical in ensuring continuity of service if the quality of the usual raw water supply or intake has been compromised by an intentional act or accident. The ability to utilize a

backup treatment or pumping facility can also be important if an intentional or accidental event, or a significant mechanical failure, puts the primary facility out of commission.

In wastewater treatment plants, if offline flow equalization/storage basins are available, a contingency plan can be prepared to store any influent wastewater in these that is suspected of being contaminated. The purpose for this is to prevent the biological treatment process from being damaged or destroyed by toxins in the raw wastewater. Ideally, the basins should be able to contain eight hours of storage at the average daily flow rate. The basins should be situated to receive flow following preliminary treatment but prior to primary treatment.

In a drinking water distribution system, each service area or pressure zone should be served from two finished water reservoirs or tanks, or directly from the treatment plant, rather than from just one source. Ideally, water should be able to reach any service connection from both directions in a street main. These capabilities are advantageous not only for security concerns but also for maintaining continuity of service during accidental incidents such as water main breaks, or during routine maintenance, such as line flushing or pipe replacement.

Drinking water utilities should have the ability to isolate individual finished water reservoirs or storage tanks quickly. As recommended in the USEPA Response Protocol Toolbox (USEPA 2004), isolation is one of the recommended initial operational response actions that can be taken when a contamination threat has been deemed “possible” by the initial incident commander, who may be the water utility emergency response manager. The decision to isolate a storage reservoir or tank will be easier if the distribution system has adequate redundancy and the affected service area can still be fed from another finished water storage structure or from the plant. The ability to quickly isolate a reservoir, tank, or even a portion of the distribution system will depend on good documentation of valve locations. Critical valves must be able to be operated manually and, if possible, remotely to achieve isolation more quickly and to reduce the flow of any contaminant to customer taps. This ability will be enhanced by a regular valve exercise program.

Standby tanks, basins, mechanical equipment, and electrical components should be part of the redundancy built into drinking water and wastewater treatment plants. To ensure that backup capacity is available when needed, the routine use of these components should be rotated. Maintenance of critical spare parts is an extension of redundancy that can help ensure continuity of operation during an emergency. Ideally, these parts should be stored in a location separate from the operating equipment so that the same fire, flood, or intentional act doesn’t destroy both operating and spare equipment.

In wastewater systems, redundancy should ideally be extended to the entire treatment facility so the treatment process consists of multiple parallel trains. In this case, one treatment train would remain operational if another was damaged. Each unit process should consist of two or more process units

operating in parallel. Pumps, motors, and chemical feed equipment should be designed in multiples, with sufficient capacity to handle peak flows if the largest piece of equipment is damaged or taken out of service. A high degree of redundancy should also be considered for critical processes such as biological treatment or disinfection systems.

In both drinking water and wastewater utilities, a sufficient quantity of treatment chemicals should be stored at the facility to permit 30 days of treatment without additional shipments. This helps to protect against loss of treatment capability resulting from accidental or intentional interruption of supporting critical infrastructures such as the transportation system, as well as incidents that could occur at the facility itself. Additionally, at least two storage tanks should be available for each chemical to provide an emergency backup.

The critical dependence of drinking water and wastewater facilities on purchased electricity provides a strong argument for maintenance of onsite backup electrical generating capability. The existence of two independent main power supplies from the same electrical utility is not a sufficient protection if the entire power grid is affected by an emergency. Backup power generation capability should be available to provide at least 48 hours of service for processes critical to maintaining adequate treatment, as well as ventilation, lighting, and the use of power tools for maintenance. If such a capability is established by a utility, it is important that generators be exercised weekly under realistic loading conditions so they can be depended on during an emergency. The utility should also install an automatic transfer switch for rapid transition to backup power when primary power fails. A lack of onsite generating capability, and maintenance problems with the backup generators that were available, were key factors in the problems encountered by a number of wastewater and drinking water utilities during the widespread electrical grid failure that occurred in August 2003 in the northeastern section of the United States.

Additionally, in terms of power continuity, the utility should install uninterruptible power supply systems for process controls, SCADA systems, alarms, computer networks, and communications systems.

The establishment of interconnection supply agreements with neighboring water utilities to provide treated (or raw) water during emergencies is another approach to compensate for loss of production or delivery capabilities in a drinking water system.

A number of states recommend that drinking water systems store at least one day's supply of finished water to ensure continued availability of water for domestic needs and fire protection in the event of a situation that significantly interferes with the utility's ability to obtain or adequately treat raw water. In some systems where backup raw water supplies, backup treatment facilities, or adequate interconnects with neighboring utility's are not available, contingency storage of more than one day's supply has been the practice. Of course, care must be taken to ensure that prolonged storage of

finished water does not result in deterioration of water quality, such as an excessive production of disinfection by-products (DBPs).

Redundancy enhancements will benefit the utility during a manmade emergency and will also be beneficial during more likely accidental events or natural disasters.

CHEMICAL TREATMENT COUNTERMEASURES

A particular safety concern for both wastewater and drinking water utilities that use gaseous chlorine is the accidental or intentional release of this treatment chemical into the environment. Chlorine cylinders should be stored in a secure location and hidden from the view of anyone outside of the facility's secured perimeter. Chlorine should be stored separately from other chemicals to avoid potential chemical reactions. Continuous gas leak detectors should be installed to monitor for leaks along with containment structures and chemical scrubbers to protect against physical damage inflicted (accidentally or intentionally) on chlorine gas storage tanks. Additionally, while utility personnel should be trained and equipped to respond to minor leaks, coordination should be made with the local HazMat team to deal with major leaks. In some utilities, the HazMat team refamiliarizes itself with the utility's chlorine facilities, and rehearses its emergency response, on an annual basis.

Many drinking water and wastewater utilities have opted to further reduce risk by switching from disinfection with chlorine gas to less hazardous liquid chlorine (sodium hypochlorite), solid chlorine (calcium hypochlorite), or onsite generation of liquid chlorine, which eliminates the storage of chlorine gas. The transition from gaseous chlorine to sodium hypochlorite was made in the author's drinking water utility in Pittsburgh in 1999. The change was made at the treatment plant and at 10 booster chlorine stations located throughout the distribution system. The results have been very positive, and the risks of accidental or intentional exposure to highly toxic chlorine gas have been significantly reduced for utility employees and the surrounding community.

Although sodium hypochlorite tends to cost a little more than gaseous chlorine, this cost for the Pittsburgh system has been offset in large part by the reduced dosage requirements for soda ash needed to raise pH at the end of the treatment process. While sodium hypochlorite acts identically to gaseous chlorine as a chemical disinfectant, sodium hypochlorite tends to elevate the pH of the water, and gaseous chlorine depresses pH. Therefore, with the use of liquid chlorine in Pittsburgh, a smaller dosage of soda ash is required to elevate finished water pH to a level of 8.4, which is the pH target for finished water in the Pittsburgh system.

The National Association of Clean Water Agencies (NACWA), under the sponsorship of DHS, has developed a chlorine gas decision tool. The tool is a CD-ROM designed to provide both drinking water and wastewater utilities with a user-friendly, but thorough, means of evaluating alternatives to chlorine gas disinfection. The CD-ROM is free and can be ordered from NACWA's Web site: www.nacwa.org.

Maintenance of a suitable chlorine residual throughout the distribution system is another operational mitigation measure that can be employed to protect against intentional or accidental contamination. This recommendation was endorsed by the National Research Council's report on the role of science and technology in countering terrorism (NRC 2002). A number of microbes believed to be candidate agents for intentional or accidental contamination of potable water are susceptible to chlorine inactivation. For example, *E. coli* O157:H7, *Salmonella*, and *Shigella* are bacteria that can be inactivated by chlorine levels typically found in drinking water distribution systems in the United States. Other microbial agents, such as anthrax spores and *Cryptosporidium* oocysts, are much more resistant to chlorine and chloramines. For most of the biotoxins there is still little information available, at least in the open literature, concerning susceptibility to chlorine. USEPA guidelines for municipal water systems using surface water recommend a residual chlorine concentration in the distribution system ≥ 0.2 mg/L, and a maximum allowable concentration of 4 mg/L (USEPA 1998).

One line of defense against microbial contamination is to maintain a significant chlorine residual in the distribution system and to increase this level in times of perceived or real danger (Brosnan 1999). For systems having trouble maintaining a chlorine residual farther out in the distribution network, an effective remedy can be construction of chlorine booster stations.

Utilities may also want to develop the capability of bringing temporary disinfection resources to contaminated sections of the distribution system. This can be accomplished through the use of portable chlorine pumping and injection systems.

Temporarily increasing chlorine levels during an emergency may increase disinfectant by-product levels. Current MCLs are 80 mg/L for trihalomethanes and 60 mg/L for haloacetic acids. However, the disinfectant by-product MCLs are based on lifetime exposure and do not necessarily constitute a restriction for short-term emergency response to a suspicion of contamination.

It should be noted that the use of a disinfectant residual as a defense against microbial contamination of the distribution system is somewhat less effective for public water supplies using chloramines, because chloramines are weaker disinfectants than free chlorine. Systems using chloramines may want to consider temporarily switching to free chlorine during periods of heightened alert or in response to a credible contamination threat. USEPA published a case study describing the emergency response, decontamination, and recovery planning of a large, unnamed combined water and wastewater utility located in the southeastern coastal United States (USEPA 2008). One of the operational measures used by this utility prior to the arrival of an anticipated hurricane is to switch from chloramines to free chlorine. The purpose is to provide better disinfection to minimize contamination impacts, and to enhance monitoring of the distribution system during the incident and

recovery phase as changes in free chlorine levels are more sensitive to the presence of contaminants than are changes in chloramine concentrations.

BACKFLOW-PREVENTION PROGRAM

Another operational measure that can reduce vulnerability in a drinking water system is maintenance of a backflow-prevention program. This could include installation of backflow-prevention devices at private residences as well as at industrial sites so that intentional and accidental injection of contaminants directly into the distribution system becomes more difficult. However, a perpetrator knowledgeable enough to intentionally inject a contaminant against system pressure into the distribution system may also be capable of circumventing a backflow-prevention device.

Some municipal water systems have been criticized for lax enforcement of backflow-prevention regulations. In one large US city, state law has required that backflow devices be installed on apartment buildings and commercial buildings since 1981. One- and two-family homes are exempt. However, a recent investigation of city records revealed that as many as 85,000 of these buildings have still not installed the devices and that many of the buildings with the devices do not meet the annual requirement for annual testing of the valves (DePalma 2007).

SYSTEM PLANS AND MODELING

Should a suspected accidental or intentional contamination event occur in either the drinking water distribution system or the wastewater collection system, it is useful to be able to predict where the contaminant slug is traveling. One response that can be considered in such an event is isolation of portions of the distribution or collection network to prevent the spread of contaminant. An accurate knowledge of the hydraulics of the distribution or collection system and accurate information of the locations of critical valves is essential for accomplishing either of these tasks.

Correspondingly, an accurate system plan should be maintained by the utility indicating the precise locations and status (open versus closed) of all system valves. Many utilities are developing GIS-based systems to assist in this process. In addition to maintaining an accurate database for this information, it is important to maintain these system components through a regular valve exercise program.

Knowledge of the flow of water through distribution and collection systems can be greatly enhanced through the use of hydraulic models. A number of models are commercially available and provide information on direction of flow and flow rates under a variety of conditions.

In addition to basic hydraulic models, USEPA has developed and made available at no charge several contaminant models that can be used in conjunction with basic system hydraulic models to better predict the movement

of contaminants. PipelineNet is a model that allows the user to predict the direction and rate of movement of contaminants in a drinking water distribution system. SewerNet is a similar model that predicts the movement and concentration of contaminants in a municipal wastewater collection system. Additional information on these water contamination models is available at <http://eh2o.saic.com>.

Information on the hydraulic characteristics of distribution systems can also be obtained using tracer studies. Furthermore, the accuracy of the hydraulic and contaminant models previously discussed can be determined, and the models can be calibrated, with tracer studies utilizing fluoride, sodium chloride, or other innocuous materials. Basic information on hydraulic modeling and tracer studies has been summarized in a USEPA guidance document (USEPA 2005).

REFERENCES

- Bernosky, J. 2002. *Water System Security: A Field Guide*. Denver, Colo.: American Water Works Association (AWWA).
- Brosnan, T., ed. 1999. Early Warning Monitoring to Detect Hazardous Events in Water Supplies. *Risk Science Institute Workshop Rep.* Washington, D.C.: International Life Sciences Institute.
- DePalma, A. 2007. Thousands of Buildings Lack Required Water Valve, New York Records Show. *New York Times*, May 19.
- Murphy, B.M., and G.J. Kirmeyer. 2005. Developing a Phased Distribution System Security Enhancement Program. *Jour. AWWA*, 97(7):93.
- National Association of Clean Water Agencies (NACWA). 2006. *Chlorine Gas Decision Tool for Water and Wastewater Utilities*. Washington, D.C.: NACWA.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academies Press.
- US Environmental Protection Agency (USEPA). 1998. Disinfectants and Disinfection Byproducts. [Rules and Regulations]. *Federal Register*, December 16, 1998. vol. 63, no. 241, pp. 69389–69476.
- USEPA. 2005. *Water Distribution System Analysis: Field Studies, Modeling and Management*. Washington, D.C.: USEPA.
- USEPA. 2008. *Decontamination and Recovery Planning: Water and Wastewater Utility Case Study*. Office of Water, EPA817-F-08-004. Washington, D.C.: USEPA.

MITIGATION OF RISK THROUGH POLICIES, PROCEDURES, AND TRAINING

The least expensive approach to reducing vulnerability to damaging intentional acts, accidents, and natural disasters is typically through changes in company policies and procedures, and provision of additional training to personnel. These are also the mitigation steps that can be implemented the most rapidly. This chapter identifies specific policies, procedures, and training programs that can be implemented at drinking water and wastewater utilities to reduce the risk from intentional or unintentional events.

RELEASE OF SENSITIVE INFORMATION

While water companies normally do not deal with classified information as do certain government agencies, some information about utility facilities and the operation of a water or wastewater system might be useful to individuals or groups intent on damaging the utility or its personnel. In particular, utilities should avoid listing sensitive information, such as specific locations of system components, on Web sites, in consumer confidence reports, and in other materials released to the public. Utilities should also tightly control the availability of facility blueprints, diagrams, GIS system maps, and other physical asset information. Additionally, details of utility security measures should never be shared with the media or public. Employees should be instructed to scrutinize all requests for potentially sensitive information concerning the water system. This includes verbal, written, telephone, and Internet queries.

Obviously, a utility must accommodate the needs of individuals and organizations that have a legitimate need for water system information. These include bidders on construction projects and contractors already working for the utility. However, utility managers need to emphasize to legitimate requestors the importance of keeping sensitive information about the utility confidential. Several approaches can be used for controlling information that must be distributed to contractors, consultants, and other outside companies, such as limiting the information provided in contract drawings and specifications to the minimum amount required to produce an adequate bid. Further information can be provided once a contract is awarded. Additionally, when sensitive documents are given to contractors, regulators, or other outside organizations, a confidentiality statement can be attached indicating that the document may not be reproduced or redistributed without authorization from the utility.

Utilities are encouraged to establish a formal information management policy (Herrick and Blaha 2007). Under this policy utilities may consider classifying information based on three levels of sensitivity:

- *Confidential information*—information that could be used in planning an attack on utility assets. This type of information requires the greatest possible restriction from general release.
- *Restricted information*—data, information, and records that should not be broadly released to the general public but may be disclosed to utility representatives or other individuals with a “need to know.”
- *Public information*—information provided to the public with few or no restrictions. This includes, among others, water quality reports, service brochures, and press releases.

Additional guidance on protecting water system security information has been provided by USEPA (2003).

RECORDS MANAGEMENT

The large number of documents maintained by an organization as complex as a public utility require that an effort be made to ensure that sensitive information is protected. Hard copies of sensitive materials should be stored in locked, fireproof metal file cabinets. Only authorized personnel should have access to these files. Critical records should also be duplicated and stored in an offsite location.

Confidential documents, such as the utility's VA, should be segmented prior to distribution. For example, rather than being given a copy of the entire report, utility or contract personnel working on a specific project associated with the VA need only have access to the portions of the document relevant to their work.

A particular issue associated with management of sensitive records by public utilities is the requirement to provide information to the public under the federal Freedom of Information Act (FOIA), which was passed by

Congress in 1966 and amended in 1974, and various state “sunshine laws.” The existence and strength of sunshine laws varies from state to state. An exemption for security-related information was included in the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), which exempts the federal government from having to release sensitive utility information such as VAs. However, because state laws are typically not superseded by federal law, utilities cannot rely on the federal FOIA exemption to guarantee their own ability to protect sensitive information. A number of states have amended their statutes to restrict release of security-related information. Each utility needs to become familiar with their particular state’s policies to determine the best approach to protect documents.

CRISIS MANAGEMENT HUMAN RESOURCES PROGRAM

As indicated in many VAs, insiders are the individuals who are usually considered to pose the greatest potential danger to an organization such as a utility. Insiders include disgruntled current and former employees as well as contractors working for the utility. Insiders present a special risk because they have an intimate knowledge of the workings of the system and its vulnerable points, and they have ready access to facilities. As indicated in chapters 2 and 3, a number of intentional acts committed by insiders have had a serious impact on drinking water and wastewater systems. This includes the intentional contamination of a drinking water system in Pittsburgh in 1980 (Moser 2005). In this incident, an employee is believed to have pumped the pesticide chlordane into a distribution system transmission line.

Establishment of a crisis management human resources program could help decrease the risk of malevolent acts being committed by disgruntled employees. These programs typically involve training for supervisors on how to recognize behaviors that might signal problems, as well as briefings for employees on what to do if they observe suspicious activity or behavior among their co-workers. Such a program may also offer an employee assistance program and include measures for troubled employees such as early intervention, counseling, restricted duty, restricted access to sensitive areas, or removal from the workplace.

Identification of Employees and Visitors

The practice of issuing badges or photo identification cards is a commonly used method for identifying and keeping track of individuals in many organizations. By using different backgrounds or symbols, badges can also be used to distinguish between various groups (e.g., employees, visitors, contractors). Badges can range from simple photo IDs, to electronic identification devices that electronically control access, to tracking systems that monitor an individual’s movement within a facility. Single-use visitor badges can be issued on

which the badge changes color, or all text disappears, after 24 hours. Badges can be color coded to indicate areas to which an individual has been granted access. Some electronic access badges can even be programmed so card readers permit access to certain areas only during specific time periods. Used in this way, badges are actually a component of an access control system.

If badges are used as a security control method, a standard procedure to maximize their protective effectiveness needs to be developed. For example, employee and contractor badges should include a current photo along with the individual's name and position. All badges should include a prominent logo that is easily identifiable from a reasonable distance. Badges should be displayed at all times, especially when entering or exiting a facility or sensitive area. Security personnel should maintain records of everyone who has been issued a badge. A procedure should be developed for handling the issue of lost badges. And, finally, when an employee or contractor terminates their affiliation with the utility, badges, along with keys, must be collected.

Employee Background Checks

Given the amount of planning that has gone into some terrorist attacks in the past, it is not inconceivable that a perpetrator could seek employment at a business or company being considered as a future target. It is also plausible that a current employee could experience financial, personal, or criminal circumstances that might induce him to jeopardize the utility for his personal benefit.

A step that utilities can take to help guard against these threats is to conduct initial and periodic background checks on company personnel. Utilities can also require that onsite contractors do the same. Specifically, background checks should be aimed at detecting false identities and identifying individuals who have a criminal past or a history of behavior that could pose a security risk to the water utility. Laws addressing employee and contractor privacy issues vary from state to state, so it is necessary to research the legal implications before instituting a background-check policy. Background screening must be lawfully conducted and consistently applied to all prospective or current employees.

Background checks can be tailored to the sensitivity of the position that a candidate is applying for or that an employee currently holds. The check can be conducted in-house or through companies that specialize in this service. The types of information collected as part of a background screening typically include criminal records, court records, educational background, previous employment, character references, licensing documentation, and credit history.

In some states, such as Pennsylvania, a basic criminal record background check is a requirement for all drinking water treatment plant and distribution system operators when they renew their state certification every three years. The records check is conducted by the Pennsylvania state police. This requirement went into effect following the events of 9/11.

Background screening can be a controversial topic. Unions and individual employees may raise objections to screening. Often, applicants and employees have concern over confidentiality of information and how the information will be used. Each utility will have to determine the criteria by which an individual is flagged “at risk” as a result of a background check and what consequences result from that classification. Some states require an individual’s consent prior to initiating a background investigation on them. Therefore, it is important to investigate legal and contractual requirements before establishing a background screening program. Failure to do so could expose a utility to lawsuits.

In January 2007, DHS Secretary Michael Chertoff requested that the National Infrastructure Advisory Council (NIAC) research and provide policy recommendations on the vulnerabilities of critical infrastructures from internal sabotage (Water Security Channel 2007). He asked NIAC to clarify potential conflicts between privacy laws and counterterrorism policy in order to better screen employees in critical infrastructure sectors. In the words of the secretary, “We have to be concerned not only about external threats to our critical infrastructure but the possibility of sleepers within the infrastructure who might turn out to be the source of threats.”

Security and Emergency Preparedness Awareness Among Employees

Every employee should be made aware of the fact that security and emergency preparedness is an important part of their job. The goal is to create a culture of security and emergency preparedness in the workplace. The ultimate goal is to establish an all-hazards approach to risk management that is integrated into the culture of the utility (Morley 2009). This may be accomplished through security and emergency preparedness awareness training. This low-cost mitigation effort can be very effective. However, security and preparedness awareness must extend across the entire work force. If a supervisor doesn’t think it’s important to keep the treatment plant doors closed and locked, the employees won’t take the mandate seriously either.

Weapons Policy

Given the number of incidents of workplace violence reported in the media each year, many companies have developed and enforce a strict “No weapons at work” policy.

COMMUNITY AWARENESS OF SECURITY

The public can be helpful in keeping an eye on drinking water and wastewater facilities. This is especially beneficial in the case of remote and unmanned structures. There is precedent for this initiative in Neighborhood Watch, which is a national crime prevention program designed to reduce crime through observant citizens. A number of utilities have actively solicited the public’s help in watching for suspicious behavior around utility reservoirs,

storage tanks, pumping stations, and even isolated fire hydrants. Activities of interest include unknown persons or vehicles loitering near facilities, individuals photographing facilities, nonutility personnel inquiring about the water system, vandals spray-painting buildings or other structures, or open gates or doors when utility workers are not in the area.

Citizens must be instructed not to take action themselves if they observe criminal or suspicious acts. Rather, they should be asked to phone police or the utility. To facilitate this, these individuals should be provided with an easy reference card, such as a refrigerator magnet, with pertinent phone numbers. Callers should also be reassured that their involvement will remain anonymous.

Some specific measures utilities can take to increase community awareness of utility security concerns include:

- Mailing customers security-related inserts with their bills
- Educating customers regarding the appearance of employees and utility vehicles
- Posting security-related information on the utility Web site
- Conducting door-to-door informational visits in neighborhoods where utility facilities have been vandalized in the past
- Presenting information to the public at community meetings
- Educating public safety personnel about utility security concerns

Regarding the orientation of public safety personnel, a couple of training videos have been produced during the past several years that are intended to increase the awareness of police to security concerns at water utilities. These videos are short and therefore suitable for showing during officer's role call. The videos can be obtained from the organizations that produced them (Pennsylvania Section AWWA 2006, Wisconsin Department of Natural Resources 2005).

Some water companies have reported that they have found many neighbors quite responsive to requests to keep a watchful eye on the public utilities that service them. Some utilities have also reported that a periodic expression of appreciation from utility officials to the citizen watch members helps reinforce the public's efforts.

PUBLIC ACCESS TO RESERVOIRS

Following the 9/11 attacks, many utilities restricted public access to raw and finished water reservoirs. In some cases where the public had used these facilities for recreational purposes for many years, the restrictions met stiff resistance.

Alternatively, some utilities consider public presence as another means of system monitoring. In 2006, the Portland (Ore.) Water Bureau reopened the parks around its five finished water reservoirs to the public during daylight hours. While there is still a fence around the reservoirs themselves, the fence around the entire property is opened at dawn and closed at dusk.

Additionally, the Water Bureau has installed cameras, motion detectors, and better lighting. The utility's position is that a public presence can be a security asset rather than a detriment. Water Bureau's Administrator David Shaff said, "By having more eyes and ears in the parks as people jog or walk the dog or simply sit and contemplate the water, we have more people who can report suspicious activity to our security people" (Nance 2006).

Treatment Facility Tours

Most public utilities cancelled public tours of treatment works immediately following the events of September 2001. This was unfortunate because tours have always been a great public relations tool and an effective means of educating students and the general public about the processes used to provide drinking water and wastewater services. Many systems subsequently resumed tours, but under more controlled conditions that include checking IDs of individuals on the tour, requiring that names of visitors be submitted several weeks in advance of the tour, and restricting public access to more sensitive areas within the treatment plant. Additionally, many utilities do not allow visitors to photograph the facilities.

USEPA has issued a series of recommendations for drinking water and wastewater utilities to follow in response to changes in DHS's color-coded Threat Level Advisory System. The recommendations include suggestions concerning the availability of public tours of utility facilities. USEPA recommends that when the threat level advisory is at a low level (green or blue), tours can be conducted, but tour participants should be required to present a form of personal identification that utility staff can document. When the threat level is yellow—which it has been for most of the time during the years following 9/11—tours should be limited to those that directly benefit the utility's ability to serve its customers. Additionally, the ratio of utility escorts to tour participants should be maintained at a level of 1 to 5. USEPA further recommends that should the threat status reach the more ominous orange or red levels, all tours should be cancelled.

CONTROLLED ACCESS TO KEY FACILITIES

An important step in securing utility facilities is accounting for all individuals entering and exiting utility property, especially key facilities. This includes employees and nonemployees. All utility employees should be encouraged to be aware of strangers in key facilities such as the treatment plant. Nonemployees should always be escorted by utility personnel. Unescorted strangers should be questioned by employees. Restricted areas can be indicated by posting "Employees Only" signs.

In some utilities, restrictions on access to certain key areas has been extended even to employees. In some plants, only individuals with a legitimate need to be in certain critical areas such as control or SCADA rooms are granted access. This can be enforced by a number of methods such as keys, swipe cards, and biometric readers.

SECURITY TRAINING

All utility or contract personnel functioning in a formal security role should receive appropriate training on general security procedures as well as company security policies. This training can be accomplished in-house or through a combination of internal and external resources.

If utility personnel are expected to handle hazardous materials such as gaseous chlorine, or respond to emergencies involving these substances, they must receive formal initial and refresher training on the handling of these materials and the use of the self-contained breathing apparatus.

All utility personnel, regardless of job title, should receive formal training on security, and the training should be reinforced periodically. This training should be focused on the organization's security and emergency procedures and may be incorporated into the company's safety training program. Such training should include emergency scenarios (natural disasters, accidents, and intentional acts) and a review of company policies and procedures, as well as security observation and awareness training. Particular emphasis should be placed on familiarizing personnel with the utility's ERP, whose update was mandated by the Bioterrorism Act. While all employees need to be knowledgeable of their roles as described in the ERP, key management personnel need to have a good understanding of the entire plan.

USEPA and a number of other government and industry organizations have strongly recommended that utilities conduct formal drills that include utility personnel, emergency responders, health agencies, regulatory agencies, and anyone else the utility anticipates having to work with during emergency situations. As discussed in chapter 17 of this handbook, these drills can range from relatively simple table-top exercises, to functional exercises, to detailed field exercises. These exercises give a utility an opportunity to test and subsequently update its ERP. Formal, scheduled training also gives the utility an opportunity to network with the response partners that they will need to work with during an actual emergency and rehearse the overall response effort. Additionally, this training gives the outside agencies a chance to update their own ERPs for water incidents.

KEY SECURITY

Utilities need to establish and maintain a formal key-control program. A serious vulnerability associated with the use of keys to secure gates and doors is that it is almost impossible to prevent the keys from being copied. This is despite efforts such as labeling keys "Do not duplicate." Furthermore, it is difficult to guarantee that keys will always be retrieved from employees or contractors whose association with the utility is terminated under either positive or negative circumstances.

A formal log should be maintained listing who has been issued specific keys and when they were issued. Spare copies of facility keys should be maintained in a secure manner. Additionally, there should be a serious company

policy forbidding keys from being left in locks, equipment, or vehicles when they are unattended.

EMERGENCY NOTIFICATIONS

Water companies should ensure that employees understand appropriate emergency notification procedures. Updated emergency 24-hour phone numbers should be posted in highly visible areas within facilities. Critical personnel should maintain ready access to these numbers at all times.

DELIVERIES

A system should be established whereby deliveries, especially bulk deliveries to treatment plants, are scheduled in advance. Additionally, both the delivery person and the delivered material should be screened and verified. Many treatment chemical vendors now provide tamper-proof locks or seals on shipments to help ensure that the delivered material has not been tampered with during shipment. However, it must not be assumed that these measures still cannot be defeated by a skilled adversary. Vendors should also be instructed to provide the utility with the names and photographs of the vendor's drivers, as well as the license plate or serial number of the truck, prior to shipping. Using this information, the driver and vehicle identity can be verified on arrival at the plant. Deliveries should not be transferred to treatment plant storage vessels until the security checks have been completed. The received loads should be logged-in and security verification documents retained by the utility.

The security requirements that a utility requires of vendors should be reasonable and should be written into the annual chemical purchasing contracts. The vendors must understand the importance of the security precautions to the utility and be aware that failure to comply with these requirements could result in the utility's refusal to accept a chemical delivery and jeopardize the continuation and future award of the supply contract.

A number of utilities conduct onsite visual inspections and simple physical/chemical analyses of treatment chemicals at the time of delivery. Inspections usually entail observation of color and physical appearance of the product as well as measurement of some simple physical/chemical properties (e.g., pH, specific gravity). While these steps are intended to protect against intentional substitution or gross contamination of treatment chemicals, they serve the additional benefit of protecting against accidental substitution and contamination events. Incidents have been documented where the wrong treatment chemical was accidentally delivered to a facility and inadvertently fed into the water during the treatment process, subsequently leading to significant negative health effects on consumers. Contaminants have also been accidentally added to treatment chemicals during shipment. This includes corrosion materials from tanker trucks as well as plastic and rubber debris leached from transport hoses during transfer of aggressive chemicals.

Welter (2009) has identified chlorine gas deliveries, particularly by truck, as the most vulnerable phase of the overall risk of using chlorine gas. Compared with the vulnerability associated with storage at the treatment location, the in-transit risk is greater because the chlorine is already on wheels and can more readily be diverted to a population center where its release could cause maximum damage. Welter proposed a policy and procedural strategy that drinking water and wastewater utilities could implement at minimum cost to reduce this risk. The policy recommendation is that utilities require chlorine vendors to implement The Chlorine Institute Security Management Plan (Chlorine Institute 2003). This plan, among other measures, requires implementation of commercially available technology to secure vehicles in transit using multiple systems. The procedural recommendation is that utilities adopt a protocol for notification in the case of delayed chlorine deliveries. Utilities should notify their chlorine supplier if a scheduled delivery of chlorine does not arrive within a specified time (e.g., 30 min). If confirmation of the delay and the whereabouts of the delivery truck cannot be obtained within another set time (e.g., 30 min), then law enforcement agencies should be notified.

EMERGENCY CONTRACTS

In a serious emergency, the resources of an individual utility will likely be overwhelmed. To expedite acquisition of outside assistance, contracts and agreements should be in place ahead of time. Many utilities have had contracts in place for emergency contractor services for years, such as piping contracts for large main breaks, emergency water hauling contracts when public water use has been restricted, and emergency laboratory services for contamination analysis. These contracts need to be kept current, with all the occasions when these services might be required (e.g., weekends, holidays) specified and the maximum lead time indicated for the contractor to render service once notified. The price differentials for goods and services procured during normal working hours versus nights and weekends should also be spelled out in the contract.

MUTUAL AID AGREEMENTS

In addition to contracts with vendors and commercial contractors, it is becoming common practice for utilities to set up mutual aid agreements with other utilities for assistance in emergency situations. Through such agreements, resources (manpower and materials) can be shared among utilities in times of crisis.

For many years, mutual aid agreements involved mainly neighboring utilities. However, the current trend is for mutual aid agreements to be established on a state-wide basis. This makes available a wide variety of resources, even to small drinking water and wastewater systems. The Water

and Wastewater Agency Response Network (WARN) is a formal system that is operated by utilities with strong support from industry organizations and USEPA. The program is at some stage of development within each of the 50 states and is modeled after intrastate mutual aid compacts developed years ago in California, Texas, and Florida.

The WARN initiative is based on the concept of utilities helping utilities and is intended to provide distressed drinking water and wastewater systems with emergency staffing, equipment, and supplies on short notice. The emergency aid is specialized, the type only water utilities are able to provide. An underlying assumption is that mutual aid from other utilities would arrive at a distressed utility's location sooner than state or federal assistance. The network can be activated in response to all types of emergencies, including natural disasters, accidents, and manmade events. The agreements are signed by utilities in advance and cover details such as emergency notification procedures, reimbursement, liability, and workers compensation. A particular advantage of the WARN program is that it can be set up at little or no cost to participating utilities.

In addition to intrastate mutual aid agreements, an initiative still under development will establish interstate mutual aid agreements under the Emergency Management Assistance Compact (EMAC). This initiative is somewhat more complicated than intrastate compacts because of legal differences between states.

REFERENCES

- Chlorine Institute. 2003. *Security Management Plan for the Transportation and On-Site Storage and Use of Chlorine Cylinders, Ton Containers and Cargo Tanks*. Arlington, Va.: The Chlorine Institute.
- Herrick, C., and F.J. Blaha. 2007. Information Disclosure and Security Information Protection at Water Utilities. *Jour. AWWA*, 99(11):40.
- Morley, K.M. 2009. An Evolving Culture of Security and Preparedness in the Water Sector. *Jour. AWWA*, 101(1):32.
- Moser, R.H. 2005. Purposeful Contamination of Distribution System With Chlordane Affecting 10,000 People. *Proc. 2005 AWWA Water Security Congress*. Denver, Colo.: American Water Works Association (AWWA).
- Murphy, B.M., and G.J. Kirmeyer. 2005. Developing a Phased Distribution System Security Enhancement Program. *Jour. AWWA*, 97(7):93.
- Nance, S.M. 2006. Portland: Opening a Park to Public Improves Security. *E-Mainstream*, 3:20.
- Pennsylvania Section AWWA and Pennsylvania State Police. 2006. *Water Security for Law Enforcement*. www.paawwa.org.
- US Environmental Protection Agency (USEPA). 2003. Protecting Water System Security Information. Washington, D.C. www.epa.gov/safewater/watersecurity/pubs/ncsl_foia_sept03.pdf.
- Water Security Channel. 2007. NIAC Gets New Assignment on Insider Threats. Water Security Channel, January, 2007.
- Welter, G.J. 2009. One Perspective on Chlorine Security. *Jour. AWWA*, 101(1):36.
- Wisconsin Department of Natural Resources. 2005. *Drinking Water Security: Roll Call Training DVD*. Madison, Wis. www.dnr.state.wi.us.

MITIGATION OF RISK THROUGH CYBER MEASURES

The Internet plays a key role in the propagation of terrorism. The number of Web sites advocating terrorism or political violence has increased from a dozen in 1997 to almost 4,700 in 2006 (Ariza 2006). Without the Internet, the fragmentation and decentralization of the jihadi movement into a still functioning global network would not be possible. As a tragic example, a computer belonging to one of the attackers in the March 2004 Madrid train bombings showed evidence of downloading from the same Web site that delivered a document entitled “Jihadi Iraq: Hopes and Dangers.” Among other charges, this document called for attacks on Spain to force a withdrawal of that nation’s troops from Iraq.

In addition to facilitating the spread of information on terrorism, the Internet is a mode of attack for individuals and groups ranging from amateur hackers to domestic and international terrorists. Water utilities, like other businesses, are very dependent on computer monitoring and control systems. This is true for the treatment, distribution, and collection aspects of the operation as well as the financial and administrative components. Over the years, water systems have increased their reliance on SCADA systems and distributed control systems (DCS) for remote command and control of water system operations. This reliance on computerized monitoring and control systems has left drinking water and wastewater utilities potentially vulnerable to both targeted cyber attack and accidental cyber events.

SCADA systems are computers and networks that control delivery of essential utilities such as electricity, natural gas, gasoline, and transportation in the United States and around the world. Use of SCADA/DCS technologies allow drinking water and wastewater utilities to better manage treatment

capacity, maintain tighter control of the treatment process, and operate their systems more efficiently and economically. As a result of this technology, more facilities are being operated unattended much of the time.

SCADA networks are designed to maximize functionality, reliability, and efficiency. As pointed out in the National Research Council's report on the role of science and technology in countering terrorism (NRC 2002), current SCADA systems have been designed with little or no attention to security. For example, data in SCADA systems are often sent "in the clear" with no attempt to scramble or mask the information being transmitted, protocols for accepting commands typically require no authentication, and control channels are often wireless or leased lines that pass through commercial telecommunications facilities. Consequently, SCADA systems are vulnerable to attack from individuals or groups, ranging from simple recreational hackers seeking a challenge and bragging rights, to sophisticated terrorists intending to redirect processes, manipulate operational data, and potentially produce wide-scale damage to people and infrastructure.

An electronic attack could be an end in itself or could be carried out simultaneously with a physical attack. SCADA systems have received less attention from security specialists because to date they have been the target of computer hackers far less frequently than financially oriented billing systems and corporate Web sites. Unlike computer systems for financial services, Web commerce, and email, SCADA computers typically aren't regularly replaced or updated with security software because of complexity, cost, and the need for uninterrupted service. This also makes SCADA systems more vulnerable. Realizing the potential threat to SCADA systems, Executive Order 13231 was issued in October 2001 creating the President's Critical Infrastructure Protection Board. One purpose of this board is to coordinate all federal activities related to protection of information systems and networks in government agencies and the private sector. The federal government has also directed the Idaho National Laboratory to focus on SCADA security, including the provision of voluntary audits for companies.

Hackers may be outsiders or individuals with inside access to a utility's information network. They can access SCADA and information systems in a number of ways, including through corporate or business networks, direct Internet connections, telephone lines, trusted third-party connections, virtual private network connections, and wireless systems (Keefe 2006). The types of attacks can include unauthorized access into the system, data interception, data modification, data destruction, and system disruption. The vulnerability of information systems to hacking has been enhanced by a number of trends including a convergence of standardized system architecture and widely used platforms (e.g. Microsoft Windows), anonymous Internet access, and readily available hacking information and tools.

A well-documented hacker event involving a wastewater SCADA system occurred in Maroochy, Australia, in 2000. A contractor had just completed a major upgrade of the SCADA system in a wastewater plant. One of the

contractor's former employees was upset because he wasn't subsequently hired directly by the utility. With his insider knowledge of the computer system, the frustrated job applicant successfully hacked into the SCADA system numerous times over a 10 week period. These episodes resulted in pump shutdowns and, on one occasion, an overflow of millions of gallons of raw sewage into a river, a park, and onto the grounds of a hotel, with a resulting cleanup effort costing thousands of dollars. The perpetrator was finally arrested and sentenced to two years in prison.

SCADA systems are particularly vulnerable because, whether system operators realize it or not, the computers associated with SCADA systems are sometimes connected in haphazard ways to the Internet. Additional vulnerability is associated with the rapid growth in easy-to-access wireless networks and the use of off-the-shelf software.

An incident which occurred in 2006 in a Pennsylvania drinking water system and was reported in the media illustrates this vulnerability (UPI 2006, Hartson 2009). A water treatment plant operator noticed a suspicious number of windows open on a SCADA server. When the system was scanned, the operator found it was infected with a virus and spyware. Although the SCADA system was protected by two firewalls, the same access that permitted three utility operators to dial in from home and remotely control the system also allowed infection to travel to the SCADA system from an operator's home personal computer. A hacker, apparently from a foreign country, gained access to the utility computer that controls the SCADA system by tapping into a plant operator's home laptop through the Internet. The FBI believes that the motive in the attack wasn't to covertly affect the treatment plant's operations, but rather to use the plant's computer for piracy purposes (movies, games, music) and to distribute mass emails or pirated software. However, concern over the incident was high because the hacked computer could potentially have been used to disrupt plant operations. Following the intrusion, the utility replaced the hard drive in its main computer, changed all passwords to the system, and eliminated home access to the SCADA system.

Vulnerabilities discovered in SCADA systems have been described in the media. A specific software vulnerability in a commonly used, commercially available SCADA system, termed a "buffer overflow," was discovered and reported to the news media by a cyber security firm (Robertson 2008). The weakness potentially allows hackers to gain control of a SCADA program by sending a computer too much data. The vulnerability could be exploited if the SCADA network is connected to the Internet or even if SCADA system computers and other computers with Internet access are connected to the same router. The SCADA system manufacturer patched the hole in the software following the report by the outside security firm.

Following 9/11, utility managers have routinely included security among their list of key criteria when selecting and designing new SCADA systems or updating already existing ones. Case studies have been published describing this process for utility personnel (Anonymous 2004). However, in the opinion

of some specialists, the water sector still lags behind other utility sectors—oil, gas, chemical, and electrical—in addressing cyber security issues (Johnson and Edwards 2007). Some steps that can be taken to improve cyber security in existing control and information networks in the water industry are discussed in the following sections.

VAs FOR CYBER SYSTEMS

Because of the importance of computerized systems in the day-to-day functions of utilities, and the complexity of these systems, utilities should hire trained IT security professionals to fully assess cyber vulnerabilities and develop mitigation measures. However, utility managers can begin assessing their vulnerabilities with a basic set of questions:

- What data are being handled by the information system and how critical are they?
- What are the consequences if the data or systems are compromised?
- Who should have access to the data, and where and when should access be provided?

Guidance material is available for self assessment of water utility control systems (WERF 2009).

RECOMMENDATIONS FOR RISK REDUCTION

Short of a rigorous VA by IT security specialists, or in addition to it, some practical counter measures can be used to protect a utility's information and SCADA systems against tampering, or at least prevent extensive damage if tampering occurs. Some of these measures have been recommended in the Department of Energy's 21-step guide to improve cyber security of SCADA networks (US Department of Energy 2002) and are included in the following discussion.

General

Install, and regularly update, virus-protection software for email and Internet access. Firewalls, an email filtering system, and IT security protocols should be used to protect cyber integrity. This is critical if a system is connected to the Internet, either by data line or a dial-up connection.

- Establish a policy preventing unauthorized addition of software by employees.
- Back up data on servers daily as a safeguard against system destruction. Categorize data and protect it accordingly. Apply the greatest amount of protection to critical programs and files.
- Disconnect unused or unnecessary computer connections. Remove sensitive information from publicly available Web sites.
- Develop a business mitigation plan that would allow the utility to continue functioning in the event of an accidental system malfunction or a major cyber attack.

- Encourage development of a cooperative relationship between a utility's IT support group and operators and technicians. This will help ensure that utility personnel comply with computer system security protocols.

Access Control

Improve physical security for computer workstations to prevent unauthorized access to the network. This may involve locating sensitive workstations, such as those tied to operational control of the treatment plant, distribution system, or collection network, into rooms requiring key or swipe card access. The information system should be alarmed so that it detects and alerts system administrators if unauthorized activity or intrusion attempts occur. For critical systems, 24-hour monitoring can be set up through a pager system.

Configure the computer system to prevent unauthorized dial-in access to data files, SCADA systems, and communications systems.

Upgrade the password-protection barrier.

- Require passwords for all devices connected to computer network.
- Change passwords regularly.
- Include numbers and symbols, as well as upper- and lower-case letters, in passwords.
- Promptly delete old accounts and passwords when they are no longer being used. Passwords should automatically be deleted after a certain amount of time has passed without use.
- Limit access to administrator log-in privileges with unlimited access to the system.
- Establish a user authentication program. This is the next level of security beyond passwords. User identity can be verified by using such tools as USB authentication keys or smart cards. The USB key or smart card, in combination with a user PIN, can identify and control which information or files a user has access to.
- For sensitive information, or control of key operations, biometric identification (e.g., fingerprints, retinal scan, voice recognition) can be required for access to terminals.
- Electronic copies of sensitive documents should be maintained on a password-protected, secure server. Only authorized staff should be granted access to this folder.

SCADA Systems

SCADA systems should not be connected to the Internet, even indirectly. Identify all connections to the SCADA network. These may include the Internet, business networks, wireless network devices (including satellite uplinks), modem or dial-up connections, and connections to regulatory agencies. Determine how well these connections are protected.

To ensure the highest degree of security, isolate the SCADA network from other network connections to as great a degree as possible. Any

connection to another network introduces security risks, particularly if the connection creates a pathway to the Internet. Information flow should be restricted between the business information system and the SCADA system. Conduct penetration testing or vulnerability analysis of any remaining connections to the SCADA network.

Most older SCADA systems have no security features. SCADA system owners can acquire security features from vendors in the form of patches or upgrades. Set all security features to provide the maximum level of security.

Limit control of utility operations to onsite or main terminals only. Remote terminals should not be utilized. While operators or managers may have access from their work computers, don't allow control from outside the network (such as from a home personal computer). Access to the SCADA system should be limited to those personnel who have a legitimate need for access. Furthermore, the access of legitimate users should be limited to only those portions of the SCADA system required for their particular job function.

Install a data log that tracks all activity on the SCADA system. If there is an intrusion into the system, the log can help indicate where, when, and by whom the system was accessed.

Don't piggy-back the utility's security system onto the SCADA system. This practice could lead to the loss of both systems in the event of an attack.

Financial pressures have decreased staffing at most drinking water and wastewater utilities to the point that few utilities could run for an extended period of time in manual mode (ASCE, AWWA, and WEF 2004). However, should there be a credible threat to the security of a utility SCADA system, a logical response would be to shut the SCADA system down pending further investigation to prevent impacts to the utility's operations and infrastructure or to the customers' well being. For this reason, utilities may opt to train staff for this contingency by operating the utility one or more days each year without the involvement of the SCADA system.

DHS has developed a Control System Cyber Security Self-Assessment Tool (CS²SAT) which provides users with a systematic approach for assessing the cyber security posture of their industrial control system networks. CS²SAT is a desktop software tool that guides users through a step-by-step process to collect facility specific control system information and then makes appropriate recommendations for improving the system's cyber security. The tool pulls its recommendations from a database of the best available cyber security practices, which have been adapted specifically for application to industry control system networks and components. Each recommendation is linked to a set of actions that can be applied to remediate specific security vulnerabilities. Information about the cyber security self-assessment tool is available by emailing cs2sat@hq.dhs.gov. The tool is available for purchase, and free to Water Environment Research Foundation subscribers and Water Research Foundation members. This tool is specifically relevant for the water

sector and has been tested by several water utilities and distributed to a number of others (Sands 2009).

Remote Sensors

Install authentication technologies into critical remote sensors (e.g., chlorine analyzers, flow monitors). These technologies can be built into the sensors themselves to ensure that the signal being received actually originated from the sensor and not from an outside source.

Vendors and Contractors

Determine whether vendors and contractors have access rights or back doors to remotely conduct system diagnostics and maintenance. If so, this could represent a difficult-to-monitor and difficult-to-control access to SCADA and business computer systems. If back doors are necessary, strong authentication protocols need to be implemented.

Formal Cyber Security Program

Establish an ongoing education program for all computer system users on cyber security threats, and on how users can help protect the system. This includes instructing personnel to release information related to computer information systems and SCADA networks only to persons authorized to receive such information. While security software provides intrusion alerts, utility operators and technicians are the most likely to notice unusual behavior of computer systems. Security awareness training helps employees understand the importance of reporting violations as quickly as possible.

Periodically audit the entire network for security vulnerabilities. Conduct computer penetration tests to assess system vulnerability. Establish system backups and disaster recovery plans to enhance recovery from a cyber attack or major system malfunction and facilitate rapid reconstruction of the network.

ROADMAP TO SECURITY CONTROL SYSTEMS

In 2007, the water sector recognized a need to elevate its awareness and understanding of threats facing process control systems (Morley 2009). The result was a report prepared by the WSCC entitled *Roadmap to Security Control Systems in the Water Sector* (WSCC 2008). The roadmap recommends collaboration with DHS's National Cyber Security Division. The vision is that within 10 years, process control systems in the water sector will be able to operate with no loss of critical function during and after a cyber event. To realize this vision, the water sector will pursue the following strategic goals:

- Develop and deploy industrial control system security programs.
- Determine where vulnerabilities exist.
- Develop and implement risk mitigation measures.
- Establish a close collaboration among stakeholders.

Additionally, a National Water Sector Cyber Security Committee has been established, in partnership with AWWA, to increase cyber security

awareness within the water sector, promote best practices, and encourage the development of standards for the water industry (Johnson and Edwards 2007).

CONCLUSIONS

While an attack on the information or SCADA network of a water system, or an accidental failure of the network, may not present the same immediate risk to public health as addition of a pathogen to a drinking water reservoir or release of chlorine gas from a wastewater treatment plant, the extent to which water utilities are managed and operated by computerized systems certainly makes cyber security a credible concern. As pointed out by Baer and colleagues (2005), another factor that makes cyberterrorism a significant threat is the difficulty associated with tracking down and capturing hackers and cyber attackers. Of the thousands of cyber attacks executed each year, only a couple of dozen perpetrators are ultimately apprehended and punished. The sheer magnitude of the Internet, and its innate anonymity, make cyberterrorism a low-risk venture for a potential adversary.

Additional information on cyber security is available from a number of sources. The National Institute of Standards and Technology (NIST) maintains a Web site that lists best practice security guidelines (www.csrc.nist.gov).

REFERENCES

- Anonymous. 2004. Harnessing SCADA Without Undermining Security. *Jour. AWWA*, 96(7):51.
- Ariza, L.M. 2006. Virtual Jihad: The Internet as the Ideal Terrorism Recruiting Tool. *Sci. Amer.*, 294(1):18.
- American Society of Civil Engineers (ASCE), American Water Works Association (AWWA), and Water Environment Federation (WEF). 2004. *Interim Voluntary Security Guidance for Wastewater/Storm Water Utilities*. Denver, Colo.: www.awwa.org/science/wise.
- Baer, M., K. Heron, O. Morton, and E. Ratliff. 2005. *Safe: The Race to Protect Ourselves in a Newly Dangerous World*. New York.: Harper Collins.
- Hartson, M.K. 2009. Cyber Security: Is Your System Safe? *Opflow*, 35(5):10.
- Johnson, S., and D. Edwards. 2007. Why Water and Wastewater Utilities Should be Concerned About Cyber Security. *Jour. AWWA*, 99(9):89.
- Keefe, R. 2006. Security Lacking in Networks Controlling Critical Infrastructures. *Austin American Statesman*, October 2.
- Morley, K. 2009. An Evolving Culture of Security and Preparedness in the Water Sector. *Jour. AWWA*, 101(1):32.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academies Press.
- Panguluri, S., W.R. Phillips, and R.M. Clark. 2004. Cyber Threats and IT/SCADA System Vulnerability. *Water Supply Systems Security*. New York.: McGraw-Hill.
- Robertson, J. 2008. Security Hole in Software Exposes World's Utilities to Net Attacks. *Associated Press*, June 11.
- Sands, C.C. 2009. Water Sector Experience with CS²SAT. *Proc. 2009 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- United Press International (UPI). 2006. Hacker Hits Pennsylvania Water System. October 31.

- US Department of Energy. 2002. *21 Steps to Improve Cyber Security of SCADA Networks*. Washington, D.C. www.counterterrorismtraining.gov/updates_102002.html.
- Water Environment Research Foundation (WERF). 2009. *Security Measures for Computerized and Automated Systems at Water and Wastewater Facilities*. WERF Project 03-CTS-3SCO. Washington, D.C. www.werf.org.
- Water Sector Coordinating Council (WSCC). 2008. *Roadmap to Secure Control Systems in the Water Sector*. Denver, Colo.: AWWA. www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf.

CONTAMINATION WARNING SYSTEMS

An important tool for increasing the security of a drinking water or wastewater utility is the establishment of a Contamination Warning System (CWS). These systems were originally referred to as early warning systems (EWSs) because the goal was to detect a contamination event early enough to warn the population at risk and prevent their exposure. However, as described in this chapter, the state of monitoring technology at this time is still fairly basic and probably not capable of providing a warning early enough to prevent exposure. Rather, the current state of technology may only alert officials in time to initiate response actions—possibly after initial exposure—to minimize the public health and economic impacts of an incident. The development of an actual EWS is probably years in the future.

The main component of a CWS is a continuous, online monitoring network with analytical equipment located at various sites in the treatment plant and distribution or collection systems. The purpose of the monitors is to detect chemical, biological, or radiological contaminants that pose a threat to a utility. The monitors may also be capable of detecting the carrier matrix within which a contaminant is injected, such as the growth medium supporting a bacterial culture.

In drinking water utilities, sensors can be deployed to monitor the raw water coming into the treatment plant and the finished water leaving the plant, as well as the finished water at strategically chosen locations throughout the distribution system. In wastewater utilities, monitoring devices can be installed at various points throughout the collection system, at the treatment plant headworks, and at the treatment plant discharge point into receiving waters. Ideally, a CWS provides multiple benefits because it could detect accidental contamination as well as purposeful contamination. For example, in a wastewater utility influent, monitoring of pH, oxidation-reduction

potential (ORP), conductivity, and temperature may provide an indication of contaminated sewage that could result in a plant upset. In the headspace of the influent pump station wet well, continuous monitoring for combustible gases would help protect the plant and its personnel. At the effluent discharge site, monitoring may detect pass-through of harmful contaminants into the environment. Monitoring devices such as chlorine analyzers may also be useful in both drinking water and wastewater facilities for process control and ensuring regulatory compliance.

A monitoring system is certainly not capable of preventing an accidental or intentional contamination event. Rather, the goal of the system is to detect a low-probability, potentially high-impact contamination incident in time to respond and reduce the impact on people, property, infrastructure, and the environment.

Several questions should be considered before establishing a CWS:

- What is the objective of the CWS?
- What are the most useful monitoring technologies?
- Where should the monitors be located and how often should they take measurements?
- How should data be analyzed and integrated?
- What results constitute an alarm?
- What should be done when an alarm goes off?

The ideal early warning instrumental technology would have the following characteristics:

- Accurate
- High sampling rate (measures the target parameters continuously or at frequent intervals)
- Rapid response time (short amount of time required for a complete analysis)
- Low detection limit
- High specificity (low cross-reactivity with nontarget substances)
- Full automation (operates online with no operator intervention)
- Detects a broad spectrum of contaminants
- Qualitative and quantitative detection (can both identify a contaminant and measure its concentration)
- Low frequency of false positive and false negative results
- Easy to operate
- Can operate remotely and report results to offsite responders
- Inexpensive

At this time, no monitoring device or system meets all of these criteria.

APPROACHES FOR ONLINE MONITORING

Five analytical approaches are currently in use for online, real-time monitoring for contaminants in water:

- Monitoring routine chemical parameters as surrogates or indicators for chemical and perhaps even biological, contamination (detecting a chemical change of state)
- Real-time toxicity biomonitoring
- Screening for radiation to indicate the presence of radionuclides
- Detecting, identifying, and quantifying specific chemical contaminants (contaminant-specific monitoring)
- Detecting, identifying, and quantifying specific pathogens (pathogen-specific monitoring)

Each of these approaches is discussed here, accompanied by a description of currently available technology as well as equipment under development.

Monitoring Routine Chemical Parameters as Surrogates for Contamination

There are several practical obstacles for online detection of contamination in drinking water and wastewater systems. One is that so many chemical or biological contaminants could accidentally or intentionally end up in water or wastewater systems. It is impossible to develop and deploy analytical devices that can accurately identify and measure each of these specific substances on a continuous online basis.

Furthermore, chemicals that may not have previously been considered to be contamination candidates could end up in a water system, or a combination of contaminants could appear, which may confuse analytical efforts to identify specific agents. In addition to the problem of large numbers of potential contaminants, at this time the technology for online monitoring for specific chemical and biological agents is at a fairly basic level.

One approach to dealing with these obstacles is to use basic chemical parameters (such as pH, chlorine concentration, total organic carbon (TOC), conductivity) as surrogates for individual contaminants. Changes in the values for these indicator parameters could signal a significant chemical change of state, which may suggest the presence of an unknown contaminant. This is similar to the use of coliform bacteria as an indicator for the possible presence of waterborne pathogens, a practical approach that has been employed by the water industry for the past 100 years. Monitoring for basic chemical parameters is feasible because online monitoring equipment has already been developed, and in some cases has been deployed for years, to measure these parameters. Additionally, most of this equipment is relatively inexpensive, especially compared to the analytical instruments that are needed to detect, identify, and quantify specific contaminants.

It is important to establish a data baseline by analyzing data from measurements taken throughout the different seasons of the year. The baseline helps decision makers determine whether an observed value for a particular measured parameter differs significantly from the norm. It is also useful to establish a relationship between changes in parameters and the presence of a specific contaminant. The idea is to generate a signature of changes

in chemical parameters that can at least tentatively identify a chemical or biological substance, or a class of contaminants, not normally present in the water being tested.

Several studies have been published supporting the concept of monitoring for the presence of contamination by tracking general chemical parameters. Byer and Carlson (2005) conducted a series of both batch and pilot-scale distribution system experiments to test whether four credible candidates for intentional contamination of water could be detected using the routine parameters chlorine residual, pH, turbidity, conductivity, and TOC. The contaminants tested included pesticides, rodenticides, and industrial inorganic compounds. The study results showed that three of the four contaminants were detected well below a concentration that would cause significant health effects, and the fourth was detected near the concentration for acute health effects.

USEPA has established a Water Assessment Technology Evaluation Research and Security (WATERS) Center in Cincinnati, Ohio. At this facility, USEPA operates a number of distribution system simulator units, which are recirculating plumbing loops designed to facilitate study of water quality dynamics in municipal distribution systems. The researchers at WATERS also conduct bench-scale experiments utilizing single-pass lines. Using this equipment, USEPA investigated the extent to which changes in standard water quality parameters indicate the presence of contaminants (Hall et al. 2007). The water quality parameters were measured using commercially available real-time sensors operated in an online mode. The sensors measured pH, free chlorine, oxidation reduction potential (ORP), dissolved oxygen (DO), specific conductance, turbidity, TOC, chloride, ammonia, and nitrate. The contaminants used to challenge the sensors included secondary effluent from a wastewater treatment plant, potassium ferricyanide, a malathion insecticide formulation, a glyphosate herbicide formulation, nicotine, arsenic trioxide, aldicarb, and *E. coli* with growth media. After a number of trials through the pipe-loop system, the results indicated that while no single water quality parameter responded to all of the contaminants used in the study, all of the contaminants caused at least one parameter to change significantly in response to the injection.

For example, wastewater caused an increase in the levels of chloride, specific conductance, turbidity, and TOC along with a decrease in free chlorine and ORP. Injection of a malathion formulation caused an increase in TOC and chloride but a decrease from baseline in free chlorine and ORP. The parameters most responsive to the presence of contaminants were free chlorine, TOC, ORP, specific conductance, and chloride. These results suggest that sensors measuring standard water quality parameters may be useful in a contamination warning system.

The USEPA studies described involved injection of contaminants into a recirculating plumbing system containing drinking water with a free chlorine residual. Because of increasing regulatory pressure to further control

concentrations, more and more US drinking water utilities are converting to maintenance of a chloramine residual rather than a free chlorine residual in the distribution system. For this reason, USEPA also conducted a series of injection experiments with water containing a chloramine residual in the recirculating plumbing loops (Szabo et. al 2008). A series of contaminants, including wastewater, nicotine, glyphosate, and malathion, were injected into the pilot distribution system. The results of these experiments indicated that, in contrast to free chlorine systems, the total chlorine measurement, which would reflect chloramine concentration, was not very responsive to the sudden occurrence of contaminants in chloraminated waters. Rather, TOC was the best contaminant indicator in these systems. Other water quality parameters (such as ORP, chloride, and nitrate) tended to be contaminant specific. Therefore, if contamination warning systems utilizing measurement of changes in basic water quality parameters (surrogates) are to be employed in chloraminated water systems, the key trigger parameter will be TOC rather than total chlorine.

Some of the types of online physical and chemical sensors currently commercially available are described in the following pages. Because the threat of accidental or intentional contamination has been perceived to be more significant for drinking water systems than for wastewater systems, most of the devices discussed in this chapter have been deployed primarily in drinking water utilities to date. However, the same technologies may be effective in protecting wastewater utilities.

Online Chlorine Measurement Systems

Residual chlorine is one of the most widely measured chemical parameters in the water industry. Free and total chlorine are measured on a continuous basis for regulatory compliance purposes to ensure adequate disinfection at drinking water and wastewater treatment plants, and maintenance of a protective residual in the drinking water distribution system. For process control purposes, chlorine can be measured on a continuous basis and the results linked with an alarm system that notifies the operator of low chlorine concentrations. Chlorine readings can also be tied into a feedback loop to automatically pace the dosage of chlorine applied at the treatment plant or in chlorine booster stations in the distribution network.

Additionally, the continuous measurement of chlorine concentration can help protect a water system against accidental or intentional contamination. A significant decrease in chlorine residual can signal an unexpected increase in disinfectant demand and consequently the presence of a contaminant in the water. The chlorine measurement devices available use either amperometric, *N,N*-diethyl-*p*-phenylenediamine (DPD), or polarographic membrane methods.

General Organic Chemical Load

Several analytical instruments can be used to provide a gross measurement of the organic chemical content of water. These include TOC analyzers and

ultraviolet-visible (UV-Vis) spectrometers. Analyses employing these devices can be performed in either batch or online mode.

TOC analysis is a commonly used technique that measures the carbon content of dissolved and particulate organic matter present in water. Many drinking water utilities monitor TOC to evaluate raw water quality or to evaluate the effectiveness of treatment processes designed to remove organic carbon. In fact, in the federal Disinfectant/Disinfection By-Product Rule, TOC is designated a surrogate parameter to gauge removal of DBP precursors during the treatment process. Some wastewater utilities employ TOC analysis to monitor the efficacy of the treatment process.

In addition to these applications, changes in TOC concentrations can be used as an indicator for contamination from organic compounds (e.g., petroleum products, industrial solvents, pesticides). While TOC analysis does not provide information about the identity of a specific contaminant, gross positive deviations from normal TOC concentrations can be an indication of a chemical threat to a system. Online TOC analyzers can be placed at critical sites within a drinking water distribution system, at the intake of a drinking water treatment plant, or in a wastewater plant influent wet well, to detect potential organic chemical compounds. TOC analysis has been shown to be an especially sensitive method for detecting changes caused by a variety of contaminants that could potentially be introduced accidentally or intentionally into a public water supply (Hall et al. 2007).

The response time for TOC analyzers varies with manufacturers' specifications. However, 5 to 15 minutes is generally required to obtain stable readings. Detection limits vary from 0.2 to 1 mg/L carbon. The costs of online TOC analyzers range from \$18,000 to \$28,000 (USEPA Security Product Guide). A commercially available TOC analyzer, used as a security monitor in the Pittsburgh drinking water distribution system, is the Sievers 5310C On-Line TOC Analyzer*, which operates using UV/persulfate oxidation and membrane conductometric detection.

Another surrogate parameter for measuring the general organic content of water is UV-Vis absorbance. A UV-Vis spectrometer will react with organic contaminants that absorb in the UV range. The alarm sensitivity for many organic contaminants is between 1 and 500 µg/L. Examples of organic compounds detected include phenol, toluene, xylene, many pesticides, some nerve gases, crude oils, and naphthalenes, among others. The types of compounds not detected include short-chained aliphatics. Response time can be less than 1 minute.

Potential advantages of UV-Vis spectrometry, compared with TOC measurement, may be shorter response time, greater sensitivity, less maintenance, and lower instrument cost. A commercially available product deployed in 15 locations within the Vienna, Austria water distribution system, as well as in

* GE Analytical Instruments, Boulder, Colo.



Courtesy of GE Analytical Instruments

Figure 12-1. Sievers 5310C On-Line TOC Analyzer

the other hand, fluorometry has been used for years to detect the presence of hydrocarbons in source waters at drinking water treatment plant intakes, and to help characterize the progress of petroleum product plumes in lakes and rivers following industrial spills. Commercially available fluorometers, such as the Turner TD 4100[†], can detect dissolved gasoline, diesel, jet fuel, and oil components such as the BTEX compounds (benzene, toluene, ethylbenzene, xylene). These instruments continually measure the fluorescence of aromatic hydrocarbons in a flowing stream of water from the low parts per billion to the high parts per million concentration range. Fluorescence occurs when a molecule absorbs light energy of a specific wavelength and emits light energy of a longer wavelength.

Online Analytical Probes and Multi-Parameter Panels

Online analytical probes are currently the most commonly used devices for contamination warning systems in drinking water. They are relatively inexpensive, simple to use, can provide continuous monitoring with remote access to data, and are commercially available from a variety of manufacturers. Many of these devices are already in place, both in drinking water and wastewater treatment plants and in the distribution and collection systems, for process control. These include electrodes that can measure a variety of different chemical parameters including pH, chlorine, fluoride, DO, ammonia, nitrate, and nitrite; thermistors for temperature; potentiometric devices

some other European and US cities, is the spectro:lyser spectrometer with the ana:alarm software package manufactured by s::can Messtechnik*. A unit utilized in the Pittsburgh Water and Sewer Authority's distribution system is the Real Tech UVT 254 Online Monitor†.

Oil and Petroleum Detection

Monitors for detecting the presence of oil and petroleum products in water have been available for quite some time. Light scattering devices are employed on commercial off-shore oil rigs to detect surface sheens on the water. However, these devices may be too insensitive for practical use in drinking water and wastewater monitoring. On

* s::can Messtechnik, Vienna, Austria

† Real Tech Inc., Ontario, Canada

‡ Turner Designs, Inc., Sunnyvale, Calif.

for ORP; conductivity cells for specific conductance; and nephelometric units for turbidity.

Several manufacturers have combined a number of already available individual sensors into panels of sensors that monitor multiple water quality parameters. The most basic application for these multiparameter panels is to detect physical and chemical changes in water quality (a change of state) that might suggest that a contaminant has been accidentally or intentionally added to the water. The objective is for the multiparameter monitor to provide an early warning for occurrence of an unspecified contaminant. Some commercially available devices include the Clarion Sentinel 500 Series^{*}, the Rosemount Analytical WQS[†], and the YSI 660 DW[‡].

A more advanced application for multiparameter panels is the attempt to establish a characteristic pattern of changes in multiple parameters that might be used to tentatively identify a contaminant. Such a characteristic pattern is sometimes termed a *signature*. Several commercial entities and research groups are currently working to develop this capability. For example, the Hach Corporation[§] markets the Guardian Blue System. This product consists of a series of sensors, which the company has previously sold individually, that are now combined into a preconfigured water panel for more comprehensive monitoring.

The expanded version of the panel includes analyzers for TOC, chlorine, pH, turbidity, and conductivity. Included in the system is an event monitor that facilitates real-time analysis of data from the water panel. The event monitor integrates the readings for all of these parameters into a composite value or vector. Should the composite value differ substantially from the typical background level, and from routine deviations from the norm caused by known utility operational changes such as turning on distribution system pumps, the event monitor triggers an alarm.

Hach has also developed an agent library that contains a signature or fingerprint of the changes expected to occur in composite parameters when one of 80 different contaminants is introduced into the water. These 80 contaminants, not published by the vendor for security reasons, are believed by the manufacturer to be potential candidates for use in an intentional contamination incident. Changes in the routine parameters are compared with the fingerprint in the agent library and a tentative identification of the contaminant is provided to the utility operator along with an estimate of the degree of confidence in the identification. The contaminant monitoring system can be set up to communicate directly with a utility's SCADA system.

* Clarion Sensing System, Inc., Indianapolis, Ind.

† Rosemount Analytical, Irvine, Calif.

‡ YSI Inc., Yellow Springs, Ohio

§ Hach, Loveland, Colo.



Courtesy of Hach Homeland Security Technologies

Figure 12-2. Hach Guardian Blue System

The Hach Guardian Blue multiparameter monitoring system was deployed at key locations to protect the potable water system during the 2008 Beijing Summer Olympics (Kroll 2008).

Multi-array Sensors

In addition to analytical probes, some online sensors measure a similar set of chemical parameters by utilizing reagent-less electrochemical technology. These units can be configured as multi-array sensors to monitor for a number of chemical parameters simultaneously. As with the online analytical probes, the multi-array sensors can be operated remotely with data reported to a SCADA system.

Censar Technologies Inc.* (formerly Dascore Six-Cense) manufactures a multi-array device called the Multiparameter Water Quality/Security Sensor. This device, designed as a 1 in.² ceramic chip layered with gold, can be permanently inserted into a pressurized water main, ranging in diameter from 2 to 72 inches, or into a sidestream of water. It can monitor simultaneously for pH, DO, temperature, ORP, conductivity, and either chlorine or monochloramine. The sensor chip is field-replaceable with a typical 6-month life according to the manufacturer. The Censar multi-array sensor has been

* Censar Technologies Inc., Wimborne Dorset, UK

deployed for several years within the Mohawk Valley Water Authority distribution system in Utica, N.Y. (Schreppel 2003).

Real-time Toxicity Biomonitoring

Because so many toxic chemicals could potentially contaminate water, it is impossible to detect all of them using contaminant-specific monitors or even surrogate chemical monitors. Therefore, some utilities employ biosensors as a broad spectrum, first-order screening approach to detect the presence of harmful substances in water. Most biomonitoring measure changes in the behavior or physiology of living organisms resulting from stresses induced by toxicity. Other biomonitoring detect toxic substances through cellular responses of prokaryotic cells (bacteria) or eukaryotic cells (from higher-level organisms). Fast-acting toxins associated with acute effects are detected most easily, while toxins associated with chronic effects (e.g., mutagens, carcinogens, teratogens) may not be detected at all.

The use of living organisms to detect toxicity in drinking water and wastewater is reminiscent of the historic use of canaries in coal mines to detect hazardous gases. The initial impression of many utility operators is that this approach seems simplistic and crude. However, the advantage of using biosensors is that there are no analytical methods or instruments available that can actually measure toxicity. Only a living organism can integrate all the factors that contribute to toxic stress.

Furthermore, biosensors can detect the combined or synergistic effects of multiple toxins. A disadvantage associated with biosensors is the fact that while they can suggest that something unusual is in the water, they can't identify the specific toxicant. Toxicity tests, utilizing living organisms as sensors, have been used for many years to monitor wastewater effluent streams for National Pollutant Discharge Elimination System (NPDES) permit compliance. However, this technology is now being adapted for use in drinking water/wastewater online screening applications. Useful locations for such monitors in drinking water utilities could include the source water influent to a treatment plant, the finished water effluent from a plant, and strategic locations within the distribution system. Useful locations in wastewater utilities might include critical sites within the collection system, as well as the influent and discharge points at the treatment plant.

A number of different biosensors are currently being used in various countries to screen for toxic substances in water. Several US cities, including San Francisco; Washington, D.C.; and New York, have acknowledged the use of online biosensors in their drinking water systems in the technical literature and popular media. The most commonly used biosensors are described in the following section. Because living organisms and cells are sensitive to chlorine and other water treatment chemicals (e.g., chloramines, copper) many biosensors have been limited to source water applications. However, devices to continuously remove chlorine have been developed by

some manufacturers (e.g., Geo-Centers, Inc.^{*}) to permit biosensors to be utilized for finished drinking water applications. Consequently, several US cities are currently employing various types of biosensors to monitor their distribution systems.

Bacteria-based biosensors. As described in chapter 15 of this book, several bacteria-based biosensors are commercially available for use as rapid analytical devices to analyze grab samples collected during the investigation of a contamination threat. These acute toxicity sensors are effective because the metabolism and/or cellular structure of bacteria react rapidly to the presence of toxins. Some bacteria exhibit natural or genetically engineered bioluminescence that emits measurable light when the bacterial cells are healthy. Because the bioluminescence is closely tied to bacterial respiration, changes in metabolism or cellular structure can decrease luminescence. A decrease in bioluminescence, which can be measured with a photometer, suggests the presence of a toxic substance. Still other detectors monitor bacterial metabolism via changes in bacterial oxygen demand.

A bacteria-based toxicity sensor that is commercially available for continuous online use in water is the TOXcontrol system manufactured by microLAN[†]. This automated biomonitoring system utilizes freshly cultivated fluorescent bacteria, *V. fischeri*, as the biological sensor. The natural luminescence of the bacteria is measured before and after exposure to 4.5 mL of the suspect water to estimate the degree of toxicity. The estimate of toxicity is calculated using a computer software package that is part of the biomonitoring system. Toxicity standards are run at preset time intervals for system calibration. The bacteria are cultivated in a separate bioreactor for automatic and controlled cultivation. The manufacturer claims that only weekly maintenance of the system is required. A thiosulfate dechlorination system can be included to permit operation within a chlorinated municipal water system.

Daphnia toximeters. Daphnia (water fleas) are small free-swimming crustaceans that are visible to the naked eye and are very sensitive to toxic substances. In fact, *Daphnia magna* has been utilized for more than 100 years for chronic toxicity testing of raw and treated waters as well as industrial effluents. Online Daphnia toximeters utilize a number of daphnids housed in a glass chamber through which the water being monitored continuously flows. The swimming behavior of the daphnids is monitored by CCTV and the data are analyzed by computer. Changes in swimming behavior by several daphnids suggest the possible presence of a toxic substance in the water. This surveillance device has been used in Europe and was employed during the 2002 Winter Olympic Games in Salt Lake City, Utah.

A Daphnia Toximeter manufactured by bbe Moldaenke[‡] is deployed

* Geo-Centers, Inc., Newton, Mass.

† microLAN, the Netherlands

‡ bbe Moldaenke, Kiel-Kronshagen, Germany

online with a measuring cycle of 30 minutes. Toxicity is monitored by observing swimming speed, swimming altitude, turning and circling movements, as well as the number of live daphnia.

Mussel monitors. Mussels are filter feeders that obtain their food by sifting through large volumes of water. If toxic substances appear in the water, mussels avoid exposure by closing their shells. The frequency of valve opening and closing can be monitored to indicate toxin avoidance behavior.

In the commercially available mussel monitors, the shells of a number of mussels are glued to the top of a flow-through unit. Valve opening and closing is monitored by high-frequency induction sensors attached to the shells. A variety of mussels have been employed for monitoring including clams, oysters, blue mussels, and even the nuisance organism zebra mussels. Delta Consult* sells the MosselMonitor which can be used to monitor chlorinated drinking waters because it utilizes a continuous thiosulfate pretreatment device to remove chlorine. According to the manufacturer, the MosselMonitor, can be operated online continuously for a two to three month period before replacement of mussels is required.

Algae toximeters. In these monitoring devices, chlorophyll fluorescence is utilized as the indicator of water quality. If water quality is good, algae photosynthesize and naturally fluoresce. However, if substances are present in the water that negatively affect the algae, both photosynthesis and fluorescence are decreased. A reduction in fluorescence indicates a decrease in the active chlorophyll concentration, and suggests the presence of a substance toxic to the algae, such as an herbicide. The commercially available systems utilize either algae already present in the water being tested or algae continually cultured in a fermenter and automatically injected, in precisely defined amounts, into the measurement chamber. The algal fluorescence sensor is normally interfaced with a personal computer to facilitate interpretation of results.

The algae toximeter manufactured by bbe Moldanke features algae that are continually cultured in a fermenter that regulates the concentration and activity of the algae. A raw water sample is automatically injected with a pre-set concentration of algae, at specified time intervals, and algal fluorescence is measured. Photosynthetic activity and fluorescence of the algae should be relatively constant if no toxic substances are present.

Fish sentinel systems. There are several types of biosensor systems that utilize fish as toxicity sentinels. The simplest approach is the avoidance behavior sensor which is based on the fact that fish tend to swim away from water containing toxic or irritating substances. Such a system typically involves housing fish in a series of connected tanks that the water being monitored continuously passes through. The sentinel fish are fed in the first tank that receives the test water and tend to spend most of their time there. However, if water quality in the incoming water deteriorates, the fish swim

* Delta Consult, the Netherlands



Courtesy of Bio-Sensor Inc.

Figure 12-3. Bio-Sensor, Inc. Fish Biomonitoring System

sors in the test chambers. The results are typically interpreted by a computer, which can be linked to an alarm. Several systems are commercially available and are being used for source water monitoring, and when accompanied by dechlorination devices, are utilized for distribution system water monitoring.

One fish sentinel system currently on the market is the Bio-Sensor model 7008*. In this device, changes in fish ventilatory behavior and certain locomotor activities are detected through noninvasive electronic sensors in each individual fish tank. When a predetermined number of the eight fish being monitored on independent sensor channels respond simultaneously in an abnormal manner, an alarm is activated. The number of fish that need to respond to set off the alarm can be adjusted by the sensor system operator. Other commercially available systems include the Intelligent Aquatic Biomonitoring System IAC 1090[†] and the Medaka Sensor[‡].

Mikol and colleagues (2007) described the New York City Department of Environmental Protection's experiences using ventilatory changes in fish

into the downstream tanks and finally into an escape tank which is plumbed so that the water doesn't turn over as frequently as in the upstream tanks. This avoidance behavior by the fish suggests the presence of toxic substances in the water being monitored.

A more sophisticated approach involves observation of changes in physiological patterns of the sentinel fish (e.g., ventilatory frequency, ventilatory depth, gill purge). Should a toxic substance appear in the water stream continually passing through the test chambers, the ventilatory patterns of the fish in the sensor system may change and the change can be detected by noncontact sen-

* Bio-Sensors, Inc., Blacksburg, Va.

† Intelligent Automation Corp., Poway, Calif.

‡ Seiko Corp., Japan

to protect the source waters for the New York City drinking water system. They found that the biomonitor could be operated for extended periods of time with minimal maintenance and downtime. They reported several instances in which the biomonitor was successfully able to detect the presence of accidentally discharged surface water contaminants in the source water. Mikol and colleagues also reported the concentration ranges of some contaminants that elicited a response among bluegills in laboratory studies that they had previously conducted. These included a positive response to cyanide at 0.01–0.10 mg/L, mercury and zinc at 0.1–1.0 mg/L, malathion at 1.0–10.0 mg/L, phenol at 10.0–100.0 mg/L, and acetone at greater than 100 mg/L.

Monitoring for radiation to detect radionuclides. Radiation monitoring equipment is designed to measure either the total amount of radiation emitted from a source (gross radiation), or the specific type and energy level of radiation emitted from a source. Utility officials trying to determine whether there is an elevated level of radiation in the water from accidental releases or intentional introductions do not necessarily require that the specific radionuclides causing the contamination be immediately identified. Rather, they would most likely be interested in utilizing some type of continuous, online screening equipment to measure gross radiation.

The common types of radiation are alpha, beta, and gamma. Alpha emitters release heavy positively-charged particles that have a short range and are unable to penetrate skin. They can cause a serious health hazard if they are consumed as part of radiation-contaminated water. Beta emitters discharge lightweight, negatively-charged particles (electrons) that have a medium range (several feet through air) and moderate penetrating capabilities through objects. In contrast, gamma emitters emit very long-range electromagnetic radiation that can penetrate through a variety of objects including human skin and clothing. Measuring alpha and beta emissions in water is difficult because these short-range radiations are easily blocked by water before they reach the detector.

Furthermore, the fact that water surfaces are not smooth interferes with the effectiveness of gas flow proportional counters, which are designed to measure alpha and beta radiation from smooth solid surfaces. For these reasons, alpha and beta radiation in water samples are usually measured in the laboratory using a large, sensitive scintillation counter.

Online instruments for monitoring alpha, beta, and gamma radiation in water have been developed. However, there are a limited number of models available, and they can be expensive. Technical Associates^{*} offers the NexGen-SSS. This is a continuous, flow-through scintillation detection system for alpha, beta, and gamma radiation monitoring. The detector can be utilized to measure one type of radiation or all three combined and can be

* Technical Associates, Los Angeles, Calif.

equipped with a device that sends an alert if unusual counts are detected. Canberra^{*} sells the OLM-100 On-Line Liquid Monitoring System, which is attached to the exterior of a pipe and continuously measures the quantity of radiation in a liquid stream. The cost of this device is between \$35,000 and \$70,000 (USEPA Water and Wastewater Product Guide).

Detecting, Identifying, and Quantifying Specific Chemical Contaminants

Unlike the general organic chemical load monitors (TOC, UV₂₅₄), gas chromatography (GC) and gas chromatography–mass spectrometry (GC–MS) can detect, identify, and measure the concentrations of specific organic compounds. In fact, in contrast with all of the online physical and chemical monitors previously described, GC and GC–MS are the only analytical instruments currently being deployed in a continuous online mode that can actually identify a specific chemical contaminant. Both of these instruments can detect and identify a large number of volatile organic compounds (VOCs) in the low micrograms per liter to milligrams per liter range and can operate automatically and unattended. In the case of GC, the components of a complex mixture can be separated, compared to known standards, and the concentrations then quantified. Using GC–MS, the organic components of a matrix are separated by GC, and a more definitive identification of specific contaminants is provided by MS using the mass-to-charge ratio of chemical compound fragments and comparing this mass spectrum with libraries that contain thousands of chemical fingerprints of known organic compounds.

Some of the online instruments collect and concentrate VOCs from water using standard purge-and-trap technology. In this process, VOCs are initially purged from the water sample using a purge gas such as helium and are sorbed onto an organic resin trap. The compounds are subsequently desorbed from the trap by flash heating and then enter the GC column for subsequent separation. In the continuous online mode, sample collection is automated and occurs at regular, programmable intervals throughout a 24-hour period.

The CMS 5000 Monitoring System manufactured by INFICON[†] is a gas chromatograph that can be operated continuously in an unattended mode to detect a variety of VOCs that may be present in either raw source water or finished drinking water. This instrument concentrates VOCs in water via the purge-and-trap method using a SituProbe. The INFICON HAPSITE GC–MS, described in more detail in chapter 15, has been retrofitted by the manufacturer to develop a system that can provide continuous online GC–MS analysis of raw and finished waters.

* Canberra, Meridean, Conn.

† INFICON Corp., East Syracuse, N.Y.



Courtesy of Inficon

Figure 12-4. Inficon CMS 5000 Monitoring System

A highly specialized mass spectrophotometer is used to screen water samples, in an online mode, at the Phoenix Arizona Water Services Department. This photoionization and quadropole ion trap, time-of-flight mass spectrometer provides high-speed screening and molecular identification for weaponized chemicals and other hazardous compounds (Calles et al. 2005). The commercially available mass spectrometer is operated in an automated mode. The advantage of this particular mass spectrometric approach is that it can be operated online and, unlike most mass spectrometers, can analyze mixtures of compounds without preliminary separation by GC. With its integrated autosampler, the instrument provides a high throughput monitor capable of analyzing samples every 45 seconds.

Detecting, Identifying, and Quantifying Specific Pathogens

The multiparameter water quality monitoring technologies described indicate the presence of unusual chemicals in water. The biosensor technologies, utilizing biological species as sentinels, detect the presence of toxic substances. The specific chemical analyzers (GC, GC-MS) identify VOCs. However, none of these devices are capable of detecting harmful microorganisms (bacteria, viruses, protozoans). Pathogenic microorganisms are often species- or tissue-specific and require incubation times of days or weeks before disease symptoms are noticeable. As described in chapter 15, some rapid analytical techniques, such as polymerase chain reaction (PCR), can be used to analyze grab samples in the field to preliminarily detect and identify pathogens. At this time, the inability to screen for microbes online is a glaring weakness in continuous monitoring technology. A couple of approaches currently being pursued for developing online microbial detection capabilities are described in the following sections.

Light-scattering technology. Light-scattering technology has been used in the water industry for decades to measure turbidity and continues to be an important tool for utility operators for day-to-day process control. Drinking water regulatory agencies rely heavily on light-scattering technology to verify the operational adequacy of individual treatment plants.

Light-scattering technology is now being explored as a continuous monitoring method for detecting and identifying waterborne microbes. The multi-angle light-scattering (MALS) technique screens a flowing column of water

and attempts to distinguish various microorganisms based on optical recognition. This reagent-less technology is used to develop an optical fingerprint of a microbe based on the dispersion of a laser beam caused by microbes present in a flowing column of water. Because a number of different angles are monitored simultaneously, a three-dimensional pattern is generated that represents the structure and size of the particle in the laser's path. The goal of MALS is to differentiate between waterborne microorganisms and inanimate particles based on the pattern of scattered light. An additional objective is to identify species or classes of microbes by comparing the pattern of scattered light with a library of unique bio-optical signatures that have been developed by analyzing known microorganisms. The light pattern resembles a fingerprint because it is unique to the internal and surface features of the microbial cell, including size, shape, morphology, and material composition.

Quist and colleagues (2004) investigated the ability of a prototype of this technology to distinguish between *Cryptosporidium* oocysts and background particles in water. In this study, the identification rate of *C. parvum* oocysts ranged from 11 to 45 percent while false positive rates varied from 0.3 to 3 percent. The limits of detection in reagent-grade water were calculated to be 7, 0.7, and 0.1 oocysts/mL in 1-, 10-, and 60-minute assays, respectively. The limit of detection in finished drinking water samples was calculated to be 75, 7.5, and 1 oocysts/mL in 1-, 10-, and 60-minute readings.

A commercial version of the MALS analytical approach, the BioSentry System, has been developed by JMAR Technologies*. The instrument consists of multiple, laser-illuminated sensor units that can provide continuous real-time monitoring of finished water in a distribution system (Adams et al. 2006). The device utilizes a 660-nm wavelength laser light and a charge-coupled detector to collect the scattered light. The scattered light is collected from multiple angles, permitting the accumulation of more information on particle size and shape than would be available from a single collection point. A computer analyzes the shape, size, index of refraction, and internal structure of the particles in order to attempt to identify the microbe. The main challenges facing this technology are false-positives and achieving detection limits of public health significance. The system typically monitors a water stream of about 35 mL per minute.

As would be expected, sensitivity and the ability to discriminate between various particles and microbes are optimal with waters containing fewer background particles (i.e., <1,000 particles per mL). Current limitations of detection, as reported by the manufacturer, are approximately 150 organisms per mL over a 5-minute period of surveillance. The commercially available system is currently programmed to detect the parasites *Giardia* and *Cryptosporidium*, rod-shaped bacterium such as *E. coli*, and bacterial spores such as *B. anthracis*. Future developments are aimed at reducing detection limits and identifying additional microbes.

* JMAR Technologies, San Diego, Calif.



Photo by Liz Wessing

Figure 12-5. JMAR BioSentry Pathogen Monitoring Device

minutes. This system identifies contaminants using a signature based on the physical constants of proteins (such as molecular weight and charge-to-mass ratio).

The UWS is based on the microChemLab technology, a handheld, manually-operated device originally developed by Sandia Labs. The test water enters the automated sampling device and a 100- μ L sample of water is collected. The sample is pH buffered and reacted with a UV fluorogenic label. The sample then enters the detection system in which electrophoresis is used to separate components of the sample and a laser-induced fluorescent protein signature is recorded. The migration times are compared with a database of separations of threat agents and, if a specified matching threshold is reached, the system communicates the results.

The goal is to refine this system so that it can function without operator intervention for up to 30 days. Ideally, a sample would be analyzed every 30 minutes. The system currently recognizes protein signatures for the biotoxins ricin and staphylococcal enterotoxin B (SEB). The next developmental targets include nitrifying bacteria, algal toxins, and the bacterium *E. coli*. Ultimately, it is hoped that the system will be able to detect and identify a variety of bacteria, viruses, protozoans, and biotoxins. Detecting microorganisms will require the ability to solubilize the cell into individual proteins. In addition to protecting municipal water supplies, other potential applications for the UWS include monitoring of agricultural water for contaminants as well as water provided to sports arenas and other public events.

Protein signatures. Tenix Corporation and Sandia National Laboratories are refining an innovative technology originally developed by Sandia Labs for online, near real-time detection of pathogens and biotoxins in drinking water and wastewater. This device, the unattended water sensor (UWS) for water distribution systems, was tested in Glendale, Ariz. (WaterWorld 2008) and at a large California Bay area utility. It is intended to provide rapid automated and unattended contaminant detection and identification at a remote location (Sandia National Laboratory 2007). The signal could then be sent to a SCADA system within

Immunoassay. Research is also ongoing to develop online and portable detection devices that use a paramagnetic microbead immunoassay that is adaptable to a microfluidic monitoring system (Heineman et al. 2007). In this assay, the biological agent is “sandwiched” between two antibodies and either electrochemical or fluorescence methods are utilized for detection. Biological agents that are potentially detectable using this approach include biotoxins, vegetative bacteria, bacterial spores, and viruses.

Preliminary studies indicate that chlorine and chloramine may decrease the sensitivity of the assay. However, this may be correctable by dechlorination with thiosulfate prior to the analysis.

Gene probes. NASA, in conjunction with a private company, Early Warning Inc., is developing a device termed the *Nanotech Biosensor* (Gordon 2009). This online monitor is intended to detect a variety of specific bacterial, protozoan, and viral pathogens within a 2- to 3-hour period, without operator intervention. The mechanism involves automated concentration of a 10 L sample of water using ultrafiltration (UF) and disaggregation. RNA is then automatically extracted and identified using gene probes. An attempt is also being made to determine whether the bacteria are viable using a subsequent culture step. Growth of viable microbes in culture will require additional hours. Detection of viruses will likely require an additional concentration step. The goal is to identify and differentiate bacteria, such as *E. coli* and *E. coli* O157:H7, at a concentration of 1 colony forming unit (CFU) per 100 mL of original water sample.

CONCLUSIONS CONCERNING CONTINUOUS MONITORING TECHNOLOGY

As indicated, there are five basic approaches to online monitoring for security concerns. While a significant amount of research and development is being devoted to physical, chemical, and biosensor systems, current technical capabilities are still rather limited. Unfortunately, the motivation for commercial development of innovative monitoring technology for drinking water and wastewater applications is probably limited because of the relatively small market represented by the water industry.

PLACEMENT OF SENSORS

A practical question that arises when utilities consider implementing a CWS is the optimum placement of sensors within the distribution system. Research on this topic has been summarized in USEPA's state-of-the-art review on EWS technologies (USEPA 2005a). For example, Uber and colleagues (2004) suggested an iterative numerical solution methodology using the “greedy heuristic” algorithm for sensor location. Berry and co-authors (2005) described the selection of monitoring locations within a distribution system as an optimization problem in which a quantity is optimized subject to a set of constraints.

USEPA's National Homeland Security Research Center (NHSRC) has developed the Threat Ensemble Vulnerability Assessment program (TEVA), which is a research project whose goal is to study contamination threats to drinking water systems and use the information gained to design monitoring and surveillance systems. TEVA uses a computational framework containing a suite of software tools that can simulate threats and identify vulnerabilities in drinking water distribution systems, measure potential public health impacts, and evaluate mitigation and response strategies. A Monte Carlo simulation approach is used to evaluate alternative sensor locations, number of sensors, sensor characteristics, sampling frequency, response time, and the type and duration of a contamination event. The criterion for performance is minimizing the number of people who would become ill from exposure to a contaminant. TEVA utilizes USEPA's EPANET software program to simulate hydraulic and water quality behavior in pipe networks. TEVA has been used to identify the optimal sensor placement in a number of large- and medium-sized drinking water distribution systems (Janke et al. 2005; Murray et al. 2006).

In collaboration with the University of Cincinnati, Sandia National Laboratories, and Argonne National Laboratory, USEPA has developed the Sensor Placement Optimization Tool (TEVA-SPOT). This software program uses algorithms to determine the optimal number and location of sensors needed to support a CWS that integrates monitoring and surveillance data from multiple detection streams. The program has been used to help design warning systems for a number of utilities. Additional information on this program is available at the TEVA Web site, www.epa.gov/nhsrc/water/teva.html.

Despite the availability of technical studies, as pointed out in USEPA's review of EWS technologies, many utilities establishing a CWS may not employ sophisticated models for sensor placement. Given limited budgetary and technical resources, many utilities make a modest initial investment in sensors to satisfy perceived security needs as well as process control and regulatory compliance requirements. These utilities may then choose to use a two-stage approach. In the first stage, likely sites for sensors are based on technological constraints such as availability of secure locations, external power, access to communications, and accessibility for maintenance. In many cases, utilities tend to use facilities that they already own or control.

In the second stage, the potential sites are evaluated in terms of the amount of useful information that can be gained if a sensor is placed at that location. This may equate to placing sensors along larger mains that provide service to the most people. Most of these sensor-placement decisions are likely to be made by in-house personnel with a good working knowledge of the water system. However, while many utilities are expected to follow this more simplistic approach to sensor positioning, the value of in-depth, sophisticated studies on the strategic positioning of monitors should not be diminished. The hope is that even the utilities implementing a pragmatic approach to sensor system design will benefit from some of the broad guidance generated by more theoretical studies.

INTEGRATED CONTAMINANT WARNING SYSTEMS

It is clear that the large amounts of data generated by a series of single parameter, and especially multiple parameter sensors, deployed throughout a water distribution network or wastewater catchment network will require an automated system for data collection, sorting, interpretation, and storage. In most cases, this will be handled by the utility's SCADA system. An integrated CWS includes not only sensors to detect the contamination, but also mechanisms to transmit, compile, and analyze data; links for communication and notification; and procedures for emergency response.

Use of data acquisition software and a central data management center is important. Individual sensors must be equipped with transmitters, modems, direct wire, or wireless devices to communicate the data to the acquisition and management systems. As indicated by Bukhari and LeChevallier (2006), a majority of the commercially available, multiparameter online monitors are equipped with analog (4–20 mA) or digital data outputs (RS-232, RS-485), thus allowing connectivity via remote telemetry units, radio transmitters, or cellular/satellite modems. Hardwired transmission requires the physical connection of cable or wire, and requires either coaxial or fiber optic technology. Wireless transmission utilizes a variety of techniques, including microwave, UHF or VHF radio, basic telephone modems, cellular telephone modems, or satellite. Wireless transmission may require direct line of sight between the transmitter and receiver, or the use of retransmitters (i.e., repeaters and amplifiers). The least expensive transmission systems are usually phone lines or direct wire. Transmission of unencrypted data is a security risk, so hardware and software may need to have encryption capabilities.

Signal authentication equipment is available to ensure that the data being received from a remote sensor is genuine and has not been manipulated by a cyber hacker. A mechanism for automated data validation can help ensure that accurate results are generated from data analysis. One approach is to compare data received from the monitoring sites with data stored at the sensor locations to validate accuracy and completeness. Traditional SCADA systems perform data validation processes such as range checking.

Additionally, the data management system must be able to perform some level of data analysis and trending to assess whether an alarm should be initiated. Algorithms have been developed and are being evaluated to determine how well the algorithms identify water quality changes in addition to how few false alarms they generate (McKenna et al. 2008).

USEPA has partnered with Sandia National Laboratories to develop data analysis software to assist water utilities in detecting contamination. This software, named CANARY, has been deployed at the USEPA Water Security Initiative pilot utility in Cincinnati, Ohio, where it is operating in real time. The CANARY software is a Windows®-based program that evaluates standard water quality data (e.g., free chlorine, TOC, pH) and uses mathematical and

statistical techniques to identify anomalous water quality incidents. Before using CANARY online for actual system monitoring, historical utility data must be analyzed to determine the natural variation of these water quality parameters. Information on the availability of CANARY is available at the NHSRC Web site, www.epa.gov/nhsrcc/water/teva.html.

Once online monitoring data indicate that a trigger level has been exceeded, a decision must be made regarding the action to be taken by the utility. For example, the system may notify operators. It may also be possible to program the data management system to automatically initiate preliminary response actions such as collecting samples or closing distribution system valves. Of course, caution must be exercised to prevent significant operational changes from being made as a result of false-positive alarms.

HYDRAULIC MODELS

The design of a CWS can be facilitated through the use of a well-calibrated hydraulic model that predicts the movement and fate of contaminants. Hydraulic models are decision support tools that assess the spread of contaminants throughout a distribution or collection system. A number of models are available commercially. Additionally, three security hydraulic models have been developed by the SAIC under contract with USEPA. One focuses on modeling contaminant movement in source waters (IC Water), and one models contaminants in drinking water distribution systems (PipelineNet) (Bahadur et al. 2003). Still another predicts the transport and fate of contaminants in wastewater collection systems (SewerNet). PipelineNet can be used to help locate monitors in a municipal drinking water distribution system once a water utility sets priorities such as physically accessible sites for monitoring; priority areas based on flow, velocity, pressure, and water quality; and proximity to critical facilities such as schools, hospitals and government buildings. These models, available free of charge to drinking water and wastewater utilities, are discussed in greater detail in chapter 6.

AUTOMATIC SAMPLE ARCHIVING

A practical component of a CWS, adopted in some recently established online monitoring systems, is the capability for automatic sample archiving. When an alarm is triggered by a field monitor, an automated sample collection device is activated without human intervention to capture and store a sample of the water responsible for setting off the alarm. The stored sample can subsequently be analyzed in the field by response personnel utilizing rapid analytical techniques. Alternatively, the sample may be transported to a laboratory for more definitive analysis. If a contaminant is introduced in slug fashion, either intentionally or accidentally, the contamination may pass by the sensor before a response team can arrive to collect a grab sample. This could make it difficult to determine whether the monitor had actually detected a transient spike of contaminant or if there was a false alarm. It could also interfere with

efforts to definitively identify the contaminant and preserve evidence for a criminal investigation. Linking an automatic sampling device to one or more online sensors can address this potential problem.

TIERED APPROACH TO MONITORING

An additional concept for CWS, advocated by Hassan and colleagues (2004), is that of a tiered approach with two stages. The first stage utilizes continuous real-time sensors that trigger an alarm when a contaminant is detected in the water. This may involve basic instrumentation such as multiparameter online sensors (e.g., pH, conductivity, chlorine residual). The alarm then initiates a second stage of monitoring that employs more sensitive and specific technologies to confirm and actually identify the contaminant. The second-stage technology could already be located at the field site and may involve instruments such as gas chromatographs or gas chromatograph–mass spectrometers that would begin automated sampling and analysis only when triggered by the first-stage alarm.

COMPREHENSIVE CWS

Given the limited capabilities of online contaminant monitoring technology, the current emphasis is on designing more comprehensive CWSs that integrate information from a variety of sources. Considered alone, any one of these information sources may not be sufficient to adequately alert a utility to the possibility of an accidental or intentional contamination of the public water supply. However, data from several sources can improve the utility's ability to detect a contamination event. The sources of information being employed for comprehensive EWSs include:

- Data from continuous online physical/chemical/radiological sensors and biosensors
- Data from routine grab samples from the distribution system
- Consumer complaints
- Enhanced security monitoring (e.g., cameras, access hatch contact alarms)
- Reports of security incidents (e.g., threatening phone calls, cut fences)
- Security advisories and intelligence threat analysis (e.g., FBI, local police, USEPA, ISAC, Infragard)
- Syndromic surveillance data (e.g., data on emergency room visits, over-the-counter drug sales, lab diagnostic test orders, 9-1-1 and poison control center calls, school absenteeism, and HMO records delivered to a central database from hospitals, pharmacies, and other agencies across a city, county, or state).

In syndromic surveillance systems, the reported illness data are not actual diagnosed diseases but rather prediagnosis markers that include chief

complaints or symptoms such as influenza-like illness, rash with fever, diarrhea/vomiting, and encephalitis. Many cities and counties use these electronic public health syndromic surveillance system programs to help identify potential disease outbreaks early.

A major waterborne cryptosporidiosis epidemic occurred in Milwaukee, Wis. in 1993, resulting in 400,000 illnesses and more than 100 deaths. One of the initial indications that a major outbreak was occurring was the fact that Milwaukee pharmacies exhausted their supplies of over-the-counter diarrhea remedies. A retrospective analysis of the epidemic suggested that the outbreak could have been detected much earlier, with a significant reduction in morbidity and mortality, had a syndromic surveillance system been in place at that time (Proctor et al. 1998).

In the opinion of some investigators, even syndromic surveillance systems are somewhat insensitive because less than 8 percent of people with gastrointestinal illness in the United States seek medical care, and even fewer have stool specimens tested for pathogens. Outbreaks involving unusual pathogens or toxins and small numbers of people would probably be missed, or water may not be considered as a likely vehicle of transmission, if perpetrators of an intentional contamination event did not claim responsibility (Khan et al. 2001).

The inclusion of enhanced surveillance activities involving multiple sources of information, rather than relying solely on water quality data from online monitors, should greatly improve the sensitivity of a CWS. In the broader sense, a comprehensive CWS is actually more than just sources of information indicating that a contaminant may be present in drinking water or wastewater. Rather, an effective CWS is a combination of monitors, institutional arrangements for detection and response, analytical tools, emergency protocols, and response mechanisms designed to provide early warning of contamination and initiate a response to minimize the impact on people, property, and infrastructure.

USEPA WATER SECURITY INITIATIVE

HSPD 9 directed USEPA to “develop robust, comprehensive, and fully coordinated surveillance and monitoring systems...that provide early detection and awareness of disease, pest or poisonous agents.” In response to this mandate, USEPA is working with technical experts and stakeholders in the drinking water industry to design, deploy, and evaluate a comprehensive drinking water continuous monitoring system that would provide an early indication of contamination and minimize the public health and economic impacts that could result. This program has taken the form of a demonstration project termed the Water Security Initiative (WSI) (USEPA 2007a).

The WSI is a demonstration project where USEPA, in partnership with select utilities and laboratories, is designing, deploying, and evaluating a model CWS for drinking water security. The initial pilot utility for the WSI

is the Greater Cincinnati Water Works. Four additional pilot cities, all with large water systems serving more than 750,000 people, have subsequently received federal grants through a competitive process, and are also part of the WSI. The additional WSI cities include New York, San Francisco, Dallas, and Philadelphia. These prototype monitoring systems incorporate information from all the data sources previously listed and explore the use of appropriate response measures to contamination threats and incidents. The ultimate goal of the project is to demonstrate the concept so that drinking water utilities of all sizes and characteristics can implement their own effective warning systems. Development of a CWS for an individual water system, outside of the initial demonstration pilots, would be at the expense of the utility itself.

USEPA has published several guidance documents on the development and operation of CWSs based on their findings in the Cincinnati pilot system (USEPA 2005b; 2007a, b; 2008a, b, c). These documents can be found at http://www.epa.gov/safewater/watersecurity/pubs/guide_securityinitiative.

CITIES DEVELOPING A CWS

In addition to the cities involved in the USEPA WSI, a number of other drinking water utilities are developing their own CWSs. While some of these utilities prefer to keep details of their CWS private, others have reported on their efforts in the literature. These include New York City (Mikol et al. 2007); Glendale, Ariz. (Thompson et al. 2008); Laredo, Texas (Shadevich et al. 2008); Ann Arbor, Mich. (Skadsen et al. 2008); and Pittsburgh, Pa. (States et al. 2007). In the Pittsburgh online monitoring system, a number of experimental trials have been conducted to test the response of the online analyzers to a variety of contaminants. The analyzers include monitors for pH, conductivity, turbidity, chlorine, and TOC, as well as online GC–MS, fish biosensors, UV transmittance, and a pathogen detector utilizing the MALS technology (States et al. 2008). This online sentinel system was also used to monitor the safety of drinking water during the G20 Summit held in Pittsburgh in September 2009.

ADDITIONAL RESOURCES

Two published reports deal specifically with the issue of continuous monitoring in water systems with an emphasis on security applications. The first report, *Interim Voluntary Guidelines for Developing an Online Contaminant Monitoring System* was produced by ASCE, AWWA, and WEF (2004), under a cooperative agreement with USEPA. This guidance document and a series of related white papers provide specific guidance to utilities about the design and implementation of online contaminant monitoring systems.

The second report, *Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality: A State of the Art*

Review, was published by USEPA's Office of Research and Development and the NHSRC (USEPA 2005a). The report is a review of EWS technologies for identifying chemical, microbial, and radiological contaminants, especially as applied to drinking water distribution systems. It also describes emerging technology and provides recommendations for additional research needed to further development of CWSs.

REFERENCES

- Adams, J.A., D. McCarty, and K. Croushore. 2006. A Real-Time Early Warning System for Pathogens in Water. *Proc. of SPIE Conference*, Orlando. Vol. 6218. Bellingham, Wash.
- American Society of Civil Engineers (ASCE), American Water Works Association (AWWA), and Water Environment Federation (WEF). 2004. *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*. Denver, Colo.: AWWA. www.awwa.org/science/wise.
- Awwa Research Foundation (AwwaRF). 2001. *Design of Early Warning and Predictive Source-Water Monitoring Systems*. AwwaRF Report 90878. Denver, Colo.: AWWA.
- AwwaRF. 2002. *On-line Monitoring for Drinking Water Utilities*. AwwaRF Report 90829. Denver, Colo.: AWWA.
- AwwaRF. 2007. *Rapid Detection of Bioterrorism Agents in Water Supplies*. AwwaRF Report 91195F. Denver, Colo.: AwwaRF.
- Bahadur, R., W.B. Samuels, and J. Pickus. 2003. *Case Study for a Distribution System Emergency Response Tool*. Denver, Colo.: AwwaRF.
- Berry, J., L. Fleischer, W. Hart, C.A. Phillips, and J.P Watson. 2005. Sensor Placement in Municipal Water Networks. *Jour. Water Resources Planning and Mgmt.*, 131(3):237.
- Bukhari, Z., and M. LeChevallier. 2006. Enhanced Monitoring to Protect Distribution System Water Quality. *Proc. 2006 AWWA WQTC*. Denver, Colo.: AWWA.
- Byer, D., and K.H. Carlson. 2005. Real-Time Detection of Intentional Chemical Contamination in the Distribution System. *Jour. AWWA*, 97(7):130.
- Calles, J., R. Gottler, M. Evans, and J. Syage. 2005. Early Warning Surveillance of Drinking Water by Photoionization/Mass Spectrometry. *Jour. AWWA*, 97(1):62.
- Gordon, N. 2009. Direct Measurement of Total and Viable Cell Concentrations of Specific Pathogens in Water Networks Using NASA's Nanotech Biosensor. *Proc. 2009 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Hall, J., A.D. Zaffiro, R.B. Marx, P.C. Kefauver, E.R. Krishnan, R.C. Haught, and J.G. Herrmann. 2007. On-line Water Quality Parameters as Indicators of Distribution System Contamination. *Jour. AWWA*, 99(1):66.
- Hassan, J., S. States, and R. Deininger. 2004. Safeguarding the Security of Public Water Supplies Using Early Warning Systems: A Brief Review. *Jour. Contemporary Wat. Res. and Edu.*, 129, 27.
- International Life Sciences Institute Risk Science Institute (ILSI). 1999. *Early Warning Monitoring to Detect Hazardous Events in Water Supplies*. Washington, D.C.: ILSI. www.ilsi.org/publications/pubslist.cfm?publicationid=268.
- Janke, R., R. Murray, J. Uber, and S. Allgeier. 2005. An Evaluation of System Architectures for Contamination Warning Systems. *Proc. 2005 World Water and Environmental Resources Congress*. Reston, Va.: ASCE.
- Khan, A.S., D.L. Swerdlow, and D.D. Juranek. 2001. Precautions Against Biological and Chemical Terrorism Directed at Food and Water Supplies. *Pub. Hlth. Rep.*, 116, 3.
- Kroll, D. 2008. Testing the Waters: An Olympic-Size Task. *Opflow*, 34(12):10.
- McKenna, S.A., M. Wilson, and K.A. Klise. 2008. Detecting Changes in Water Quality Data. *Jour. AWWA*, 100(1):74.
- Mikol, Y.B., W.R. Richardson, W. Van Der Schalie, T.R. Shedd, and M.W. Widder. 2007. An Online Real-Time Biomonitor for Contaminant Surveillance in Water Supplies. *Jour. AWWA*, 99(2):107.
- Murray, R., Berry, J.W., and Hart, W.E. 2006. Sensor Network Design for Contamination Warning Systems: Tool and Applications. *Proc. 2006 AWWA Water Security Congress*, Washington, D.C.

- Proctor, M., K. Blair, and J. Davis. 1998. Surveillance Data for Waterborne Illness Detection: An Assessment Following a Massive Waterborne Outbreak of *Cryptosporidium* Infection. *Epidemiol. Infect.*, 120, 43.
- Quist, G.M., R. DeLeon, and I.C. Felkner. 2004. *Evaluation of a Real-Time Online Monitoring Method for Cryptosporidium*. AwwaRF Project 91020F. Denver, Colo.: AWWA.
- Sandia National Laboratory. 2007. Sandia's Unattended Water Sensor Capable of 24/7 Detection of Toxins, Bacteria in Water Supplies. Los Alamos, N.M. www.sandia.gov/news/resources/releases/2007/watersensor.html.
- Schreppel, C.K. 2003. Distribution System Security: Setting the Alarm for an Early Warning. *Opflow*, 29(6):1.
- Shadevich, Y. 2008. Laredo, Texas Case Study: Developing a Contamination Warning System. *Proc. 2008 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Skadsen, J., R. Janke, W. Grayman, W. Samuels, M. Tenbroek, B. Steglitz, and S. Bahl. 2008. Distribution System On-Line Monitoring for Detecting Contamination and Water Quality Changes. *Jour. AWWA*, 100(7):81.
- States, S., M. Stoner, C. Westbrook, D. Heza, and L. Casson. 2007. Development of a Contamination Warning System for the Pittsburgh Water and Sewer Authority. *Proc. 2007 AWWA WQTC*. Denver, Colo.: AWWA.
- States, S., B. Hohman, C. Westbrook, M. Stoner, and L. Casson. 2008. Challenge Studies of the Pittsburgh Distribution Network Pilot Contamination Warning System. *Proc. 2008 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Szabo, J.G., J.S. Hall, and G. Meiners. 2008. Sensor Response in Chloraminated Water. *Jour. AWWA*, 100(4):33.
- Thompson, K.A. 2008. Operational Enhancements Resulting from the Development and Implementation of a Contamination Warning System for Glendale, Arizona. *Proc. 2008 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Uber, J., R. Janke, R. Murray, and P. Meyer. 2004. Greedy Heuristic Methods for Locating Water Quality Sensors in Distribution Systems. *Proc. 2004 EWRI Congress*. Denver, Colo.: AWWA.
- USEPA. 2005a. *Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality: A State of the Art Review*. Washington, D.C.: USEPA. www.epa.gov/nhsr/pubs/reportEWS120105.pdf.
- USEPA. 2005b. *Water Security Initiative: Water Sentinel System Architecture*. EPA-817-D-05-003. Washington, D.C.: USEPA. <http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm>.
- USEPA. 2007a. *U.S. EPA Water Security Initiative*. Washington, D.C.: USEPA. www.epa.gov/safewater/watersecurity/pubs/fs_watersecurity_securityinitiative.pdf.
- USEPA. 2007b. *Water Security Initiative: Interim Guidance on Planning for Contamination Warning System Deployment*. EPA-817-R07-005. Washington, D.C.: USEPA. <http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm>.
- USEPA. 2008a. *Interim Guidance on Developing Consequence Management Plans for Drinking Water Utilities*. EPA-817-R-08-001. Washington, D.C.: USEPA. <http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm>.
- USEPA. 2008b. *Water Security Initiative: Interim Guidance on Developing an Operational Strategy for Contamination Warning Systems*. EPA-817-R-08-002. Washington, D.C.: USEPA. <http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm>.
- USEPA. 2008c. *Water Security Initiative: Cincinnati Pilot Post-Implementation System Status*. EPA-817-R-08-004. Washington, D.C.: USEPA. <http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm>.
- USEPA Water and Wastewater Product Guide. Washington, D.C.: USEPA. www.epa.gov/safewater/security.
- WaterWorld. 2008. City, Firm Partner on Contaminant Warning System Implementation. *WaterWorld*, 24(1):30.

RESPONSE TO INCIDENTS AND THREATS

Almost every utility will at some point be affected by a natural disaster or major accident. Financial, cultural, and political considerations place a practical limitation on the extent to which PPSs can be employed to safeguard utilities against such incidents. And it is almost impossible to prevent certain malevolent acts, such as injection of a contaminant directly into the distribution or collection system, from occurring if a perpetrator is determined. For all of these reasons, utility managers need to emphasize effective planning of their responses to natural disasters, accidents, and manmade events to reduce the impact on drinking water and wastewater systems and the public that they serve.

The importance of effective response planning is underscored by the public criticism that has been leveled against responses to past security breaches at water systems. The following example was published in a water industry newsletter. While this is an actual report of an incident, the names of the town and utility have been removed to avoid embarrassment to local officials and utility personnel.

“Local officials are criticizing the way a break-in at the water plant in a local county was handled, an incident that resulted in the shutting off of water services to many residents in the region.

“Roughly 30 hours passed between the discovery of the break-in Sunday morning and Monday’s precautionary shutdown of the water plant, which serves more than 4,000 customers.

"The security breach prompted hours of bureaucratic debate before residents were alerted to the possible danger, but the emergency-notification system failed to reach thousands of residents with the final decision: Don't drink, bathe or cook with the water.

"On Tuesday, officials began handing out bottled water to residents, several restaurants were forced to close, and state officials launched a battery of tests on samples from the plant.

"County officials say they don't think the intruders at the water plant had an opportunity to contaminate supplies and no illnesses linked to the water have been reported."

—*WaterTech e-News Daily*® (Jan. 15, 2003)

The importance of response planning is also highlighted by the inclusion of public works staff as official first responders in the early stages of an incident in Homeland Security Presidential Directive 8 (HSPD 8). Utility personnel are described in HSPD 8 as being responsible for the protection and preservation of life, property, evidence, and the environment. In the directive, public works personnel include drinking water and wastewater system employees.

A good response plan is one of the most effective tools that a utility can develop to improve their security and preparedness.

EMERGENCY RESPONSE PLANS (ERPs)

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) amended the SDWA by adding section 1433, "Terrorist and Other Intentional Acts." In addition to requiring all drinking water utilities serving more than 3,300 people to conduct a VA of their systems, the regulation required these same utilities to prepare or upgrade their existing ERPs to address intentional acts and incorporate the findings of the VAs. Because the Bioterrorism Act did not include the wastewater industry, there is no similar federal requirement for wastewater systems.

AWWA's manual of water supply practices, M19, *Emergency Planning for Water Utilities* (AWWA 2001a), was subsequently updated again in 2001 to include preparation and response recommendations for human-induced emergencies cased by theft, vandalism, accidents, and terrorism along with the more traditional information about planning for natural disasters such as floods, earthquakes, tornadoes, and hurricanes. Because major disruptions to water utilities have more frequently been caused by natural events than intentional events, the emphasis in the manual has always been on natural events. But shortly after Sept. 11, 2001, AWWA published a supplement to M19 that emphasizes response planning for security incidents entitled *Security Analysis and Response for Water Utilities* (AWWA 2001b).

USEPA has produced two guidance documents to assist utilities in developing or updating their ERPs. The first, *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* (USEPA 2003), was developed for large water systems (serving more than 100,000 people). The second document, *Emergency Response Plan Guidance for Small and Medium Community Water Systems to Comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (USEPA 2004), provides guidance on developing or revising ERPs for small (between 3,300 and 49,999 people served) and medium (between 50,000 and 99,999 people served) community drinking water systems. These documents describe the basic elements needed in an ERP and are easily adaptable to an all-hazards approach. The documents are available on the USEPA water security Web site, www.epa.gov/safewater/watersecurity/pubs.

USEPA and National Environmental Safety and Health Training Association (NESHTA) have produced a video on ERPs for small water systems serving fewer than 10,000 people. The video uses scenarios to show the viewer how to develop or revise an ERP, and highlights the relationship between an ERP and a system's VA results. The video is available, at no cost, from the NESHTA Web site, www.neshta.org/PDFs/orderform.pdf.

In 2004, the Water Environment Research Federation (WERF), in collaboration with USEPA, published *Emergency Response Plan Guidance for Wastewater Systems* to assist wastewater utilities in preparing their ERPs. The guidance is downloadable from WERF's Web site, www.werf.org.

An ERP is a guide that water and wastewater utilities follow to direct their response to emergencies. The plan should be comprehensive enough to cover natural disasters, accidents, and major equipment failures as well as terrorism and other intentional acts. Emergency plans may have a variety of titles including Emergency Preparedness Plans, Emergency Operations Plans, Contingency Plans, and Emergency Response Plans. Regardless of title, these plans all address the same issues. They should specify notification procedures, identify resources, and assign roles and responsibilities to specific individuals and groups within the organization. And perhaps most importantly, ERPs need to specify response actions that will control the impact of a critical incident, prevent the incident from escalating, and enhance the recovery process.

An ERP is a working document that should be used before, during, and after an emergency. It should be reviewed and revised on a regular basis, if for no other reason than to keep the notification information current. The plan, as it pertains to terrorism and other manmade incidents, is an outgrowth of, and should be developed from, the completed VA and actions that have been taken to mitigate risk from adversarial acts.

ERPs were already required for drinking water and wastewater utilities in most states prior to the Bioterrorism Act requirements for drinking water

systems. A number of states provide extensive guidance and templates for preparation of the plan and have made it an inspectable item during state regulatory visits. USEPA's position is that utility emergency plans must comply with all applicable state and local regulations. The USEPA guidance documents previously described are meant to supplement, but not replace or supersede, state requirements.

Ideally, prior to any emergency, an ERP has been coordinated with state and local emergency response organizations, regulatory authorities, and elected officials. Key utility personnel should be familiar with the entire plan. All utility personnel must know their individual roles as specified by the plan. The plan should be kept as simple as possible to ensure understanding and effective execution by everyone assigned a role. To guarantee successful implementation during an emergency, the plan should be periodically exercised. Chapter 17 describes tabletop and functional exercises that can be used to train personnel on the content and execution of the plan.

Essential Components of ERPs

ERPs should describe all emergencies that a utility might encounter and provide a detailed set of corrective actions. The plan must identify who is to be contacted and when. Points of contact and phone numbers should be included for equipment vendors, service providers, chemical suppliers, laboratories, and the media. Key information concerning the utility, such as the location of maps, schematics, and operations and maintenance (O&M) manuals, needs to be included in the ERP so that in a critical situation, replacement personnel could step in and operate the utility's facilities. Other critical items include relevant information on treatment processes and water storage as well as listings and locations of emergency equipment and spare parts.

On the personnel side, an ERP should define the chain of command during various types of emergencies as well as how the utility intends to coordinate response efforts with other governmental and private sector response agencies.

EMERGENCY NOTIFICATIONS

An important aspect of emergency response is emergency notification and determining which individuals or agencies need to be notified at each stage during the emergency. While much of this will be determined by local regulation and protocol, certain notifications seem to be commonly accepted throughout the nation.

Law Enforcement

The most universally agreed-on notification is local law enforcement. Receipt of a written or telephonic threat to a utility certainly requires notification of law enforcement as the threat itself may be a felony. The discovery of a security breech (e.g., a cut fence surrounding a water facility, or a broken hatch on a finished water storage tank) suggests the possibility that someone may

have tampered with the water and therefore suggests that the utility should contact local police. At the very least a cut fence or padlock represents an act of vandalism which should be documented by law enforcement.

Additionally, indications that someone may be attempting or threatening to attack a utility via a physical means or through the intentional release of a hazardous treatment chemical also suggest the need to notify law enforcement because the situation may pose a risk to people working at the utility or living in the surrounding community. In the event of a possible cyber attack on a water utility, the need to immediately notify the police may seem less compelling, but the intentional hacking into a utility SCADA or information system could result in a deterioration of water quality or identity theft of personnel or customer records, so law enforcement should be notified.

Law enforcement notification may also include the FBI, particularly because tampering with a public water supply is a federal offense. In most cases utilities can expect local law enforcement officials to make the decision to notify the FBI. However, in numerous briefings from FBI agents and Joint Terrorism Task Force members that this author has been involved with during training sessions across the nation, it has become clear that federal law enforcement officials want to be made aware of suspicious incidents involving public utilities. This can include direct phone calls from utilities themselves. The FBI has stated repeatedly that while an agent may not respond to each call, it is important that the bureau be made aware of these incidents because it tracks regional or national trends and could notice a pattern that indicates a more serious threat. The question of who notifies the FBI in these situations is something that utility officials should discuss with local law enforcement officials during the emergency planning phase.

Although notifying law enforcement as soon as an incident or threat occurs involving a public utility is a commonly accepted practice, the necessity of other notifications varies from state to state and utility to utility.

State Regulatory Agencies

A number of states have mandated that the state primacy or permitting agency be notified if there is reason to believe that an intentional or unintentional incident may have occurred involving a drinking water supply or waste water system. This is especially true if the event could potentially affect public health.

In Maryland, the Drinking Water Management section of the Code of Maryland Regulations (26.04.02.28.28) directs water suppliers to contract the approving authority when a reportable incident occurs during the operation of the water treatment and distribution system within one hour of the water supplier becoming aware of the incident. Reportable incidents include: “any occurrence in the operation, maintenance, repair, or extension of a water supply system or its appurtenances that causes a permanent or temporary change that may adversely affect the quality or quantity of water supplied to the users of the system.”

The Pennsylvania Department of Environmental Protection (PADEP) enforces the federal SDWA in that state. PADEP has notified all public water suppliers that they are required by state regulation (Title 25 Pa. Code Section 109.701) to phone the agency, day or night, within one hour of discovery of "any event that significantly increases the potential for drinking water contamination." These events include vandalism, tampering, contamination, or receipt of a threat. They also include suspected threats such as videotaping, photographing, or surveillance of facilities; individuals entering unauthorized areas; and inquiring phone calls. Following receipt of notification from a utility, PADEP will notify the Pennsylvania Emergency Management Agency and a number of other state and federal agencies. PADEP indicates that it will use the information received from the utility to assess the need for public notification and to discuss protective actions that may be necessary.

National Response Center

The National Response Center (NRC) is the national point of contact for reporting chemical, biological, and radiological spills into the environment that occur anywhere throughout the United States. This organization serves as the communications and operations center for the National Response Team and disseminates spill data to federal on-scene coordinators. Additionally, NRC notifies several federal agencies about a variety of types of incidents. Phoning the NRC is a way to alert the federal government, with just one phone call, that a situation is occurring that may potentially require federal assistance. While there is no regulatory mandate for a utility to contact the NRC if a threat, suspicion, or actual malevolent incident has occurred at a water or wastewater system, the USEPA recommends that utilities and other responders call the center. This one call could significantly decrease the time required for federal backup to arrive should the need for such assistance develop. Incidents can be reported to the NRC at 1-800-424-8802 or (202) 267-2675.

Neighboring Water Utilities

Another entity that a utility may want to contact if they become suspicious of the possibility of a malevolent act is neighboring water and wastewater utilities. This notification is useful for a number of reasons. For example, it is not out of the realm of possibility that a perpetrator who has phoned a threat to a water utility may have mistakenly contacted a different utility from the one whose facilities he may actually be targeting. Customers call the wrong utility frequently in areas served by more than one water or wastewater system. Or, this same perpetrator may have threatened other utilities in the area or attempted to breach their security. Sharing of information among utilities may reveal patterns or trends.

Finally, bringing neighboring utilities into the loop early facilitates their assistance should a threat turn out to be a real event. An early notification may reduce the preparation time required by the neighboring utility should their help be needed. The assistance will occur even more quickly and efficiently if mutual aid agreements for emergency response are already in place.

EMERGENCY OPERATIONAL RESPONSE

Operational Responses to Wastewater Contamination Threats

As discussed in chapter 3, The Threat to Wastewater Systems, contamination of wastewater systems can pose a significant risk to people, property, infrastructure, the wastewater treatment process, and the environment. Contaminants of concern include flammable and explosive substances, toxic chemicals, certain pathogens, and radionuclides. A number of practical steps can be taken to lessen the impact of contaminants once they appear in the wastewater collection or treatment system. As discussed, some of these may be taken at different stages of the threat process, starting from when a contamination event is merely suspected to the point where it is confirmed.

Monitor the entry point to the wastewater treatment plant. Influent channels, grit chambers, and primary clarifiers are locations where the visual, odor, and chemical characteristics of the raw wastewater can be inspected at ground or aboveground level for the first time. Changes in the color, sheen, consistency, or odor of the raw sewage at these sites can signal a problem. Visual inspections should be made hourly under routine circumstances and as frequently as necessary when utility operators suspect a contamination event.

Continuous chemical monitoring of the wastewater influent can be performed at the influent pump station wet well or at the facility's headworks. If this is not done on a continuous basis, chemical analyses should certainly be conducted in the event of a suspicion of contamination. Measurement of pH, ORP, conductivity, and temperature may provide an indication of contaminated sewage. Monitoring the combustible gas concentration in the headspace of the influent pump station wet well can indicate the presence of flammable or explosive substances.

Slow the flow of raw wastewater into the treatment plant to permit more extensive treatment. Divert suspect wastewater to backup storage basins, if available, to prevent damage to treatment plant microbes.

Isolate and shutdown redundant unit wastewater treatment processes. If redundant units are available, this will prevent contaminants from destroying the entire treatment process.

Pretreat the suspect wastewater as it enters the treatment works. This could include addition of powdered activated carbon, a strong oxidant such as chlorine or potassium permanganate, or a caustic substance to neutralize or precipitate toxic chemicals.

Increase the disinfectant dosage to reduce the passage of infectious pathogens through the treatment plant and into the environment.

Bypass the wastewater treatment plant and discharge untreated, contaminated wastewater directly to receiving waters in order to preserve treatment capabilities. (NOTE: This action should only be taken after consultation with the regulatory or permitting agency.)

Operational Responses to Drinking Water Contamination Threats

Increase chlorine. An operational response for suspected contamination incidents in drinking water systems is to increase chlorine residuals (Brosnan 1999). This could be effective for inactivating pathogens or oxidizing readily oxidizable chemical contaminants. However, if the utility only disinfects at the treatment plant, an increase in chlorine dosage may not be able to catch up with a slug of contaminant that has been accidentally or intentionally introduced somewhere within the distribution system. For utilities that practice booster chlorination within the distribution network, increasing chlorine levels within the distribution network may be more effective.

Isolate storage reservoirs or tanks that are suspected of being contaminated. This step is especially practical if a water system has enough built-in redundancy that a particular distribution system service zone receives water from more than one finished water source. If this is not the case, then storage facilities must be isolated more cautiously because this operational measure could deprive certain neighborhoods of water for fire protection.

Isolate portions of the distribution system that are believed to be contaminated. Practically speaking, the isolation of one pressure zone from a neighboring pressure zone is only reliable if the utility maintains a regular valve exercise program. Isolating areas within a single pressure zone in time to prevent the spread of a contaminant would be even more difficult because of the large number of valves that need to be closed in a short amount of time.

Flush portions of the distribution system that are suspected of being contaminated. Flushing multiple hydrants was used to clear a portion of the Pittsburgh water distribution system following the inadvertent injection of firefighting foam into the drinking water network by the fire department during a warehouse fire (States et al. 2008). Utilities trying to rid a distribution system of a dangerous contaminant need to make certain that the release of the contaminant to the environment doesn't create additional risk. This could be the case if the contaminant were a toxic volatile organic substance or a radionuclide.

ROLE OF UTILITY PERSONNEL IN RESPONDING TO EMERGENCIES

An ongoing debate in US water and wastewater utilities concerns the role of utility personnel in responding to emergencies at their utility. Of particular concern is response to threats and incidents of intentional, or even accidental, contamination in which the credibility of the incident, and the identity of the suspected contaminant, are unknown. Many utility operators and workers feel that this response should be handled completely by public safety or HazMat personnel.

HSPD 8, published in 2003, designates “public works staff”—including water and wastewater employees—as official first responders in the early stages of an incident affecting their facilities. It further states that these

individuals are responsible for the protection and preservation of life, property, and the environment. However, the directive does not go into detail on the specific duties that utility first responders are expected to assume.

The USEPA *Response Protocol Toolbox for Drinking Water* (USEPA 2004) and the USEPA *Wastewater Response Protocol Toolbox* (USEPA 2009) each present recommendations for utilities and other response agencies on how to deal with contamination situations. The Toolboxes suggest that, especially in the case of larger utilities, it is appropriate for the utility to take an active role in the initial investigation and operational response to a suspected contamination incident. However, the Toolboxes stop short of listing specific tasks that the utility should complete versus those that should be the responsibility of other agencies, such as public safety and state or federal response teams. The USEPA guidance documents indicate that these details must be worked out on a state or local basis. Some utilities, such as the Massachusetts Water Resources Authority in Boston, have been very proactive in developing a formal rapid response field team for contamination events that include in-house HazMat capabilities (Gregoire and Sparkas 2006).

The role that an individual water utility plays in an emergency affecting their facilities should be decided by utility officials, in concert with regulators and other responders, prior to an event. These roles should be described in the utility's ERP and need to be rehearsed during tabletop and field exercises. Formal training should not only include utility site characterization teams, but also management and other utility employees (Magnuson et al. 2008a). The extent of a utility's response effort will be dictated by the resources and training of utility personnel, and the availability of other resources in the region, as well as local and state regulations and standard operating procedures (SOPs).

In the case of a suspected contamination event in a drinking water or wastewater system, utilities may need to turn to local HazMat teams for assistance in response. HazMat teams are not necessarily well prepared to respond to a water emergency and many teams are not familiar with water sampling techniques. Utilities should coordinate and train with local HazMat teams prior to an incident or threat, and specifically discuss who will be responsible for which phases of the response (Magnuson et al. 2008b).

USEPA RESPONSE PROTOCOL TOOLBOXES

After 9/11, the water industry realized, as did other critical infrastructure sectors across the nation, that it could potentially become the target of malevolent acts. As discussed previously, a number of scenarios cause concern among water utilities including physical attacks (bombings, arson); cyber attacks; and the intentional release of hazardous treatment chemicals such as gaseous chlorine and ammonia. However, one of the scenarios of greatest concern is intentional contamination of drinking water or wastewater systems because this is the scenario that could affect the most people, in the shortest amount of time, with the most serious consequences.

With increased concern about the possibility of intentional contamination, the water industry looked to the federal government for guidance on how to deal with this threat. USEPA, the lead agency for protection of water systems, had not previously felt the need to develop this guidance. However, several major drinking water utilities in California had already begun this type of contingency planning. Rather than duplicate efforts, USEPA partnered with these utilities to prepare guidance applicable to the entire nation. A number of other water utility professionals, representatives from water industry organizations, regulators, and public health officials served as technical reviewers, producing a consensus document that represents many viewpoints (Magnuson et al. 2005).

The combined effort lasted two years and resulted in a 500-page document entitled *The Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents* (USEPA 2003–2004). The entire document is available on the USEPA Web site, www.epa.gov/watersecurity. Also available from the Web site are the *Water Security Handbook*, a 50-page condensed version of the Toolbox especially suitable for small utilities, and *Response Guidelines*, a collection of checklists and forms from the Response Protocol Toolbox that can be carried into the field during an emergency to help guide and document activities. A short, practical summary of Module 2 of the Toolbox, the “Contamination Threat Management Guide” was published in the AWWA periodical *Opflow* (Kufus 2006).

In 2009, USEPA published *Wastewater Response Protocol Toolbox: Planning for and Responding to Wastewater Contamination Threats and Incidents*, a guidance document, similar to the drinking water version, dealing with both intentional and accidental contamination events in wastewater systems. As with the drinking water guidance documents, the wastewater document can also be downloaded from the USEPA water security Web site.

The formats for the drinking water and wastewater contamination documents are similar. Each is divided into six modules.

Module 1 (Water-Utility Planning Guide) provides an overview of contamination threats. It also discusses the concept of due diligence and lists suggestions for utilities planning their responses to contamination threats and incidents.

Module 2 (Contamination Threat Management Guide) is the hub of both Toolboxes because it addresses the overall management of a contamination threat. Threat management involves evaluation of the threat and making decisions regarding appropriate response actions. Evaluation of the threat is a three-step process in which responsible officials make determinations as to whether a contamination threat is *possible*, *credible*, or *confirmed*. Each of these successive decisions requires a greater amount of evidence and entails more significant response actions. For example, USEPA recommends that the public be notified about the contamination incident once officials have determined that the threat has reached the credible stage.

Figure 13-1 represents the threat management decision process that USEPA recommends to drinking water utilities when evaluating a drinking water contamination threat. A similar decision tree appears in the *Wastewater Response Protocol Toolbox*. The threat management decision tree describes the sequence of events leading from the initial decision that the contamination threat is possible to the point where officials determine, based on analytical data or a preponderance of other evidence, that the threat is actually confirmed. The recommended timeline appears on the left border of the matrix.

If it can be done, USEPA recommends that the initial incident commander in charge of the event make the decision as to whether the threat is possible within one hour of becoming aware of the threat. USEPA further recommends that officials make the decision that the threat is credible within six to eight hours following the initial determination that the threat is possible. The reason for the short time frame is the imminent significant risk to public health and property posed by a contamination event in either a drinking water or wastewater system. As indicated in the decision tree, the determination that a threat is confirmed may require more time because it will probably require analytical data.

Module 3 (Site Characterization and Sampling Guide) presents procedures for safely investigating the site of suspected contamination, or downstream sites that may have subsequently been affected by the contaminant. Specifically, the module describes the qualifications of the individuals that should be dispatched to the site, as well as steps taken to ensure the safety of the site characterization team. This section describes protocols for performing a field safety screening check, conducting rapid testing of water samples in the field, and collecting samples to be sent to reference laboratories for definitive analysis. Module 3 also provides various forms that can be used to document the site investigation and describes a model sample collection kit.

Module 4 (Analytical Guide) is of primary interest to laboratory personnel who will be analyzing samples to determine the identity and quantity of what may be potentially hazardous contaminants in drinking water or wastewater samples. This section is also important for utility personnel planning for the analysis of emergency samples prior to an event. Module 4 offers a framework for analyzing samples containing unknowns. Just as utilities can use the guidance in the *Response Protocol Toolboxes* to develop their ERPs, laboratories can use the analytical approach in this module when developing their individual laboratory plans. Module 4 deals with chemical, microbial and radiochemical contaminants.

Module 5 (Public Health Response Guide) deals with the public health response measures that can be used to minimize public exposure to contaminated drinking water or wastewater. It discusses the important issue of who is responsible for making the decision to initiate public health response actions, and which roles public health agencies, utilities, and regulatory agencies play. The module also considers specific public health responses, such as when it

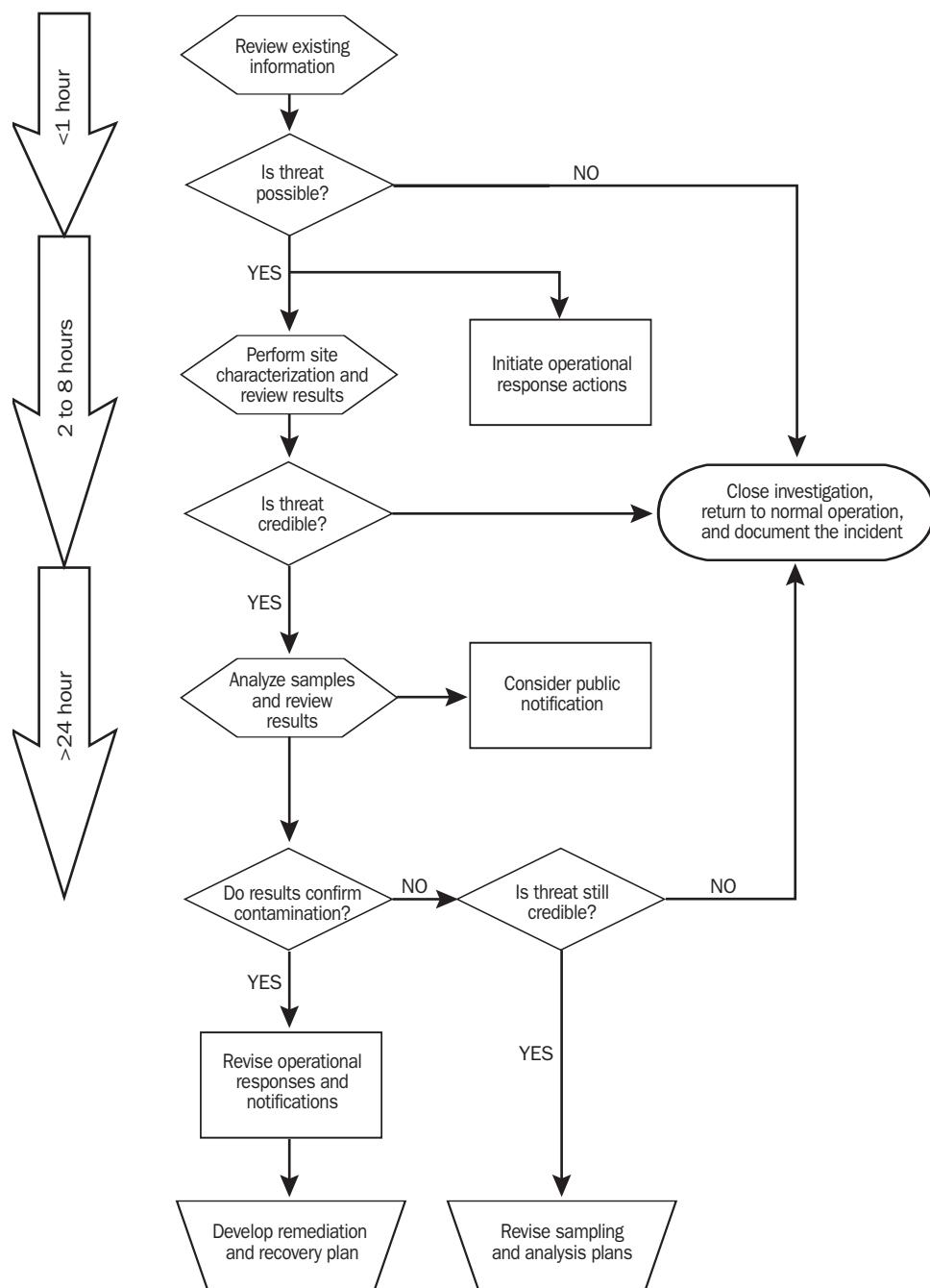


Figure 13-1. Threat management decision tree

may be necessary to issue “Do Not Use,” “Do Not Drink,” or “Boil Water” advisories in the event of a drinking water contamination.

Module 6 (Remediation and Recovery Guide) provides general guidance for water utilities and other organizations that would be responsible for decontamination and rehabilitation efforts aimed at bringing a drinking water or wastewater system back into service following a contamination event. The guidance in this module is based on USEPA’s extensive experience with Superfund projects.

In general, the Response Protocol Toolboxes offer specific guidance on numerous emergency response issues, including whom to notify, actions to take, how to conduct a threat evaluation, how to collect and ship samples, how to analyze samples, and how to recover from an actual contamination incident. However, the Response Protocol Toolboxes do not attempt to answer questions concerning *who* will be involved in the various stages of response, such as who will respond, who will sample, who will conduct analyses, who will make public health decisions, and who will manage remediation and recovery efforts. These questions are best answered by utility and local or state authorities who have direct knowledge of local and regional capabilities for responding to contamination threats.

USEPA emphasizes that the recommendations in the Toolboxes are not meant to be prescriptive. Rather they are intended to be broad guidance that utilities and emergency responders can adapt to their own local situations. State and local regulations, the training and equipment resources available in a particular area, and agreements that may already be in place between utilities, regulatory agencies, health agencies, and other organizations in a particular city or county may influence the degree to which USEPA’s recommendations are adopted. USEPA also emphasizes that there is no regulatory requirement that mandates that utilities follow the guidance in the Toolboxes. These documents are simply offered as optional tools. Finally, USEPA recommends that the Toolboxes not be used as a references during an emergency because the documents are simply too large to be useful during the course of an actual response. Rather, the guidance documents should be consulted when a utility is updating its own ERP. USEPA encourages utilities to use any of the suggestions offered in the Toolboxes, and cut and paste any of the protocols or forms provided in the documents to fit their own ERPs.

REFERENCES

- American Water Works Association (AWWA). 2001a. Manual M19, *Emergency Planning for Water Utilities*. Denver, Colo.: AWWA.
- AWWA. 2001b. *Security Analysis and Response for Water Utilities*. Denver, Colo.: AWWA.
- Brosnan, T., ed. 1999. *Early Warning Monitoring to Detect Hazardous Events in Water Supplies*. Risk Science Institute Workshop Report. Washington, D.C.: International Life Sciences Institute.
- Gregoire, J.J. and J.A. Sparkas. 2006. Sampling From a Distance Took In-House Insight. *Opflow*, 32(10):28.
- Kufus, M. 2006. Applying the Threat Response Toolbox. *Opflow*, 32(2):10.

- Magnuson, M.L., S.C. Allgeier, B. Koch, R. DeLeon, and R. Hunsinger. 2005. Responding to Water Contamination Threats. *Environ. Sci. & Technol.*, 153A. Washington, D.C.
- Magnuson, M.L., E. Hedrick, E. Savage, J. Swertfeger, and M. Tyree. 2008a. Site Characterization Training and Drills for Utility Personnel Responding to Water Contamination Emergencies. *Proc. 2008 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Magnuson, M.L., S. Minamyer, and M.S. Rees. 2008b. Is Your Local HazMat Team Prepared to Respond During a Water Contamination Emergency? *Proc. 2008 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- States, S., J. Carroll, G. Cyprych, K. Hayes, J. Kuchta, M. Little, A. Pyle, M. Stoner, C. Westbrook, and L. Casson. 2008. An Accidental Contamination Event in the Pittsburgh Water Distribution System (A Case Study). *Proc. 2008 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- US Environmental Protection Agency (USEPA). 2003. *Large Water System Emergency Response Guide Plan Outline: Guidance to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*. Washington, D.C.: USEPA. www.epa.gov/safewater/watersecurity/pubs/erp-long-outline.pdf.
- USEPA. 2003–2004. *Response Protocol Toolbox: Planning for and Responding to Contamination Threats to Drinking Water Systems*. Washington, D.C.: USEPA. www.epa.gov/safewater/watersecurity/pubs/guide_response_overview.pdf.
- USEPA. 2004. *Emergency Response Plan Guidance for Small and Medium Community Water Systems to Comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*. Washington, D.C.: USEPA. www.epa.gov/safewater/watersecurity/pubs/small_medium_ERP_guidance040704.pdf.
- USEPA. 2009. *Wastewater Response Protocol Toolbox: Planning for and Responding to Wastewater Contamination Threats and Incidents*. Washington, D.C.: USEPA. www.epa.gov/safewater/watersecurity.
- Whitler, J. 2007. Emergency Preparedness for Drinking Water and Wastewater Systems. *Jour. AWWA*, 99(3):36.

EMERGENCY MANAGEMENT OF DRINKING WATER AND WASTEWATER INCIDENTS

Over the years, a recurring set of problems has been encountered in the management of large-scale emergency situations. A single incident may affect multiple infrastructures and community services. The scale of an incident may exceed the capacity of local, state, and federal responders. Response agencies may have different organizational structures. And, incompatible communications and terminology differences may exist among the various agencies.

Homeland Security Presidential Directive 5 (HSPD 5), Management of Domestic Incidents, was issued by the federal government in February 2003 to address these problems and improve the overall response to emergencies resulting from both manmade and natural causes. The goals of HSPD 5 included the development of a comprehensive national approach for incident management that encompasses all of the relevant phases: prevention, preparedness, response, and recovery. The directive is also intended to better coordinate the efforts of all responding agencies within both the public and private sectors and to integrate the crisis and consequence management components of emergency response that traditionally have been treated separately.

More specifically, HSPD 5 appointed the secretary of the DHS to be the principal federal official (PFO) for domestic incident management. In practice, the DHS secretary is expected to appoint a representative to act as PFO for specific emergencies. During the catastrophic hurricanes of 2005, two senior Coast Guard officers were directed to lead the federal response.

Admiral Thad Allen was appointed PFO for Hurricane Katrina, and Rear Admiral Larry Hereth was appointed PFO for Hurricane Rita. HSPD 5 also directed the DHS secretary to develop two new initiatives: the National Incident Management System (NIMS) and the National Response Plan (NRP), now known as the National Response Framework (NRF).

NATIONAL INCIDENT MANAGEMENT SYSTEM

NIMS is a standardized management plan that provides a core set of concepts for incident command and multi-agency coordination during incident response. In the words of former DHS Secretary Tom Ridge, the aim of NIMS is to ensure “One mission, one team, one fight” through establishment of a nationwide template to enable federal, state, and local governments to better prepare for, prevent, respond to, and recover from domestic incidents regardless of complexity or cause. This approach is applicable to natural disasters, terrorism, acts of war, major accidents, and other emergencies, including those affecting public utilities. The goal is to establish common principles, terminology, organizational structures, and procedures that all responders can follow during an emergency to better coordinate response actions. NIMS is based on standard emergency management systems, such as the Incident Command System (ICS), which is already used in most jurisdictions throughout the United States. The five focus areas in the NIMS are

- preparedness,
- communications and information management,
- resource management,
- command and management, and
- ongoing maintenance and management.

Adoption of NIMS is mandatory for federal agencies. NIMS is also essentially mandatory for state and local government agencies because adoption of NIMS is a precondition for receipt of federal preparedness grants and contracts, although not for disaster relief. The program is described in detail in *National Incident Management System*, originally published in March 2004, revised in May 2006 based on lessons learned during Hurricane Katrina, and again in December 2008 (DHS 2008). Specific information on NIMS compliance requirements can be found at www.fema.gov/emergency/nims/compliance/2007.shtml. Free NIMS training is available online at <http://training.fema.gov/emiweb/is/700a.asp>.

NATIONAL RESPONSE PLAN and NATIONAL RESPONSE FRAMEWORK

The NRP went into effect in April 2005 in an effort to integrate all federal government prevention, response, and recovery plans for management of domestic incidents into a single, all-disciplines, all-hazards plan. The NRP outlined how federal agencies should work together and how the federal

government should coordinate with state, local, and tribal governments, and the private sector during emergencies. All types of emergencies can be dealt with using the NRP including natural disasters, hazardous material events, pandemics, and terrorism. The NRP superseded the previously applicable Federal Response Plan and is intended to help deal with the broader national impact of domestic incidents.

The NRP uses NIMS as a foundation and incorporates NIMS concepts, principles, and processes, and applies them to a national structure. The basic premise of the NRP is that all incident response begins at the local level, and incidents should be handled at the lowest geographic, organizational, and jurisdictional level possible. The top priority of incident management is to save lives and protect the health and safety of the public, responders, and recovery workers.

The NRP defines certain roles for elements of DHS. For example, the Homeland Security Operations Center was established as the primary national-level hub for communications and information pertaining to domestic incident management. This center was later renamed the National Operations Center. Additionally, the Joint Field Office is established as the focal point for coordination of federal support to on-scene management efforts during a major emergency. It serves as the coordination point for the federal Joint Operations Center, which is typically under the control of the FBI, and the Disaster Field Office, which has normally focused on response and recovery efforts for agencies such as FEMA. This consolidation is consistent with the goal of integrating the crisis and consequence phases of emergency management.

Following Hurricane Katrina in late summer 2005, President George W. Bush ordered the NRP to be reviewed and updated to incorporate lessons learned from this disaster. In March 2008, the NRF was released and replaced the NRP. By adopting the term *framework* in the title, DHS believes the document is now more accurately aligned with its intended purpose: a guide that details how the nation conducts all-hazards response from the smallest incident to the largest catastrophe.

The NRF differs from the original NRP in several aspects. First, the NRF reflects lessons learned from disasters, such as Hurricane Katrina, that occurred after release of the NRP. Secondly, the NRF broadens the focus from a purely federal plan to one that encompasses all levels of government as well as nongovernmental agencies. Thirdly, the NRF methodically describes the who, what, and how of emergency preparedness and response. The NRF also identifies special circumstances where the federal government exercises a larger role, such as incidents where federal interests are involved and catastrophic incidents where a state would require significant support.

The NRF can be downloaded from www.fema.gov/nrf. The download consists of the NRF base document, Support Function Annexes, and Support Annexes. The annexes are individual documents designed to provide concepts of operations, procedures, and structures for use by all partners responding under the NRF. At this point, the former NRP's Incident Annexes remain in effect until superseded.

Online NRF training is provided in FEMA Course IS 800B, “National Response Framework,” which is available at the FEMA website www.fema.gov.

INCIDENT COMMAND SYSTEM (ICS)

Significant emergency situations demand so many resources and skills that no single local, state, or federal agency could possibly provide them all. The ICS has been used to coordinate the activities of multiple response agencies in emergency situations throughout the United States for the past 30 years. Developed in the 1970s in response to wildfires in California that caused a number of deaths and millions of dollars in damage, the purpose of the ICS is to ensure effective incident management. After the wildfires, local, state, and federal fire authorities collaborated to form Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE), which looked at the response to the fires and determined that poor incident management, rather than a lack of resources, was to blame for the extensive negative consequences. ICS was developed to correct this situation. The ICS structure is similar to the command and general staff structure that has been used for decades in the US military to coordinate the activities of army battalions, brigades, and divisions. Although NIMS is a recent development, it has not replaced the ICS. Rather, NIMS requires that on-scene emergency management be performed using ICS.

While police, fire, and other emergency responders are well versed in the use of ICS, this is a relatively new concept for water and wastewater utilities. Should an accidental or intentional emergency situation occur that significantly affects a drinking water or wastewater system, ICS will be employed. Therefore, utility personnel need to become familiar with this approach.

ICS is an emergency management system designed to integrate personnel, equipment, facilities, procedures, and communications to enhance incident management. ICS establishes common terminology, procedures, and organizational structure in addition to consistent position titles and common incident facilities to be used by responders at all levels of government as well as in the private sector. ICS is adaptable to any type of emergency anywhere throughout the country. It is modular in organization and scalable to the magnitude of the emergency. ICS also specifies an orderly chain of command within the ranks of emergency organizations with each manager responsible for only three to seven subordinates—a manageable span of control—and each responder reporting to only one supervisor, which guarantees unity of command.

Every emergency, regardless of its nature, requires a certain set of functions to be performed. The incident command structure is organized to accomplish those functions, as shown in Figure 14-1. However, ICS is not just an organizational chart, but rather a management system. Because the system can be structured to fit the emergency, only functions or positions that are needed to manage a specific incident need to be filled.

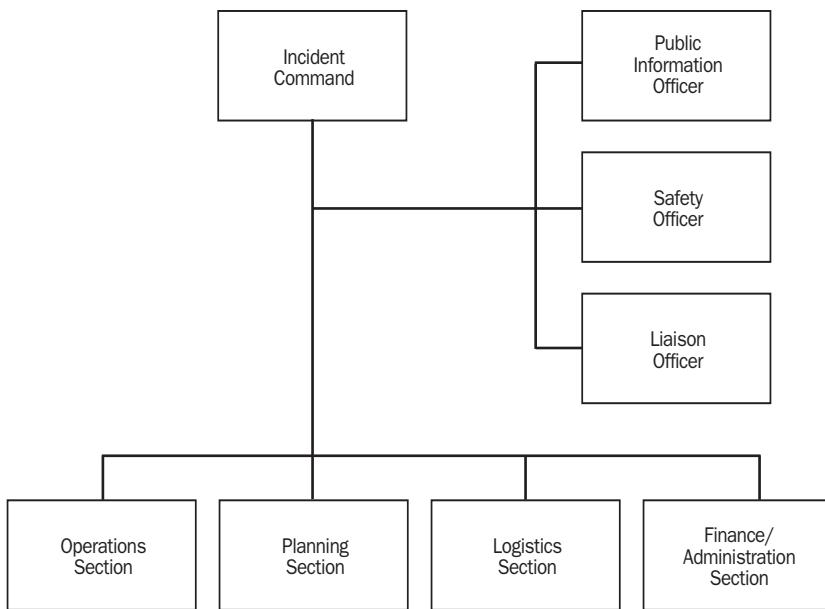


Figure 14-1. Basic ICS structure

The command section is responsible for overall management of the situation and includes the *incident commander* and *command staff*: *public information officer*, *safety officer*, *liaison officer*, and if needed, a *legal advisor* and *medical advisor*. The agency with primary jurisdictional authority over the incident normally designates the incident commander. Incident command functions begin with the development of incident objectives. These provide the basis for the incident action plan (IAP), which in turn directs the response operations. Command functions also include approval of the IAP and of all requests pertaining to the ordering and release of resources.

Within the scope of his or her authority, the incident commander establishes incident objectives and determines strategies, resources, and the appropriate ICS structure needed to meet those objectives. The ultimate responsibility for the resolution of an incident, however, remains with the chief elected official, chief executive officer, or agency administrator. Therefore, these individuals must remain active participants, supporters, supervisors, and evaluators of the incident commander, but should avoid micromanaging the response.

The command staff functions as advisors to the incident commander on various aspects of the operation. The public information officer advises the incident command on all public information matters related to management of the incident, including media and public inquiries, and emergency public information and advisories. The safety officer monitors safety conditions, develops safety protocols, and advises the incident commander on issues regarding incident safety. The liaison officer serves as the primary

contact for agencies supporting the response. If a utility is not an integral part of the ICS structure during an emergency, the liaison officer can serve as a point of contact to help the utility tap into the flow of information from incident command.

The general staff of an ICS includes the chiefs of the operations, logistics, planning, and finance and administration sections. These section chiefs need to be headquartered at the incident command post (ICP) and continually interact with each other. The general staff develops estimates of the situation and recommends courses of action for consideration by the incident commander. The planning section prepares the IAP to meet the incident objectives specified by the command. Planning also collects, analyzes, and disseminates information and intelligence, and maintains resource status and incident documentation.

The operations section develops tactical objectives, conducts tactical operations to carry out the plan, and directs all tactical resources. Because most of the tactical fieldwork and hazardous activities are performed by this section, most of the resources are typically assigned here. The logistics section provides support, resources, and all services needed to meet operational objectives. This includes personnel, equipment, supplies, communications, food, medical services, facilities, and transportation. This section also develops portions of the IAP and forwards them to the planning section. The finance and administration section monitors costs, provides accounting and procurement services, and processes claims for accidents and injuries. Much of the documentation kept by this unit is necessary for agencies seeking reimbursement following the emergency.

Every incident must have either either a verbal or written IAP. The incident commander can develop the IAP if no planning section has been established. The plan provides direction for actions to be taken during the specific operational period that the plan covers. An operational period can be of various lengths but usually does not exceed 24 hours. At their simplest, IAPs address the following four questions:

- What needs to be done?
- Who is going to accomplish which tasks?
- How will communications be carried out?
- What should be done if someone is hurt?

There are two approaches to incident command, the single command and the unified command. Single command is used when an incident occurs within a single jurisdiction and minimal functional overlap exists among responding agencies. In this situation, the appropriate jurisdictional authority designates a single incident commander who is solely responsible, within the confines of his or her authority, for establishing incident management objectives and strategies. The incident commander is directly responsible for ensuring that all functional area activities are directed toward accomplishment of these objectives.

The unified command approach is typically followed when an incident involves more than one jurisdiction or response by multiple agencies. This approach helps organizations with different legal, geographic, and functional responsibilities interact effectively. Under the unified command approach, all agencies with jurisdictional or functional responsibility participate in the command structure. The exact composition of the structure depends on the location and type of incident, jurisdictions involved, and functional agencies involved. Individuals designated by their jurisdictional authorities represent their authorities and agencies and use a collaborative approach to manage the crisis. The command group must work together to establish a common set of incident objectives and strategies, and ensure execution of integrated operations. Unified command works best when participating members

- locate together at a central incident command post;
- keep each other informed of specific requirements;
- establish consolidated incident objectives, priorities, and strategies;
- establish a single system for ordering resources;
- develop a consolidated IAP (written or oral) and update it at regular intervals; and
- establish procedures for joint decision making.

The unified command approach changes no other aspect of ICS other than allowing all agencies with a responsibility in the incident to participate in the decision-making process.

Unified command is not a new concept. For years, the US military has used a similar approach to integrate different military services (e.g., Army, Navy, Air Force) in joint operations.

FEMA offers several online courses on ICS. These include ICS-100, *Introduction to the Incident Command System*; ICS-100.PW, *Introduction to the Incident Command System for Public Works Personnel*; and ICS-200, *Basic Incident Command System*. In addition to the Web-based courses, FEMA's Emergency Management Institute offers ICS-300, *Intermediate Incident Command*; and ICS-400, *Advanced Incident Command*, which are several day-long courses offered at various training locations. Information on ICS training is available on FEMA's Web site, www.training.fema.gov/emiweb/IS/ICSResource/index.htm.

EMERGENCY OPERATIONS CENTER

The emergency operations center (EOC) is the physical location or headquarters in which the coordination of information and resources to support incident management takes place. The EOC is the support arm of the response effort and is typically operated by a community or jurisdiction (city, county, region, state) as part of its emergency preparedness program. The EOC should be housed in a secure location and equipped with food, water, emergency power generation equipment, and other basic amenities so that it will be self-sustaining during extreme emergencies. An alternate EOC should

be available if the main location is not accessible because of the nature of the emergency. The EOC may be a permanent organization and facility or may be established to meet temporary, short-term needs. The physical size, staffing, and equipping of an EOC depends on the size of the jurisdiction being served, resources available, and the anticipated incident management workload. However, regardless of the size or complexity of an EOC, it should accomplish the following functions:

- coordination
- communications
- resource dispatching and tracking
- information collection, analysis, and dissemination

A standing EOC is typically located in a central, permanently established facility. Consistent with the guidelines outlined in NIMS, the EOC is normally organized by emergency support function (ESF)(e.g., ESF #3, public works and engineering; ESF #4, firefighting). EOC staff usually includes government officials, agency department heads, and volunteer agencies.

New York City recently opened a new Office of Emergency Management Headquarters and Emergency Operations Center in downtown Brooklyn (*Government Technology* 2006). The \$50 million facility was funded by money provided to New York City in the weeks following 9/11. The 65,000 ft² building contains a 130-agency EOC that is staffed 24 hours per day, and serves as the central point of coordination for emergencies and special events in New York City. The new EOC is backed up by an already existing EOC and was built to replace the former facility, located at 7 World Trade Center, which was destroyed by the terrorist attacks.

In addition to the ICS courses, FEMA offers an online EOC course entitled IS-275, *The EOC's Role in Community Preparedness, Response, and Recovery*. Information on this course is also available at the previously mentioned FEMA Web site.

Interaction of ICP and EOC

The ICP is where the single command or unified command personnel are physically located and from which they oversee all incident operations. Every incident must have some form of ICP, which is normally situated near the incident site, possibly in a vehicle, trailer, tent, or building such as a school. The actual location may change during the course of an emergency. The ICP focuses on the tactical on-scene response activities because direct tactical and operational responsibility for incident management rests with incident command.

The EOC is most often located in a central, permanently established facility. The EOC focuses on coordination of information and resources to support on-scene management of the incident, which occurs at the ICP. Elected officials and top management, such as utility directors, will usually gather at the EOC. The ICP may perform an EOC function in smaller-scale incidents or during the initial phase of response to large, more complex

events. While the EOC is basically responsible for community-wide resource management, eventually the EOC may become the major tactical headquarters of the response effort. When not collocated, the EOC and the ICP must be in constant communication with each other. EOCs at all levels of government must be capable of communicating with each other during incidents.

DEPARTMENTAL OPERATIONS CENTER

Individual agencies involved in response to a situation typically set up their own departmental operations centers (DOC) within the physical structure of their own organizations. For example, the water department may set up a DOC in its downtown headquarters building or at a treatment plant. The DOC is where key water department personnel assemble during an emergency to coordinate the response of that particular organization. The DOC should be located at a site that would be expected to be accessible during most anticipated emergencies. As in the case of a city, county, or state EOC, an alternate location should be designated in case the primary DOC site is not available during a particular incident.

The DOC for a water or wastewater utility should contain copies of the utility's ERP along with system drawings, O&M manuals, and other key documents that may be needed during a crisis. The DOC should also be equipped with all of the types of communications equipment that may be used to communicate within the agency or with other organizations during the emergency. The personnel manning the DOC focus their efforts on internal agency emergency response. Agency representatives will likely be stationed at the ICP and EOC as well, and they will need to maintain communications with the DOC.

CONCLUSIONS

With the exception of utilities located in parts of the country frequently threatened by natural disasters such as hurricanes or tornadoes, drinking water and wastewater personnel are often relatively unfamiliar with standard concepts of emergency management, such as the ICS. Should an emergency occur that interferes with the ability of a utility to provide drinking water or wastewater services, utility personnel will be part of the response, and thus must understand basic emergency management practices. In the event of a terrorism incident, or other significant emergency, a utility will need to coordinate with a number of other response agencies. These agencies operate according to the guidelines spelled out in the NIMS, the NRF, and the ICS. Additionally, water personnel may play an active role in single or unified commands or in EOCs.

Drinking water and wastewater personnel should become familiar with emergency management concepts and are strongly encouraged to incorporate NIMS and ICS approaches into their utility's ERP. A good training resource

for NIMS, NRP, and ICS are the free, online courses offered by FEMA on its Web site, <http://training.fema.gov/EMIWeb>.

REFERENCES

- Department of Homeland Security (DHS). 2008. *The National Incident Management System*. www.fema.gov/emergency/nims/. Washington, D.C.
- DHS. 2008. *The National Response Framework*. www.fema.gov/nrf/. Washington, D.C.
- DHS Federal Emergency Management Agency (FEMA). Emergency Management Institute (website for ICS and other emergency management independent study courses and resources). Washington, D.C. www.training.fema.gov/EMIWeb/EMI-Courses/EMICourse.asp.
- Government Technology*. 2006. State-of-the-Art Emergency Management Headquarters Opens in Brooklyn. *Government Technology*. December 5. [www.govtech.net/news/story IPP](http://www.govtech.net/news/story/IPP).

ANALYTICAL RESPONSE TO WATER CONTAMINATION THREATS

Should a drinking water or wastewater utility suspect that a contaminant has intentionally or unintentionally entered the water system, part of its response activities would be to investigate to determine whether this indeed was the case. The investigation may include collecting and analyzing samples for the presence of unknown or suspected contaminants. As suggested in USEPA's Response Protocol Toolboxes for Drinking Water (USEPA 2004) and for Wastewater (USEPA 2009), and USEPA's Sampling Guidance for Unknown Contaminants in Drinking Water (USEPA 2008), the initial analytical effort may consist of rapid field testing of the suspect water at the site of suspected contamination by a site characterization team (SCT). Initial testing should include a combination of field analytical techniques, the sophistication of which will vary with the level of training and resources of the field response team. Following preliminary field analysis, samples should be collected by the site characterization team and, if the situation dictates, be transported to one or more laboratories for definitive analysis. Some utilities, such as the Philadelphia Water Department, have developed detailed laboratory ERPs for this type of event (Gaffney and Burlingame 2009).

This chapter describes some of the analytical techniques that can be used for field safety screening and rapid field testing of water by the site characterization team. Discussion follows regarding the laboratory resources currently available for more detailed analysis and some of the resources that are in development.

FIELD SAFETY SCREENING

As described in Module 3 of the Response Protocol Toolboxes, USEPA recommends that the site characterization team conduct a field safety screening, first at the perimeter of the suspected site of contamination and then at the site itself. The screening helps the response team evaluate whether the environment is safe. This initial evaluation then informs the incident commander's decision as to whether the team can proceed with field testing and sampling of the suspect water. For example, the detection of hazardous substances in the environment would likely prompt the incident commander to recall a utility team and replace it with a HazMat team.

At a minimum, USEPA recommends that the SCT screen for excessive levels of radioactivity at the perimeter and again in the immediate vicinity of the investigation site. This screening can be conducted using commonly available radiation monitoring equipment such as a Geiger–Müller (G–M) counter.

Expanded field safety screening can be conducted for other hazards, such as volatile chemicals, weaponized chemicals, and biological contaminants. However, USEPA stresses that equipment for this testing should only be used by individuals trained in its use, and the performance of the equipment should be validated.

For instance, screening of the air for combustible gases, toxic gases, and VOCs in the area of the investigation site could be accomplished using commercially available gas detectors (sniffer-type devices). The MSA Orion Multi-Gas Detector^{*} is a handheld unit that detects combustible (lower explosive limit [LEL]) gases, oxygen, carbon monoxide, and hydrogen sulfide in the air. RAE Systems Inc.[†] manufactures the MultiRAE Plus One to Five Gas Monitor with VOC Detection (model PGM-50/5P), which can be used for field safety screening of the air. The instrument has sensing capability for four gases. These include oxygen and combustible gases LEL, as well as two others from the following list: carbon monoxide, hydrogen sulfide, sulfur dioxide, nitric oxide, nitrogen dioxide, chlorine, hydrogen cyanide, ammonia, and phosphine. The instrument also contains a photoionization detector (PID) that can screen for a variety of VOCs. While the VOC detector can provide an overall estimate of the concentration of VOCs, it can't identify specific chemicals. The detection range for VOCs is 0 to 2,000 ppm with a resolution of 0.1 ppm in the 0 to 200 ppm range. This device can be used as a personal monitor, a hand-held sniffer, or as a continuous-operation area monitor.

The use of a sampling probe can facilitate use of these instruments in confined spaces without requiring team members to enter the area. This is especially useful for teams investigating the possibility of combustible or toxic fumes in manholes or catch basins during the investigation of wastewater contamination events.

* MSA, Pittsburgh, Pa.

† RAE Systems Inc., San Jose, Calif.

Some of the equipment described in the next section on rapid field testing of water can also be used for screening the air or environmental surfaces for hazardous substances. This includes field portable immunoassay, PCR, and GC–MS devices.

RAPID FIELD TESTING OF WATER

As the name indicates, rapid field testing of water is intended to be conducted in a short amount of time at a field site. The location could be the suspected site of contamination or a downstream site where the contaminant is believed to have spread through the water system. Because this initial analysis is conducted rapidly under field conditions, the analytical results obtained must be considered preliminary and presumptive. A rapid field test is intended to detect

- hazardous conditions (e.g., elevated radiation levels) that would require that additional site processing be conducted by more specialized responders such as HazMat teams,
- indicators that there has been a significant change in the chemical state of the water (e.g., changes in pH, TOC, chlorine content, conductivity etc.), which may suggest the presence of contaminants, and
- preliminary indications of the identity of specific contaminants (e.g., free cyanide).

Subsequent confirmatory analyses need to be conducted in a reference laboratory to validate the results of field testing. The underlying goal of rapid field testing is to produce results quickly and accurately enough to help response officials make timely evaluations of the credibility of a threat and initiate response actions that reduce the impact of the contamination event and help protect the public, utility workers, infrastructure, private property, and the environment. The presumption is that results of definitive analyses in a reference lab would typically not be available soon enough to help inform evaluations or operational response decisions that would need to be made within hours after discovery of a threat. The greatest challenge of rapid field testing is to produce accurate results that don't lead to false-positive or false-negative conclusions concerning the presence and identity of contaminants (Magnuson et al. 2005).

A number of commercially available rapid analytical techniques have been evaluated for use in suspected cases of contamination of drinking water supplies (States et al. 2003, 2004). These technologies are briefly described in this chapter and in Table 15-1. While some work has been conducted to determine the applicability of these methods for use with drinking water samples, little work has been reported validating the applicability of these technologies for wastewater samples. Matrix effects in the various types of wastewater samples, ranging from untreated wastewater through treated POTW effluent, may preclude the use of some of these techniques.

The capabilities and limitations of some rapid analytical methods for drinking water investigations are described in the following sections, along with potential applications for wastewater investigations. Additional information on a variety of commercially available technologies can be found in USEPA's Security Product Guide at www.epa.gov/safewater/security/guide/index.html. Verification reports for field instruments that have undergone independent testing through USEPA's ETV program or TTEP are available at www.epa.gov/etv/homeland/index.html.

Core Testing

Module 3 of USEPA's Drinking Water Response Protocol Toolbox (USEPA 2003) and Wastewater Toolbox (USEPA 2009) recommends procedures to be used during the site characterization process when responding to the suspicion of contamination. One recommendation is that the site characterization team conducts a rapid assay of the suspect water in the field using at least five basic core tests. These include screening for radiation and cyanide, as well as measurement of chlorine concentration, pH, and conductivity. Cyanide testing is recommended because a number of easy-to-use field tests are commercially available that have been validated by USEPA's ETV program. Cyanide screening is also recommended because over the years, cyanide has been one of the most commonly threatened intentional contaminants for drinking water. Measurement of chlorine, pH, and conductivity is prescribed because changes in one of or more of these basic chemical parameters could indicate that a foreign substance had either intentionally or accidentally been added to the water. Measurement of these parameters in the field is similar to the concept of continuous, online measurement of basic parameters in a drinking water CWS in that these parameters act as indicators or surrogates for the presence of chemical, and perhaps even biological, contaminants. Continuous monitoring was discussed in chapter 12 of this handbook. Significant changes in the values for these parameters indicate a chemical change of state. A variety of portable devices for core testing are available from a number of vendors. Chlorine (free or total) is easily measured using colorimetric methods. Cyanide can be screened for using either colorimetric methods or an ion selective electrode. Conductivity and pH can be measured with ion selective electrodes.

Screening for Radiation

In the Response Protocol Toolboxes, USEPA recommends that during the site characterization process, the response team screens the water for excess radiation that would suggest the presence of radionuclides. The most common types of radiation are alpha, beta, and gamma. While detection of excess radiation in any of these categories would not identify the specific radioactive contaminant in the water, the presence of excess radiation indicates to responders that the site is potentially hazardous and should be investigated by a team equipped and trained to deal with radioactive hazards.

Measurement of radiation in water samples in the field is more complicated than measurement in air. The highly penetrating gamma radiation

can be detected in water samples using a sodium iodide probe. However, alpha and beta emissions are more difficult to measure, for example, with a pancake G-M probe, because short-range radiation is easily blocked by the water itself before it reaches the detector. Additionally, water surfaces are not smooth and can therefore interfere with the effectiveness of gas-flow proportional counters designed to measure alpha and beta radiation from smooth surfaces. Alpha and beta radiation in water samples is more accurately measured in the laboratory using a large, sensitive scintillation counter.

Several manufacturers provide field radiation detectors. For example, Ludlum Measurements, Inc.* sells the battery-operated Model 2241-3RK Response Kit, which costs approximately \$2,200, for alpha, beta, and gamma surveys in the field. This instrument contains four detector setups including an alpha–beta–gamma pancake G–M detector, and a sodium iodide gamma scintillator. The Hach Corporation† offers the Radalert 50 Handheld Nuclear Radiation Monitor (\$288) for monitoring area or perimeter background radiation. The device measures alpha, beta, gamma, and x-radiation using a G–M detector. Hach also sells the Inspector Alert Handheld Nuclear Radiation Monitor (\$565), which measures alpha, beta, gamma, and x-radiation in the field using a two-inch pancake G–M detector.

Acute Toxicity Screening

Acute toxicity screening tests are broad spectrum assays designed to indicate the presence of acutely toxic substance such as industrial chemicals, chemical weapons, or biotoxins in a water sample. Some tests involve biochemical reactions while others are bioassays utilizing organisms. Three commercially available tests used for security screening at a number of drinking water utilities are Microtox, Eclox, and the IQ Toxicity Test. Some acute toxicity tests (e.g., Microtox) have been utilized in the wastewater industry for years for nonsecurity related applications.

The Microtox system‡ is a broad-spectrum acute toxicity bioassay that can be used in the laboratory or the field. Microtox is the lab version and Deltatox is the portable field version. Microtox and Deltatox are based on a bacterial bioluminescence test described in Method 8050 of *Standard Methods* (APHA, AWWA, and WEF 1998). The assay is a metabolic inhibition test that utilizes a suspension of naturally luminescent marine bacteria, *Vibrio fischeri*, as the test organism. The assay involves adding approximately 10^6 of these bacteria, stored in a freeze-dried condition, into a water sample and measuring the resulting light output of the bacteria with a photometer (after 5, 15, or 30 min of exposure). If an acutely toxic substance is present in the sample, the substance should negatively affect the cellular structure or metabolism of the bacteria resulting in a measurable decrease in bioluminescence.

* Ludlum Measurements Inc., Sweetwater, Texas

† Hach Corp., Loveland, Colo.

‡ Strategic Diagnostics, Inc., Newark, Del.

By comparing luminescence for a sample with the luminescence measured for a negative control (i.e., bacteria suspended in reagent grade water), the system's software can indicate the presence of a toxic substance and gauge the intensity of the toxin's effect expressed as a percentage reduction in light emitted.

The Eclox system* is a simple water assay developed as a field-testing kit for the British military. The original application was to enable soldiers to perform rapid tests on raw water to determine treatability, and subsequently on treated water to help confirm safety for consumption. However, the simplicity and speed of testing also make the kit attractive for emergency use by water utilities investigating contamination threats. The Eclox screen is a rapid chemiluminescence assay for the presence of toxic substances. The test mixes a plant enzyme with other reagents to produce light.

Certain pollutants in water interfere with the chemical reaction and reduce the amount of luminescence. The extent of inhibition of chemiluminescence is assumed to be proportional to the concentration of the contaminant. Specifically, a distilled water blank, and subsequently water samples, are added individually to a mixture of the chemical luminol, a reaction enhancer (para-iodo-phenol), an oxidant, and the plant enzyme horseradish peroxidase. The resulting biochemical oxidation-reduction reaction releases free radicals, producing a stable chemiluminescence. The light released is measured over a four-minute period. Any substance in the water sample that absorbs free radicals (e.g., urine or fecal material) or attacks the enzyme (e.g., phenols, amines, or heavy metals) will reduce light output. The light released when bacteria are exposed to sample water is compared with that from bacteria exposed to a distilled water reference. The extent (percentage) of inhibition, indicated by reduction in luminescence in the sample water, is a measure of relative water quality.

Still another acute toxicity screening method that is commercially available, but based on a completely different test mechanism than those previously described, is the IQ Toxicity Test†. Rather than use a chemical reaction or bacterium, this assay utilizes an aquatic invertebrate as a toxin indicator. *Daphnia magna* is a freshwater crustacean (water flea) that is small, yet visible to the naked eye. Because *Daphnia* are sensitive to a variety of chemicals, they have been used for years as an indicator organism in both acute and chronic toxicity assays.

In the IQ Tox assay, the toxicity of a water sample is characterized by observing stressor-related suppression of *Daphnia* enzyme activity. Groups of six daphnids are placed into each of a series of clear 10-mL exposure chambers, some containing a negative control (reagent-grade water) while others contain the water being tested. Once the organisms are in contact with the control and

* Severn Trent Services, Oxfordshire, U.K.

† Aqua Survey, Inc., Flemington, N.J.

sample water for a one-hour period, a fluorogenically-tagged sugar suspension is added to each of the compartments. After an additional 15 minutes, the exposure chambers are illuminated with long-wave UV radiation (black light). The healthy control organisms will have ingested the tagged sugar (galactose) and expressed the enzyme (galactosidase). The marker, while unable to fluoresce when attached to the sugar molecule, is now liberated and fluoresces as it flows through the organism's circulatory system. If the *Daphnia* suspended in the sample water are not glowing like those in the control chamber, they are considered to be adversely affected by toxic substances in the water sample.

Acute toxicity screening tests are not precise analytical methods. Rather, they are the equivalent of chemical smoke detectors because they may indicate the presence of a toxic substance. Results from these tests must be compared with baseline data from earlier tests conducted on the same waters, prior to a suspicion of contamination, and be interpreted with a great deal of caution. The advantages of acute toxicity tests are that they detect a large variety of potentially toxic chemicals and produce results in a short amount of time. The disadvantages are that they can't identify the toxic substance and, because they are based on biological indicator systems, can sometimes produce spurious results. A comparison study of commercially available rapid toxicity tests for use on drinking water samples has been conducted by the US Army (van der Schalie et al. 2006).

Rapid Immunoassay

Immunoassay-based identification systems are immunochromatographic assays that qualitatively detect chemical or biological agents (antigens) by relying on the specificity of an antigen–antibody binding event. Immunoassay technology has been used as an analytical tool since the early 1980s to detect pathogens in clinical specimens, and since the 1990s in environmental applications to detect certain pesticides. When used to screen for biological agents, the antibodies target proteins that are unique to the agent. Several kits are commercially available for onsite screening for specific chemical and biological substances that might be used for intentional contamination of air, food, or water. The results are generally available within 15 minutes but are considered to be presumptive. Rapid immunoassay test results must be interpreted with extreme caution because they are susceptible to false-positive results. A study of several commercially available kits for detection of anthrax spores indicated poor sensitivity with a minimum detection limit of 10^5 to 10^6 spores per sample (King et al. 2003).

BTA (Bio Threat Alert) test strips* are based on the analytical technique, lateral flow immunochromatography. The suspect material, solid or liquid, is mixed with buffer and five drops of the mixture are added to the sample port of the test strip. The target agent moves along the membrane, inside the plastic test strip case, by capillary action. If the target substance is

* Tetracore, Gaithersburg, Md.

present in the sample above a certain concentration, the antibodies and target antigen combine in the test strip to form a reddish band that appears in a window. If a band only appears in the "C" window, the test is negative. This result indicates a successful positive control assay that uses a control antigen provided in the kit. However, if a band also appears in the "S" window, the sample is considered positive for the agent of concern.

The test strips can be read visually without the use of instrumentation. However, an electronic test strip reading device (Guardian Reader)^{*} is also available. According to the manufacturer, the reader increases detection sensitivity by 0.5 to 1 log-units because the optical technology can recognize positive results that may be too faint to see with ambient lighting. The reader is portable, powered by AC or battery, and can be taken to the site of suspected contamination. Also available are swab collection kits for sampling environmental surfaces, and a battery-operated portable air sampler (BioCapture BT-550)[†] which collects and concentrates aerosol samples and adds the sampled particles directly to a BTA test strip. Screening of environmental surfaces, air samples, and water samples at the site of suspected contamination is consistent with the field safety screening and rapid water testing recommendations presented in the USEPA's Response Protocol Toolboxes for drinking water and wastewater emergencies. Currently, the manufacturer offers the following specific test strips and detection limits. The detection limits shown here were obtained without the use of an electronic reader:

- *B. anthracis* (anthrax) (1×10^5 cfu/mL)
- *Y. pestis* (plague) (2×10^5 cfu/mL)
- *Francisella tularensis* (tularemia) (1.4×10^5 cfu/mL)
- Botulinum toxin (10 µg/L)
- SEB (2.5 µg/L)
- Ricin (50 µg/L)

The SMART (Sensitive Membrane Antigen Rapid Test) Ticket[‡] is another lateral flow immunoassay kit for detecting and identifying multiple analytes. The system detects agents (antigens) in the sample by immuno-focusing colloidal gold-labeled reagents (antibodies) and their corresponding target antigens onto small membranes. Within 15 minutes of addition of 100 µL (3 drops) of liquid sample onto the test ticket, formation of red lines, in both the internal control and sample compartments, indicates a positive result. Tests are commercially available for anthrax, cholera, tularemia, and plague bacteria as well as *Botulinum*, ricin, and SEB toxins. Unlike the BTA test strips, the manufacturer of the SMART kit does not offer an electronic reading device. However, accessory kits are available to assist in collection

* Alexeter Technologies LLC, Wheeling, Ill.

† Mesosystems Technology, Inc., Albuquerque, N.M.

‡ New Horizons Diagnostics, Columbia, Md.

of samples from liquids, air, and environmental surfaces. The manufacturer claims an overall detection limit similar to that advertised by the previous vendor (i.e., 10^5 cfu/mL for bacteria and 50 µg/L for biotoxins).

Rapid Enzyme Test

A rapid field enzyme test was developed a number of years ago for the qualitative detection of pesticides and nerve agents based on their inhibition of the enzyme cholinesterase. In this commercially available assay, a membrane disk, which is saturated with cholinesterase and attached to a test ticket, is dipped for a period of 1 minute into a water sample. The ticket is subsequently folded, for a period of 3 minutes, so that the sample disk is pressed tightly against a second disk containing an ester. If no pesticides or nerve agents are present in the water sample, the cholinesterase hydrolyzes the bound ester forming a blue-colored reaction product. However, if sufficient pesticide or nerve agent is present in the sample being tested, it inhibits the cholinesterase chemically bonded to the ticket preventing the reaction and resulting in no color change. A white color on the second disk indicates a positive result for the presence of pesticides or nerve agents.

The manufacturer of the enzyme assay provides no detection data for nerve agents, but lists detection limits for several pesticide groups (e.g., carbamates, 0.1 to 5 mg/L; thiophosphates, 0.5 to 5 mg/L; and organophosphates, 1 to 5 mg/L).

Field Detection and Identification of Pathogens

Nucleic acid-based techniques detect and identify biological agents through the targeting of nucleic acids (DNA). PCR is a nucleic acid-based molecular biology technique developed in the early 1980s that amplifies DNA. Originally applied as a clinical analytical method, it has since been extensively used in genetic research and forensic applications, and is becoming more widely utilized in environmental analysis. PCR is an analytical approach for detecting and identifying specific microorganisms in environmental samples. However, while usually not prone to false positives, the technique is susceptible to interferences that may be present in the sample matrix.

As a tool for identification of environmental microorganisms, PCR requires pretreatment of a sample to lyse microbial cells and expose nucleic acids. This step can involve the use of lytic enzymes, freeze-thaw cycles, or bead heating techniques. A combination of DNA primers, enzymes, and nucleotide bases are then added to the preparation. The primers are designed to compliment and combine with a unique segment of DNA in the target microorganism (i.e., the specific virus, bacterium, or protozoan that the analyst is attempting to detect). The enzyme, DNA polymerase, and excess nucleotide bases are added to synthesize copies of the target DNA beginning with a typical 25 to 35 base-pair primer unit. The process of separating (denaturing) double-stranded DNA, attaching (annealing) the primer to the single-stranded target DNA, and synthesizing (extending) a new strand of DNA (amplicon) is controlled by cycles of temperature change (heating and

cooling). Denaturation typically occurs at 94 °C, annealing at 60 °C, and DNA elongation at 72 °C. There is a doubling of double-stranded DNA with each temperature cycle. Therefore, an original double-stranded DNA in a sample, exponentially multiplied through a series of 30 temperature cycles, can produce a billion new copies of DNA.

The presence of a large number of DNA strand copies permits detection by one of several analytical techniques such as fluorogenic gene probes or gel electrophoresis and is used to identify microorganisms that carry the target DNA within them. This assay can also be used to detect residual DNA that is bound to toxin preparations, such as *botulinum* toxin or ricin toxin, if the sample containing the toxin has not been subjected to conditions that cause extensive degradation or removal of the DNA from the organism that produced the toxin. Detection strategies can be designed so that multiple locations within the DNA of a biological threat agent are targeted, thereby increasing confidence in the identification.

Idaho Technology* has developed the R.A.P.I.D. (Ruggedized Advanced Pathogen Identification Device) LT PCR laboratory system to detect a number of pathogenic bacteria, viruses, and protozoans in clinical and environmental samples, which could be used as bioterrorism agents. The system, which costs approximately \$40,000, is built on LightCycler® technology and combines rapid air thermocycling and a real-time fluorometer to identify contaminants in less than 45 minutes. Software loaded onto a laptop computer is used to automatically run the analytical program and analyze the results. The pathogens currently detectable by the commercially available system are listed in Table 15-1. Test kits for a number of additional pathogens should be available in the near future.

Idaho Technology has also developed a more rugged version of the LT laboratory system described above. This instrument permits PCR analysis in the field. The unit, which costs about \$55,000, is termed the R.A.P.I.D. PCR System. Emergency response teams and utility teams can utilize this instrument to screen for pathogens at the site of suspected intentional or accidental contamination. The R.A.P.I.D. system is used extensively by the US Department of Defense, including the National Guard Civil Support Teams. The system's analysis speed and detection capabilities make it a good tool for utility personnel or emergency response teams investigating suspected water contamination incidents.

Table 15-1. Pathogens detected by R.A.P.I.D. per analyzers

| | |
|---|---|
| <i>B. anthracis</i> (anthrax) | <i>Campylobacter</i> spp. |
| <i>F. tularensis</i> (tularemia) | <i>E. coli</i> O157 |
| <i>Y. pestis</i> (plague) | <i>Salmonella</i> spp. |
| <i>Brucella</i> spp. (brucellosis) | <i>Listeria monocytogenes</i> (listeriosis) |
| <i>C. botulinum</i> (botulinum toxin) | <i>Variola</i> spp. (smallpox) |
| <i>Cryptosporidium</i> spp. (cryptosporidiosis) | Ricin toxin |

* Idaho Technology, Inc., Salt Lake City, Utah



Courtesy of Idaho Technology Inc.

Figure 15-1. Idaho Technology R.A.P.I.D. PCR system

Specifically, the R.A.P.I.D. system process involves a preliminary DNA extraction step in which the cell walls of microbes in a small volume of water sample (or a sample concentrate) are disrupted by a mechanical bead-heating process. Substances, such as environmental humic and fulvic acids, that could potentially interfere with the PCR process are removed using a purification kit. The purified sample DNA is then added to a freeze-dried mixture of DNA primers, nucleotide bases, polymerase enzyme, buffer, and gene probes. The DNA-specific probes have fluorescent dyes attached to them to permit detection of the target DNA once it is copied. Because only a small volume of the sample is added to thin capillary tubes in preparation for DNA amplification (multiplication) by temperature cycling (heating and cooling), cycling is rapid. Forty-five cycles of temperature change can be completed within a 30-minute period. As DNA is amplified, via temperature cycling, the amount of fluorescent probe taken up by the copied DNA continues to increase. The increasing fluorescence is measured by a fluorometer, on a real-time basis during amplification, indicating the presence of target DNA as it is being synthesized.

Some advantages of this commercial system are that the sample preparation procedure is standardized, the analytical system is closed to reduce the potential for laboratory DNA contamination, the kit includes positive and negative DNA controls, and the initial data interpretation is automated. The R.A.P.I.D. PCR system can be used to detect pathogens and some toxins in water samples (rapid field testing), and through the use of swabs these substances can also be detected on environmental surfaces at the suspected site of contamination (field safety screening). Using this system for investigation of suspected contamination events permits screening for select bioterrorism agents such as *B. anthracis*, *Y. pestis*, and *Brucella* species without culturing the specimen and thereby increasing the amount of potentially dangerous select agents.

Field Detection and Identification of Organic Compounds

As indicated in chapter 12, Contamination Warning Systems, an increase in the background concentration of TOC is one of the most sensitive surrogate indicators for the presence of contaminants containing organic carbon. The Sievers 900 Portable TOC Analyzer* is a field deployable unit that can be used to measure TOC in water samples at the sites that are suspected of being contaminated. This instrument measures TOC using UV/persulfate oxidation and membrane conductometric detection.

A general screening for the presence of VOCs in the field can be obtained with commercially available “sniffer” devices. The ppbRAE Plus Monitor (model PGM-7240), manufactured by RAE Systems Inc.†, can be used to analyze the head space of liquid samples for VOCs volatilizing from a water sample or liberated from the sample by shaking or agitation. This handheld continuous monitor, equipped with a photoinization detector (PID), can detect the presence of approximately 250 compounds, including toxic industrial chemicals and chemical warfare agents. While the instrument cannot identify specific compounds, it can provide an estimate of the total concentration of VOCs. The detection range is 1 µg/L to 2,000 µg/L, with a resolution of 1 µg/L within the 0 to 10 µg/L range. The device should be calibrated monthly using isobutylene. A similar VOC screening device is the MSA Passport PID II Portable Gas Detector‡. The operating range for this instrument is 0.1 to 10,000 µg/L isobutylene.

A more detailed detection and identification of organic compounds in the field can be obtained using field deployable GC or GC–MS. INFICON§ manufactures and distributes the portable HAPSITE Smart GC–MS which identifies and quantifies volatile hydrocarbons onsite in air, soil, and water samples. The system has been used for detection of toxic substances and chemical weapons of mass destruction by the military, United Nations inspectors, and HazMat response teams. The HAPSITE GC–MS is equipped with a “situ probe” purge-and-trap sampling device. With this system, collection and concentration of VOCs is accomplished on site by placing the probe, which is connected to the GC–MS, into the sample bottle or actual water body (lake, reservoir, stream, etc.) being tested. A more recent version of this instrument is the Inficon ER.

The purge-and-trap GC and GC–MS systems are field deployable and operate either by rechargeable battery or from a 24-volt converter when external power is available. They can each analyze individual samples or operate automatically for unattended continuous water stream analysis. Typical detection limits are in the low parts per billion (µg/L) to parts per million (mg/L)

* GE Analytical Instruments, Boulder, Colo.

† RAE Systems Inc., San Jose, Calif.

‡ MSA, Pittsburgh, Pa.

§ INFICON, Inc., East Syracuse, N.Y.



Courtesy of Inficon

Figure 15-2. Inficon Hapsite GC-MS

range. The gas chromatograph portion of the system is temperature programmable (45° to 225 °C) and can detect volatile compounds with a molecular weight ranging from 45 to 300. The mass spectrometer utilizes an electron multiplier detector. The GC-MS system has the mass spectra of 170,000 organic compounds, including those of chemical warfare agents, stored in its library to facilitate identification of unknowns.

The advantage of a field-portable GC or GC-MS over use of an off-site laboratory is that analyses can be run more quickly and results employed more directly to guide the site investigation and inform urgent utility operational responses and public health decisions. The systems can be used to screen for VOCs in both air and water samples using the *situ* probe sampler. Monitoring of air samples (field safety screening) and water samples (rapid field testing of water) are both recommended during site characterization in the USEPA Response Protocol guidelines. Table 15-2 summarizes the characteristics of the rapid field techniques previously described.

SAMPLE CONCENTRATION IN THE FIELD

One of the problems associated with rapid field testing of natural water, drinking water, or wastewater samples is that the detection limits of some of the analytical techniques (e.g., immunoassay, PCR) are not low enough to produce results of public health significance. This suggests the need for a rapid sample concentration method that can be employed in the field prior to testing.

The Pittsburgh Water and Sewer Authority Laboratory developed a simple field concentration method that can be used by a site characterization team to concentrate a water sample in a 15-minute period (States et al. 2006). This method successfully concentrates protozoans and bacteria, but the filter pores are too large to trap viruses. The technique involves filtration of two liters of finished drinking water through a commercially available disposable filter unit that has a 300-mL capacity polypropylene filter funnel containing a 47-mm diameter, 0.45-µm pore-sized, mixed cellulose ester membrane

Table 15-2. Rapid analytical techniques summary

| Assay/Test | Rapid Immunoassays | Rapid Enzyme Test | Rapid PCR | Field Deployable GC or GC-MS | Acute Toxicity Screening Methods |
|-----------------------------------|--|--|---|---------------------------------------|--|
| Manufacturer | BTA Test Strips (Tetracore) SMART Tickets (New Horizons) | Severn Trent | Idaho Technology | INFICON | Eclox (Severn Trent) Microtox (Strategic Diagnostics) IQ Tox (Aqua Survey) |
| Contaminants detected | Pathogens: anthrax, plague, <i>tularemia</i> , cholera Biotoxins: <i>Botulinum</i> , ricin, SEB | Insecticides: organophosphates, carbamates, thiophosphates Nerve Agents | Pathogens: Anthrax, plague, <i>tularemia</i> , <i>brucella</i> , <i>Campylobacter</i> , <i>E. coli</i> O157, <i>Salmonella</i> , <i>Listeria</i> Biotoxins: <i>Botulinum</i> , ricin | VOCs | Industrial chemicals, weaponized chemicals, biotoxins |
| Detection limits* | Pathogenic Bacteria: 10^5 CFU/ml Biotoxins: 2 to 50 ppb(μ g/L) | Insecticides: 0.1 to 5 ppm (mg/l) Nerve Agents: Data not available | Approximately 10^3 cfu/ml | PPb to ppm (Low μ g/L to mg/L) | Eclox: Simple Microtox and IQ Tox: Moderately difficult |
| Difficulty in performing analysis | Simple | Simple | Moderately difficult | Most difficult | Eclox: 5 Microtox: 45 IQ Tox: 90 |
| Time†‡ (minutes) | 15 | 5 | 90 | 60 | |

Notes: * Manufacturer's reported detection limits without sample concentration.

† Run time for the field test (including sample preparation).

‡ Most of these methods allow more than one sample to be run simultaneously.



Figure 15-3. Field concentration apparatus

filter. This is the same type of filter typically used in water laboratories for bacteriological testing utilizing the membrane filtration method. The filter unit used in the published method was manufactured by the Pall Corporation (part number 4815) and costs approximately \$4 per disposable unit.*

The two liter sample is drawn through the membrane filter via suction produced by a hand-operated pump. Following filtration, the membrane filter is removed from the filter unit using forceps and sterile technique and inserted into a sterile, disposable 15-mL polystyrene centrifuge tube (Corning model #25310).† 2.0 mL of surfactant (0.5% Tergitol 7, or equivalent) is added to the centrifuge tube either before or after insertion of the rolled up membrane filter. The tube is then capped and vortexed at maximum speed for a period of one minute using a portable field vortex. The washed filter is removed again using sterile technique. In the case of drinking water samples, the 2-mL eluate containing the bacteria and protozoans captured on the membrane filter represents a 1,000-fold concentration, by volume, of the original sample water. The concentrate can then be screened for the presence of various contaminants using rapid field analytical screening techniques such as rapid immunoassay or PCR.

This field concentration technique can also be used to concentrate natural waters (e.g., rivers, lakes) and treated effluent from wastewater treatment plants. However, because of elevated turbidities in natural waters and wastewater plant outfalls, and therefore the smaller volumes that can be passed through the filter, the achievable concentration factors are less than for drinking water samples. The field concentration apparatus is shown in the Figure 15-3.

* Pall Corp., Ann Arbor, Mich.

† Corning Glass Works, Corning, N.Y.

Still another approach to field concentration is the use of ultrafiltration (UF) for recovering and concentrating microbes from large volumes (greater than 100 L) of water. Because of their minute pore sizes, UF filters are capable of simultaneously concentrating viruses, as well as bacteria and parasites, based on size exclusion. Published studies have shown high percentage recoveries of spiked microbes (Hill et al. 2007). The CDC is currently using this technique for rapid concentration of microbes from water samples in their Laboratory Response Network (LRN) laboratories. USEPA has been working for the past several years on a version of the UF concentration method that can be used in the field (Lindquist et al. 2007).

SAMPLE COLLECTION

Following rapid field testing of water in the field, the next task that the site characterization team needs to accomplish is collection of samples for more definitive analyses in laboratories. Module 3 of USEPA's Response Protocol Toolboxes for Drinking Water (2004) and Wastewater Systems (2009) contain guidance for proper collection of samples in the field. These modules contain important information on ensuring the safety of the field personnel collecting the samples. The modules also recommend a field water sample collection kit. This kit contains appropriately sized sample bottles to ensure that all of the categories of contaminants that might be anticipated during an accidental or intentional contamination event in either a drinking water or wastewater system can subsequently be analyzed in a laboratory. Emphasis is placed on using sample bottles constructed of appropriate materials for the contaminant class being tested for (e.g., glass versus plastic), as well as field preservation techniques to ensure the stability of analytes prior to laboratory analysis.

A number of state regulatory agencies, response organizations, and utilities have prepared and prepositioned field sampling kits in anticipation of contamination events. The California Department of Public Health, with the assistance of local water system laboratories, has developed an emergency water quality sampling kit for use in suspected contamination incidents (Crisologo 2008). Once the occurrence of a credible event has been indicated, the state health department deploys three kits to the incident site. One kit is used to sample water at the incident site, one serves as a backup, and the third is used to sample water upstream of the site in order to obtain background data.

DEFINITIVE LABORATORY ANALYSIS

Rapid field testing of water by the site characterization team at the suspected site of contamination is just one step in the site characterization process and the overall investigation of the contamination threat. As described in USEPA's Response Protocol Toolboxes, should incident command determine

Table 15-3. Definitive analytical methods recommended for various categories of contaminants

| | |
|---------------------|---|
| Inorganic chemicals | Ion chromatography Atomic absorption spectrophotometry Inductively coupled plasma Inductively coupled plasma–mass spectrometry |
| Organic chemicals | GC GC–MS Liquid chromatography Liquid chromatography–mass spectrometry Immunoassay test kits |
| Biotoxins | Immunoassay test kits GC–MS Liquid chromatography Liquid chromatography–mass spectrometry |
| Bacteria | Culture Biochemical and serological tests PCR Sequencing |
| Protozoa | Immunofluorescence microscopy Sequencing |
| Viruses | Mammalian cell culture PCR Sequencing |

Adapted from: Magnuson et al. 2005

that the threat of contamination is not only possible but actually credible, the samples collected during the site characterization process need to be sent to one or more qualified labs for definitive (confirmatory) analysis involving identification and quantification of chemical, biological, and/or radiochemical contaminants. In some cases, incident commanders, utilities, and other officials may decide not to wait for a formal determination of credibility of the threat but may opt to send samples for more conclusive analysis immediately following collection.

A difficult challenge for any laboratory is to detect, identify, and quantify unknown, and possibly hazardous, substances in a water sample. Module 4 of USEPA's Response Protocol Toolboxes describes an analytical approach for the analysis of samples from a suspected contamination site. The approach is not a detailed, prescriptive protocol but rather a flexible framework for an individual laboratory to develop its own approach for the analysis of water samples containing unknown contaminants. The recommended methods include a combination of standardized tests as well as exploratory techniques. Analytical methods recommended for various categories of contaminants are detailed in Table 15-3.

USEPA's Response Protocol Toolboxes do not prescribe which laboratories should be responsible for comprehensive testing of the samples. This is

a decision that needs to be made by officials in charge of a specific incident and should be addressed prior to the incident in the utility's ERP. The laboratories used may be a combination of utility, commercial, government, and academic labs. The final laboratory selection will be influenced by the laboratory resources available as well as local and state SOPs.

As discussed in the Response Protocol Toolboxes, if there is an indication that the suspect contaminant is especially hazardous, analysis should be conducted by specially certified laboratories. For example, if field screening or other information suggests that the water may have been contaminated with a radionuclide, the sample should be processed by a laboratory certified to handle radioactive materials. If there is an indication that the water has been contaminated with a select biological agent such as the bacteria *B. anthracis*, *Brucella* spp., *Y. pestis*; the virus *Variola* spp.; or the biotoxins ricin or botulinum toxin, etc., then the samples should be analyzed by a laboratory that is part of the CDC's Laboratory Response Network (LRN). LRN labs are specially licensed to deal with select biological agents.

Finally, if there is an indication that the water may have been contaminated with a weaponized chemical such as the nerve agents soman, sarin, or VX, the samples should be sent, via the FBI, to a lab certified to work with such agents (e.g., the U.S. Army Laboratory at Edgewood Chemical and Biological Center in Maryland, or the Lawrence Livermore Lab in California). If the determination is made that samples are hazardous enough to need to be sent to any of these specialty laboratories, it is also imperative that these samples be collected and shipped by appropriately trained and equipped HazMat response teams. If there is no indication of special hazard, the samples may be sent to more general laboratories.

CALIFORNIA MUTUAL AID LABORATORY NETWORK

The California Department of Public Health has organized a consortium of laboratories called the California Mutual Aid Laboratory Network (CAMAL Net) (Crisologo 2008). The consortium includes laboratories from the California Department of Health, USEPA, the California Department of Water Resources, and a number of public water systems and is patterned after the WARN described in chapter 18. CAMAL Net would be activated to handle the surge in sample analyses that would be required should there be a major accidental or intentional contamination event in California. These analyses could include those needed to determine the extent of the contamination event as well as those needed to determine the effectiveness of the cleanup process.

CDC LABORATORY RESPONSE NETWORK

The LRN was established by the CDC in collaboration with the FBI and the Association of Public Health Laboratories in accordance with Presidential

Decision Directive 39 (PDD-39), which outlined national anti-terrorism policies and assigned specific missions to federal departments and agencies. The LRN became operational in 1999 with the objective to ensure an effective laboratory response to bioterrorism. The LRN is an integrated network of state and local public health, federal, military, and international laboratories that can respond to bioterrorism, chemical terrorism, and other public health emergencies.

The LRN is organized into three groups of laboratories:

- *Sentinel laboratories* include hospital-based and public health labs that provide the initial screening of samples and either rule them out as containing potentially harmful agents or refer them to higher-level labs for additional analysis and confirmation.
- *Reference laboratories* are responsible for investigation and/or further referral of specimens. They include more than 100 state and local public health, military, international, veterinary, agricultural, food, and water testing labs.
- *National laboratories* include those operated by CDC, the US Army Medical Research Institute for Infectious Diseases, and the Naval Medical Research Center. They are responsible for identifying strain characteristics, bioforensics, select agent activity, and handling highly infectious biological agents.

While the LRN laboratories have particularly strong capabilities in the area of clinical samples, the network is rapidly improving its capabilities to respond to contamination threats in drinking water samples as well. Because of the danger associated with handling select biological agents such as anthrax, ricin, and botulinum toxin, among others, water samples believed to contain such materials would be directed very quickly to the LRN for analysis.

USEPA ENVIRONMENTAL LABORATORY NETWORKS

Should the public water supply of a major US city become contaminated, the laboratory resources in that particular area could be quickly overwhelmed in analyzing samples to determine the identity of the contaminant, the extent of water system exposure, and verifying the effectiveness of remediation efforts. In anticipation of such an eventuality, HSPD 9 charged USEPA to “develop nationwide laboratory networks to support monitoring and response during intentional and unintentional contamination events.”

USEPA’s Water Security Division and the USEPA regional laboratory chiefs have developed Regional Laboratory Response Networks in which USEPA regional labs, state environmental and public health labs, and utility labs integrate their resources to respond to drinking water contamination emergencies in their regions. The regional laboratory networks will provide the backbone for a national Water Laboratory Alliance (WLA), which will be

described by the Water Laboratory Analysis—National Response Plan (WLA–NRP)(Mapp 2009).

The WLA is a national network that includes USEPA regional labs, state environmental and public health labs, and utility labs from across the country. The WLA uses standardized analytical procedures to respond to drinking water sector contamination threats and incidents. This national network also includes specialized laboratories with analytical capabilities to deal with nonroutine chemical, biological, and radiological contaminants including chemical warfare agents.

The WLA is being developed based on existing laboratory networks such as the CDC's LRN. Similar to the CDC LRN, the WLA will consist of three tiers of laboratories:

- *Sentinel laboratories* will perform routine monitoring and surveillance and will rule out or refer samples to confirmatory labs for further analysis.
- *Confirmatory laboratories* will perform rapid, high-confidence presumptive and confirmatory identification of samples referred by sentinel labs. These labs will have Biosafety Level (BSL) 2/3 facilities, limited surety capability for chemical warfare agents, and will be able to analyze radioactive samples.
- *Reference laboratories* will provide definitive characterization of chemical, biological, and radiochemical (CBR) agents and attribution of the source. These labs will have highly specialized containment (BSL 3/4) facilities, chemical surety, and highly trained staff.

Once fully developed, the WLA will be an integral component of USEPA's Environmental Response Laboratory Network (eRLN). While WLA focuses only on drinking water, the eRLN involves analyses of all environmental matrices (air, soil, water). The eRLN will incorporate many of the elements (e.g., laboratory types, proficiency testing, standardized methods) found in CDC's LRN and the Food and Drug Administration's Food Emergency Response Network.

COMMERCIAL LABORATORIES

Some commercial laboratories offer a 24/7 emergency response program for analysis of water samples in the event of a suspected contamination incident (Snell 2006). During an incident, these labs can screen for presence/absence, as well as provide confirmation and quantification, of a number of classes of contaminants and individual contaminants using the analytical framework recommended in Module 4 (Analytical Module) of USEPA's Response Protocol Toolboxes. Some labs promise verbal results within a matter of hours. Some also provide sample collection kits to utilities to have on hand in the event of an incident. Typically the contract labs require that an agreement be signed prior to an event. This approach provides a workable analytical option for utilities planning for laboratory services in their ERPs.

MOBILE LABORATORIES

Still another approach to providing rapid analysis of field samples is the deployment of mobile laboratories. A number of emergency response agencies from various levels of government have developed truck-mounted mobile labs to respond to a variety of contamination events involving air, water, and other environmental matrices. The US Army National Guard has established at least one civil support team in each state. The team deploys with mobile laboratories to respond to threats of bioterrorism and is also employed ahead of time during planned events such as major sporting venues and political assemblies, among others.

A US Department of Agriculture mobile laboratory in a trailer was successfully deployed to respond to the mailborne anthrax attack in Washington DC in 2001. This lab, equipped with two real-time Idaho Technology R.A.P.I.D. PCRs (described in a previous section) screened multiple envelopes, air samples, and environmental swabs from buildings throughout the area for the presence of anthrax spores (Higgins et al. 2003).

WATER CONTAMINANT INFORMATION TOOL

In 2005, USEPA developed the Water Contaminant Information Tool (WCIT). WCIT is a password-protected, online database that currently contains information on 102 contaminants that would pose a serious threat if they were intentionally or accidentally introduced into drinking water or wastewater systems. The information in WCIT is obtained from the open literature and is therefore not classified. However, once this information from a variety of sources is compiled into a single reference database, it is considered sensitive because it potentially provides useful information for individuals wishing to threaten or contaminate a water system. For this reason, access to the WCIT database must be obtained ahead of time from USEPA through a formal registration process. Organizations that are eligible for access to WCIT include water utilities, regulatory agencies, water industry organizations, health agencies, and government laboratories.

While WCIT contains information on a number of aspects of the selected contaminants, most importantly it provides information about their analytical characteristics. Specifically, the database lists rapid analytical tests that can be used to detect these contaminants in the field as well as more definitive assays that can be used to confirm the identity and quantity of contaminants in the laboratory.

Additional information on WCIT, and registration instructions, can be obtained from the following Web sites: www.epa.gov/wcrt or <http://cdx.epa.gov>.

USEPA LABORATORY COMPENDIUM

A source of information on laboratories currently able to accept emergency samples is available from USEPA's Environmental Laboratory Compendium.

The compendium is a database of nationwide environmental laboratories available to water utilities and to government agencies. The database lists each laboratory's specific capabilities for analyzing chemical and biological analytes as well as chemical warfare, bioterrorism, and radiochemical agents. The compendium was developed as a tool to quickly identify labs that can support incident-specific response and recovery. It is intended to assist utilities, and federal and state agencies in responding to contamination threats, terrorist attacks, or natural disasters. Access to the database is restricted. Interested organizations must first register with USEPA at their Web site, www.epa.gov/compendium.

STANDARDIZED ANALYTICAL METHODS

To standardize contaminant identification in environmental samples across multiple laboratories following a homeland security-related contamination incident, USEPA's National Homeland Security Research Center (NHSRC) has compiled a list of laboratory methods for contaminants relevant to water security. The list is designated the Standardized Analytical Methods (SAM) document. These methods can be used by laboratories analyzing environmental samples for biological, chemical, radiochemical and biotoxin contaminants. The listing is especially intended for use in remediation activities following a contamination incident.

To date, the SAM document lists methods to identify and measure approximately 120 chemical contaminants, 18 radionuclides, 11 pathogens, and 17 biotoxins that may be of concern. The document can be accessed online from the USEPA Web site, www.epa.gov/NHSRC/pubs/report-SAM030107.pdf.

NEMI–CBR

The National Environmental Methods Index for Chemical, Biological, and Radiological Methods (NEMI–CBR) was developed through a partnership between USEPA and the U.S. Geological Survey. NEMI–CBR is a secure, on-line, web-based database for locating and comparing analytical methods for chemical, biological, and radiological-related contaminants that could pose a threat to water systems. NEMI–CBR includes methods for both screening and confirmation and, where applicable, provides multiple methods for the same analyte. Laboratories can use this database to compare the performance, speed, and relative costs of various analytical techniques.

NEMI–CBR is a modification of the National Environmental Methods Index (NEMI), which is a freely accessible database of environmental methods searchable on the Internet at www.nemi.gov. Because NEMI–CBR deals with contaminants that have been selected as being potentially problematic in water systems, access to the database requires preregistration. Registration for NEMI–CBR is obtained jointly with registration for WCIT previously described.

REFERENCES

- American Public Health Association (APHA), American Water Works Association (AWWA), and Water Environment Federation (WEF). 1998. *Standard Methods for the Examination of Water and Wastewater*, 20th ed. Washington, D.C.
- Crisologo, J. 2008. California Implements Water Security and Emergency Preparedness, Response, and Recovery Initiatives. *Jour. AWWA*, 100(7):30.
- Gaffney, L.J., and G.A. Burlingame. 2009. Laboratory Emergency Response: Screening of Unknown Contaminants in the Field and in the Lab. *Proc. 2009 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Higgins, J.A., M. Cooper, L. Schroeder-Tucker, S. Black, D. Miller, J.S. Karns, E. Manthey, R. Breeze, and M.L. Perdue. 2003. A Field Investigation of *Bacillus anthracis* Contamination of U.S. Department of Agriculture and Other Washington, D.C. Buildings During the Anthrax Attack of October 2001. *Appl. Environ. Microbiol.*, 69(1):593.
- Hill, V.R., A.M. Kahler, N. Jothikumar, T.B. Johnson, D. Hahn, and J.L. Cromeans. 2007. Multistate Evaluation of an Ultrafiltration-Based Procedure for Simultaneous Recovery of Enteric Microbes in 100-Liter Tap Water Samples. *Appl. Environ. Microbiol.*, 73(13):4218.
- King, D., V. Luna, A. Cannons, J. Cattani, and P. Amuso. 2003. Performance Assessment of Three Commercial Assays for Direct Detection of *Bacillus anthracis* Spores. *J. Clin. Microbiol.*, 41(7):3454.
- Lindquist, H.D.A., S. Harris, S. Lucas, M. Hartzel, D. Riner, P. Rochele, and R. DeLeon. 2007. Using Ultrafiltration to Concentrate and Detect *Bacillus anthracis*, *Bacillus astrophilus* Subspecies *globigii*, and *Cryptosporidium parvum* in 100-Liter Water Samples. *J. Microbiol. Methods*, 70(6):484.
- Magnuson, M.L., S.C. Allgeier, B. Koch, R. DeLeon, and R. Hunsinger. 2005. Responding to Water Contamination Threats. *Environ. Sci. Technol.*, 39:153A.
- Mapp, L. 2009. Water Laboratory Alliance: A Focus on Laboratory Response. *Proc. 2009 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Snell, L.J. 2006. Public Water Supply Security and Emergency Response: An Environmental Laboratory Perspective. *Proc. 2006 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- States, S., M. Scheuring, J. Kuchta, J. Newberry, and L. Casson. 2003. Utility-based Analytical Methods to Ensure Public Water Supply Security. *Jour. AWWA*, 95(4):103.
- States, S., J. Newberry, J. Wichterman, J. Kuchta, M. Scheuring, and L. Casson. 2004. Rapid Analytical Techniques for Drinking Water Security Investigations. *Jour. AWWA*, 96(1):52.
- States, S., J. Wichterman, G. Cyprych, J. Kuchta, and L. Casson,. 2006. A Field Concentration Method for Rapid Response to Security Incidents. *Jour. AWWA*, 98(4):115.
- US Environmental Protection Agency (USEPA). 2004. *Drinking Water Response Protocol Toolbox: Planning for and Responding to Contamination Threats in Drinking Water Systems*. Washington, D.C.: USEPA.
- USEPA. 2008. *Sampling Guidance for Unknown Contaminants in Drinking Water*. Washington, D.C.: USEPA.
- USEPA. 2009. *Wastewater Response Protocol Toolbox: Planning for and Responding to Contamination Threats in Wastewater Systems*. Washington, D.C.: USEPA.
- van der Schalie, W.H., R.R. James, and T.P. Gargan. 2006. Selection of a Battery of Rapid Toxicity Sensors for Drinking Water Evaluation. *Biosensors and Bioelectronics*, 22:18.

EMERGENCY COMMUNICATIONS WITH THE PUBLIC

Crisis or emergency risk communication is the attempt to provide information that helps individuals, stakeholders, or an entire community make the best possible decisions during an emergency. Unfortunately, during the past decade in the United States, we have witnessed too many occasions of crisis communications in action, including the events of 9/11, the mailborne anthrax attacks, the Washington, D.C. snipers, and Hurricane Katrina. In some cases, the emergency communications with the public have proved excellent, while in other situations the communications efforts have been poor. Good crisis communications can calm public fears, provide necessary information, inspire support for response efforts, and help save lives. Inadequate crisis communication can exacerbate fears, undermine public confidence, and reduce response effectiveness. There is little doubt that emergency communications can directly influence events and the outcome of a critical situation.

In the age of 24-hour, on-the-scene, global, instant news, and a well-read populace, the requirement to communicate effectively with the media during a crisis is greater than ever before. Because during an emergency most people immediately click on a television or log-on to an Internet news site to obtain the latest information on the status of an unfolding event, and find information on steps to protect themselves and their families, there is a greater need than ever for utilities to establish a working relationship with the media.

This chapter discusses some of the basic principles of emergency communications. It also summarizes suggestions for dealing effectively with the media. This information has been gleaned from the literature, discussions

with public information officers and risk communication specialists, and personal experience from years of working in the drinking water industry and dealing with reporters. Finally, message mapping for water and wastewater utilities is introduced as a tool that can assist crisis communicators in delivering emergency information accurately and effectively through the media to the people who need the information.

CRISIS COMMUNICATIONS OVERVIEW

Several key points concerning communications with the public during a water emergency merit mention.

First, the primary goal during a serious water emergency is to save lives and protect public health. Unlike most other commodities and services, the provision of safe drinking water and the efficient removal of sanitary wastes is a public health function. This concept is even more important during an incident in which a pathogen or toxin may have entered the public water supply with the potential for causing injuries or death. During an emergency, utilities must ensure the public understands that the protection of their health is the utility's overarching goal, and this message must be communicated in a manner that engenders trust and confidence. Otherwise, people may not pay attention to critical emergency information that may be important for their safety.

Secondly, during an emergency it is essential that government representatives, response agencies, and utilities speak with one voice. Consistent messages are vital. Inconsistent messages can increase confusion and anxiety, and diminish the credibility of officials. Most public information specialists and industry organizations also recommend that, if possible, the utility should be the first to release information on how an emergency is affecting the water supply. During later stages of an emergency, when emergency operations and joint information centers have been activated, public information will come from one of these sources. However, the utility should always avoid giving the impression that it is delaying or withholding important information. Delayed release of information can result in a loss of public confidence and accusations of a cover-up. In the worst-case scenario, delayed release of information could result in adverse public health impacts.

Communication objectives, during an emergency, should primarily focus on

- Situation status updates
- Public protection measures, such as boil water advisories
- Measures that help the utility to better deal with the situation, such as through issuance of water conservation advisories.

During an accidental or intentional contamination of the drinking water or wastewater, the information that consumers will want and need to receive can be anticipated. This includes

- Description of the contaminant

-
- Public health effects resulting from the contaminant
 - Geographical extent of affected area
 - How the contaminant got into the water
 - Limits on use of the water and protective actions that consumers should take
 - Expected duration of the emergency
 - How utilities, health agencies, and law enforcement are responding
 - Locations for alternative water supplies or sanitary services
 - Sources for more detailed information (e.g., hot-line numbers, web sites)
 - Reassurance that the public will be kept informed

Just as a utility prepares an ERP prior to a crisis occurring, the utility should also develop an emergency communications plan. This plan contains lists of individuals who should be notified during an event, media contacts who the utility has worked with previously, utility personnel who may be relied on to serve as spokespersons for various types of emergencies, templates for anticipated press releases, and utility and community background information that might be needed on short notice during an incident.

Finally, during periods of crisis, it is clear that the public obtains most of its information from the media. Therefore, if the utility wants to effectively communicate with their customers, they have to be able to work with the media, and ideally should have established relationships with various media outlets before an emergency arises.

DEALING WITH THE MEDIA

Utilities and other organizations tend to view reporters with suspicion because of fears of being criticized by the media, or being quoted out of context. Therefore, the relationship with the media has the potential to become adversarial. However, during a crisis, one of the most important means for utilities and other response officials to communicate with the public, especially in a large water system, is through the media. Therefore, utilities need to develop and maintain a working relationship with both the electronic and print media. Many of the following suggestions may seem obvious or just plain common sense, but they serve as reminders for utilities preparing for the inevitable necessity of dealing with the media during a natural disaster, major accident, or manmade emergency:

Develop a working relationship with the media prior to an emergency. This will help utility staff feel more comfortable with reporters, and reporters will more likely trust the utility. A practical way to establish this rapport may be to invite the local newspaper or TV station for a treatment plant tour, and provide them with information for a background story on the water system that they can use during a slow news week.

Appoint one person (and an alternate) to be the media point-of-contact and primary spokesperson during an emergency.

Understand the challenges facing the spokesperson.

- Taking the utility from an “it” to a “we”
- Build trust and credibility for the organization
- Muster support for the response effort
- Ultimately, help reduce the number of illnesses, injuries, and deaths that could result from an emergency.

The utility public information officer is not necessarily the ideal spokesperson for every situation. Sometimes it is more appropriate for the executive director or a utility specialist in a particular area (e.g., water quality manager, chief of engineering) to act as spokesperson for certain issues. Whoever serves as spokesperson must have a thorough understanding of the utility and the situation at hand.

Clearly state the utility's priorities during a crisis—namely, protecting public health, and getting the situation under control. The spokesperson must assure the public that the utility is doing everything it can to meet those priorities.

Determine objectives for an interview or press conference prior to talking to the media. Is the utility trying to inform the public, convince them of the need for a particular response action, or reason with them? If possible, the spokesperson should specify the parameters for the interview or briefing before-hand to ensure that certain issues are addressed.

Prepare fact sheets about the utility in advance, and maintain press release templates that can be quickly filled in with details. Press releases should contain the following standard information: who, what, when, where, why, and, if known, how. Press releases should also contain the name and phone number of a contact person at the utility who can provide additional information.

Conduct press conferences and news briefings in a press room that is physically separated from the emergency command center. This is true whether the briefing is being held in a city or county EOC or the operations center for the water utility. The separation eliminates a source of distraction for the personnel who are actually working on the response to the situation. It also prevents the media from seeing information that may still be considered sensitive at that point in the emergency.

Do your homework before meeting with the media. Spokespersons must be certain of the facts prior to an interview or briefing. Spokespeople should prepare their remarks ahead of time and follow standard public information guidelines such as giving their title and spelling their name when introducing themselves.

Try to anticipate the perceptions and fears of the public, as well as likely questions.

The spokesperson should repeat the question before answering to ensure that the question is understood. If a question contains leading or loaded language, reframe it to eliminate the loaded language and then answer the

question. Break down multiple-part or complex questions into manageable segments and answer each part separately.

Be prepared for the “ambush” interview. Some press officers prepare a short sound bite that they can use to satisfy the reporter who tries to catch them off guard. Other spokespersons simply inform the reporter that it would be better to hold their question until the next scheduled news briefing so that all media outlets can receive the same information at the same time.

Answer sensational or irrelevant questions as briefly as possible and return to the key message. Use the following “bridges” to return to the key message

- “What I think you are really asking is...”
- “What I am really here to discuss is...”
- “Your readers/viewers need to know...”
- “What is important to remember is...”

Refrain from answering hypothetical or “what if” questions and deal only with the situation at hand.

Keep the message simple. Spokespeople should avoid technical jargon, industry acronyms and slang, and keep the discussion simple and direct to avoid confusion. If a technical term must be used, define it. It is generally recommended that communications be kept at about the eighth-grade level when dealing with the general public so that everyone can understand the message. This is especially important during high-tension situations when stress may impair an audience’s comprehension.

It may be necessary to communicate with the public before all the facts are known. If certain information is not known, admit it and describe what is being done to gather the information. Avoid conjecture and speculation.

A spokesperson should never discuss the costs of an incident, or issues such as the extent of insurance coverage, while a situation is still unfolding. The public may resent a preoccupation on costs when public safety is at stake.

Never use the phrase “No Comment.” This response appears evasive. Instead, explain why you can’t answer a particular question.

Avoid talking to reporters off the record. There is no guarantee that this agreement will be respected.

Use open body language. The spokesperson should sit or stand with arms relaxed by his or her sides. Crossed arms or hands on the hips appear defensive or cocky. Make eye contact when possible. Humor should be used very cautiously, as it can be a minefield, especially during a serious situation.

Never speak on behalf of other organizations. Similarly, utility spokespersons should refrain from answering questions outside of the utility’s area of expertise, such as health-related questions. These should be referred to appropriate agencies or officials.

Avoid assigning blame to other entities. This could result in embarrassment, and even future litigation, against the utility. Also, avoid premature assessment of the performance of response agencies.

Respect media deadlines. Hold news conferences early enough to allow reporters to prepare their stories for scheduled newscasts. Be on time for

interviews and briefings to help the utility project the image of competence. Following each news briefing, schedule a time for the next information update and meet this schedule even if there is no new information to report.

Maintain control of personal emotions. The spokesman should remain calm, appear authoritative but not arrogant, be polite, and never allow difficult questions to become personal. It is all right to be angry at the microbes or natural disasters that cause illness and death, but it is inappropriate to show outrage or become indignant with reporters.

Most importantly, be honest and straightforward with the media. It is vital to maintain the trust and confidence of the media and public. The public's tolerance for being deceived, especially in a time of crisis, is very low.

ADVICE FROM CRISIS COMMUNICATIONS SPECIALISTS

Crisis and risk communications that deal with natural, accidental, and contrived events has been extensively researched and discussed in the literature. A number of researchers have devoted years to this study and have come up with some interesting conclusions concerning effective public communications methods during an emergency.

In his publications (Covello et al. 2001), and on his website, www.centrforriskcommunication.org, Vincent Covello, a noted crisis communications specialist, has offered a number of important concepts dealing with crisis communications. Some of these concepts are highlighted here.

27/9/3 Rule: Key messages must be concisely stated if they are to be delivered through the media. Based on an analysis of 10 years of print and media coverage of emergencies in the United States, Covello found that the average length of a sound bite in the print media is 27 words, the average duration of a sound bite in the broadcast media is nine seconds, and the average number of messages reported in both print and broadcast media is three. Additionally, the quotes most likely to be used as sound bites contain compassion, conviction, and optimism.

Primacy-Recency Principal: This is the “first–last” principle, which essentially states that the most important messages should occupy the first and last positions in a list. In high-stress situations, listeners tend to focus on and remember what they hear first and last rather than what is said in the middle of a statement.

Citing Third Parties or Sources: Citing third parties, or sources that would be perceived as credible, increases the likelihood that a message will be believed and accepted by the audience.

95 Percent Rule: 95 percent of all questions that will be asked by stakeholders or the media can be anticipated in advance. In fact, Covello (2005) has provided a list of the 77 most frequently asked questions by journalists during a disaster or crisis.

Peter Sandman, another crisis communications specialist, also presents some general principles of emergency communications in his presentations, publications, and on his Web site, www.psandman.com. Some of his principles include speaking tips for spokespeople in emergency situations.

Do not over-reassure. Paradoxically, when people are unsure about how worried they should be, they often become more alarmed when officials seem too reassuring.

Acknowledge uncertainty. Sounding more certain than you really are rings false and can set you up to be wrong. Say what you know but emphasize what you don't know.

Tell people what to expect. Being forewarned helps people cope with adversity.

Offer people things to do. Self-protective action can help reduce fear. Action helps people deal with fear, outrage, panic, and even denial. If you have things to do, you can tolerate more fear. These are types of behavior that can be suggested to an uncertain public:

- Symbolic behaviors—things that don't help externally, but help people to cope, such as attending a community vigil.
- Preparatory behaviors—things to do now that will minimize risk if bad things happen.
- Contingent behaviors—things not to do now, but only if bad things happen, such as implementing a family disaster plan.

Acknowledge people's fears. When people are afraid, the worst thing to do is to pretend that they are not. The second worst thing is to tell them they should not be afraid. Both responses leave people alone with their fears.

Establish your own humanity. Express your feelings about the crises and show that you can bear them.

CRISIS COMMUNICATION PLAN

Emergencies are chaotic enough without the disorganization that results from not having a response plan. This is why the federal government, through the Bioterrorism Act, mandated that all drinking water utilities serving more than 3,300 people develop an ERP to guide a utility's response during emergencies. For the same reason, it is important to develop a crisis communication plan ahead of time. Such a plan is not intended to be a step-by-step guide for every emergency. Rather, it lays out the foundation for an agency's emergency communications by addressing such topics as roles, responsibilities, and available resources.

The CDC suggests that the following elements be included in a crisis communication plan (CDC 2002):

- A signed endorsement from the utility or agency director
- Designated line and staff responsibilities for the public information team
- Procedures for information verification and clearance/approval

As previously stated, additional elements of a crisis communication plan include:

- Media contacts
- Templates for press releases
- Utility background information

MESSAGE MAPPING

Mental noise theory, a primary construct of risk communication, indicates that when people are upset, they often have difficulty hearing, understanding, and remembering information. Research indicates that mental noise can reduce a person's ability to process information by more than 80 percent. An approach to overcoming the communication barrier created by mental noise is to develop a limited number of key messages that are brief, credible, and easily understood (Minamyer 2008).

Message mapping is a tool developed by Vincent Covello that can be used to effectively frame and deliver risk information (Covello 2005). Used correctly, message maps developed prior to an incident can help ensure that emergency information has the best chance of being heard, understood, and remembered. It helps organizations and agencies convey timely, accurate, clear, and credible information. Message maps enable audiences to better understand issues, act constructively on the information provided, recover more quickly from the stress of an event, and gain trust in emergency managers.

There are seven steps involved in the message mapping process.

1. Identify stakeholders
2. Identify probable stakeholder questions
3. Analyze the questions to identify the underlying concerns
4. Develop key messages
5. Develop supporting facts for the key messages
6. Test and practice messages
7. Deliver message maps through the appropriate information channels

A message map is an organized means for displaying layers of information. It is a visual aid that provides at a glance the communicating organization's messages for high concern issues such as a terrorist attack or a natural disaster. The map contains detailed, hierarchically organized responses to anticipated questions or concerns. As illustrated in Table 16-1, a message map is a grid containing multiple boxes.

The top portion of the message map identifies the audience for the main message and the particular concern that the message map is intended to address.

The next layer of the map contains the three key messages that are intended to respond to the audience's questions or concerns. The three key messages can also serve singularly or collectively as a media sound bite. Sound bites are important for successful media interviews.

Table 16-1. Message map template

| MESSAGE MAP TEMPLATE | | |
|----------------------------|----------------------------|----------------------------|
| Stakeholder: | | |
| Question or Concern: | | |
| Key Message 1 | Key Message 2 | Key Message 3 |
| Supporting information 1-1 | Supporting information 2-1 | Supporting information 3-1 |
| Supporting information 1-2 | Supporting information 2-2 | Supporting information 3-2 |
| Supporting information 1-3 | Supporting information 2-3 | Supporting information 3-3 |

The bottom layer of the message map contains supporting information that amplifies the key messages by providing additional facts or details. The supporting information can also take the form of visuals, analogies, personal stories, or references to credible sources of information. The supporting information is typically blocked in groups of threes under the key messages.

A sample message map is presented in Table 16-2. This map summarizes the type of information that a water utility, mayor, or EOC might deliver to the public in a news conference conducted to inform people of a credible contamination threat to the water supply.

The use of message mapping provides a number of benefits. It serves as a handy reference for officials and spokespersons who must respond quickly to questions on topics where timeliness and accuracy are important. Multiple spokespersons or agencies can use the same message map to help guarantee dissemination of consistent messages, keeping with the principle of multiple partners speaking with one voice. Additionally, message maps can reduce the chances of “speaker’s regret,” which can occur when the spokesperson says something inappropriate or doesn’t say something that should have been said.

Once developed, message maps can be used to structure press conferences, media interviews, information forums, public meetings, Web sites, telephone hot-line scripts, and fact sheets or brochures focused on frequently-asked questions.

USEPA (2007) has published a message mapping guide entitled “Effective Risk and Crisis Communication During Water Security Emergencies: A Risk Communication and Message Mapping Guide for Water Sector Utilities.”

PUBLIC NOTIFICATION

In the event that a believable threat exists that a public drinking water supply has been accidentally or intentionally contaminated, the public needs to

Table 16-2. Sample message map

| Credible Threat of Contamination of the Municipal Water Supply | | |
|---|--|---|
| Stakeholder: Public/Media | | |
| Question or Concern: What has happened | | |
| Key Message 1: Police have informed us of a credible threat of an attack against the water supply. | Key Message 2: The threat involves an unknown location. | Key Message 3: The threat involves an unknown contaminant. |
| Supporting information 1-1: Information indicates that the city water system is the target. | Supporting information 2-1: We have elevated our security level. | Supporting Information 3-1: We have increased our sampling and monitoring efforts. |
| Supporting information 1-2: We have activated our ERP. | Supporting information 2-2: We are working closely with law enforcement. | Supporting information 3-2: We are conducting these activities with the Health Department. |
| Supporting information 1-3: We are working closely with emergency response organizations and local officials. | Supporting Information 2-3: We encourage the public to report any suspicious activity to local police. | Supporting information 3-3: We have found no indication of an attack so far, but the investigation is continuing. |

be notified so that they can avoid exposure to the suspect water. In the *Response Protocol Toolbox for Planning for and Responding to Drinking Water Contamination Threats and Incidents* (USEPA 2004), the USEPA recommends that the public be notified once a threat has been determined to be credible by the responsible officials.

Public notification in response to a drinking water contamination threat or incident may be required under the Public Notification (PN) Rule (CFR Part 141, Subpart Q). Specifically, this rule requires public notification in a “situation with significant potential to have serious adverse effects on human health as a result of short-term exposure” as determined by the primacy agency in its regulations or on a case-by-case basis. In the PN Rule, this is referred to as a Tier 1 public notice. The means used to notify the public can also be specified by the regulatory agency. In some states, notification must be made not only through media announcements but through more effective, higher technology methods such as auto-dialer telephone systems, reverse 911 systems, or email messages.

In addition to notifying the public of a drinking water contamination event, public advisories are issued to prevent additional exposure of the public to the contaminants. Advisories range from “boil water” notices, to “do not drink,” and in very serious circumstances, “do not use” advisories. Because

a “do not use” advisory could potentially interfere with fire protection, it is important that the most appropriate advisory be delivered to the public. Module 5 of the *Drinking Water Response Protocol Toolbox* provides extensive guidance on selection of the proper advisory. Additionally, the CDC, in conjunction with the USEPA and the AWWA, is developing a Drinking Water Advisory Toolkit that can be used by state and local health and drinking water authorities who are responsible for issuing drinking water advisories (AWWA 2009). The toolkit will provide guidance on when to issue an advisory, how to identify target audiences, and how to overcome communications challenges related to dissemination, comprehension, and implementation of an advisory message. Information on the toolkit is available at zdq8@cdc.gov or jcw3@cdc.gov.

NATIONAL COMMUNICATIONS SYSTEM

In addition to a need for effective communications between emergency management officials and the public during an emergency, it is also critical that government agencies, response organizations, infrastructure officials, and other key response partners be able to communicate with each other. Landline and wireless communications often become congested during major emergencies.

The National Communications System (NCS) was formed in 1963 in response to communications deficiencies experienced during the Cuban Missile Crisis in 1962. NCS became part of the DHS in 2003. The NCS mission, as defined by Executive Order 12472, is to provide priority telecommunications services and other related programs to support national security and emergency preparedness efforts across federal, state, and local government; critical infrastructure industries; and other authorized organizations. NCS services support the initiation, coordination, and restoration of national security/emergency preparedness telecommunications during crises, terrorist attacks, or natural disasters. Access to these services, described as follows, is available to key national security/emergency response personnel at the federal, state, local, and tribal levels of government, as well as in critical infrastructures such as drinking water and wastewater. Information about NCS services and programs are available on the NCS Web site at www.ncs.gov/services.html.

The Government Emergency Telecommunications Service (GETS) is an NCS landline priority service that provides emergency personnel access and priority processing in the public telephone network during an emergency event when the probability of completing a phone call significantly decreases. Subscribers use a calling card that triggers priority treatment over the general public by dialing a unique access number and entering a PIN. Emergency responders receive priority by having their calls queue to the first available lines. More information about GETS is available at www.gets.ncs.gov.

The Wireless Priority Service (WPS) is the NCS nationwide wireless counterpart to the GETS program and provides emergency responders with similar priority treatment if they experience high levels of congestion when dialing from their cell phones. WPS provides priority for calls originating from cell phones through a combination of special cellular network features and provides the same high probability of completion capability achieved by GETS. Most importantly, WPS addresses congestion in the local cell, which is often the reason why cellular calls cannot be completed during heavy calling periods or when damage to network infrastructure occurs. WPS allows authorized personnel to gain access to the next available wireless radio channel in order to initiate calls during an emergency. Subscribers invoke the WPS service by dialing a unique access code before entering their destination number. Additional information about WPS is available at www.wps.ncs.gov.

CONCLUSIONS

Effective communications during a crisis can go a long way toward protecting public health and improving the overall emergency response effort. The scientific application of crisis communications methods is a legitimate tool for response and recovery, just like any other resource applied during a disaster. Crisis communications is not an attempt at mass mental therapy or an attempt to deliver propaganda or spin to the public. Rather, it is a reasoned communication approach to the selection of the appropriate message, messenger, and method of delivery for intended audiences. Effective crisis or risk communications can be a resource multiplier during a response effort.

Dr. Julie Gerberding was appointed director of the CDC following the mailborne anthrax attacks in the autumn of 2001. The anthrax attacks drew a great deal of public attention to the CDC and its role as an official emergency communicator during national public health emergencies. In an interview following her appointment, Dr. Gerberding was asked if she had an ideal crisis communicator that she might emulate. Her response, obviously referring to the 9/11 events in New York City, was quite interesting:

“I think that Mayor Rudy Giuliani is a role model of effective communications during a crisis. What I observed about his communication was that he was consistently there with news. He read the news, he told the truth, he said what he knew when he knew it and he told people what he didn’t know and what they were doing about it. He communicated a very strong message of empathy that came across as sincere and heartfelt. If people can identify with a spokesperson as someone who cares—someone who is not just there providing the most recent sensational information—it can go a long way. Your credibility as a communicator will be enhanced.”

REFERENCES

- American Water Works Association (AWWA). 2009. Drinking Water Advisory Toolkit Under Development. *Jour AWWA*, 101(2):120.
- Centers for Disease Control and Prevention (CDC). 2002. Synergy CD. Atlanta, Ga.: CDC.
- Covello, V.T. 2005. Risk Communication, Message Mapping, and Bioterrorism: A New Tool for Communicating Effectively in Public Health Emergencies and Crises. *Bioterrorism Preparedness and Response*. San Francisco: Jossey-Bass.
- Covello, V.T., R.G. Peters, J.G. Wojtecki, and R.C. Hyde. 2001. Risk Communication, the West Nile Virus Epidemic, and Bioterrorism: Responding to the Communication Challenges Posed by the Intentional or Unintentional Release of a Pathogen in an Urban Setting. *Jour. Urban Hlth.*, 78:382.
- Minamyer, S. 2008. Effective Crisis Communication During Water Security Emergencies. *Jour. AWWA*, 100(9):180.
- US Environmental Protection Agency (USEPA). 2003–2004. *Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents*. Washington, D.C.: USEPA. www.epa.gov/safewater/watersecurity/pubs/guide_response_overview.pdf.
- USEPA. 2007. *Effective Risk and Crisis Communication During Water Security Emergencies*. Washington, D.C.: USEPA. www.epa.gov/nhsr/pubs/600r07027.pdf.

EMERGENCY RESPONSE TRAINING

The Bioterrorism Act of 2002 required drinking water utilities serving more than 3,300 people to conduct a VA, and based on what was learned in the VA, develop or upgrade an existing ERP to cover the utility's response to manmade emergencies such as terrorism. Although wastewater utilities were not mandated by federal regulation to conduct VAs or modify ERPs, many of them have voluntarily taken the same action.

While excellent response plans can be prepared, the plan alone cannot guarantee an effective response to an emergency. The plan is only as good as the people who must execute it. And, the best way to ensure their performance is to make sure that they have been adequately trained on the plan and have participated in exercises using the plan. Utilities are concerned with accidental situations and natural disasters as well as emergencies of human origin. Training and exercising the various components of an ERP will improve the utility's ability to deal with all of these contingencies.

EXERCISES

All utility personnel must know their duties during various emergencies, and key personnel need to be well versed on the entire ERP. Familiarity with the plan can be achieved by reading the plan or through classroom training or briefings on its content. But merely being familiar with the plan does not guarantee a successful response in a crisis. Utilizing the plan during exercises has a number of benefits. For example, organization personnel can test the ERP and identify gaps in planning. Key staff can improve their ability to make critical decisions in a timely manner and with limited information. And exercise participants can role-play collaborative problem solving in a stressful situation. Exercises give the players an opportunity to practice responses

and make mistakes in situations that do not affect public health and safety. Finally, exercises give utility employees an opportunity to establish contacts and build working relationships with public safety personnel, health officials, and regulatory agency representatives who would likely play a role in responding to utility emergencies.

Tabletop Exercises

Several levels of tabletop exercises can be utilized to practice emergency response. These vary in intensity and may be used in a serial fashion, beginning with the simplest type of exercise and progressing to the more complex.

The simplest tabletop exercise is the *roundtable discussion* which convenes a limited number of utility personnel to discuss responses to hypothetical scenarios. These personnel may include the utility director and the public information officer as well as the chiefs of the various sections including operations, distribution or collection system, water quality, treatment plant, engineering, and security. Roundtable discussions are especially useful when a utility is updating its ERP. These training events are simple, inexpensive, and are ideal forums for brainstorming new ideas.

A more complex tabletop exercise is the *simple functional exercise* in which utility personnel are joined by representatives from other governmental and nongovernmental organizations who would also be involved in a response to a water emergency. This may include public safety responders, law enforcement personnel from various levels of government (including the FBI), emergency management officials, health department representatives, regulatory agency personnel from the state and federal levels, and elected officials.

Again, participants gather around a table and discuss scenarios, agency capabilities and responsibilities, and response actions. The exercise could involve a general discussion, or could be driven by a hypothetical scenario. If a scenario is involved, the players will have the opportunity to propose response actions for their organizations and then discuss these responses as a group.

The next level of tabletop complexity may be termed an *enhanced functional exercise*. As in the simple functional exercise, representatives of all agencies that would respond to an emergency should be represented. However, in the enhanced exercise, participants are given a chance to interact with each other in response to a hypothetical scenario in a similar fashion to how they would interact in a real crisis. A particular advantage to this approach is the opportunity to practice interagency communications, which is especially effective if the functional agencies can be physically isolated from each other, as in a real-life situation, rather than gathered around a single conference table. Communications can be conducted by written message, telephone, or radio.

This is an excellent opportunity to actually rehearse a combined agency response. Because of the complexity of the training environment, this type of exercise requires significantly more planning and coordination than the

exercises described earlier. Because a detailed scenario may be involved, with multiple, staged “injects” of information to the various agencies involved in the exercises, the use of third-party exercise facilitators is beneficial. A number of these exercises have been conducted across the United States during the past several years, including those sponsored by industry organizations, the military, and the USEPA (Whelton et al. 2006).

Full-Scale Exercises

The ultimate exercise is the full-scale, scenario-driven emergency response drill. Full-scale exercises test the effectiveness of emergency management plans in an interactive manner over a substantial period of time. This training involves mobilization of personnel and resources and the movement of emergency responders, equipment, and resources to demonstrate emergency coordination and resource capability. Emergency operations centers and incident command posts may be established, and usually outside agencies are extensively involved. This training event is significantly more costly and requires a great deal more preplanning, than tabletop exercises. The DHS has held a number of large, full-scale exercises, including the Top-Off series. While the Top-Off series hasn’t focused on drinking water or wastewater emergencies, utilities and water regulatory agencies have participated.

In reality, water contamination scenarios do not lend themselves to full-scale exercises to the same extent as airline crashes, physical assaults on buildings, airborne bioterrorism events at sporting events, and other man-made emergencies. Physical destruction of a utility’s assets would be more comparable to these situations. Drinking water or wastewater contamination scenarios typically do not center on a well-defined incident site, but rather involve more widespread portions of a community water system potentially affected by a contaminant. For this reason, emergency response exercises for water incidents can usually be conducted effectively at a tabletop level.

In 2008, USEPA, under its Water Security Initiative (WSI), conducted a full-scale exercise of the Greater Cincinnati Water Works contamination warning system and associated consequence management plan (Fencil and Hartman 2009). The exercise was a scenario-driven simulation that implemented the Cincinnati water utility and local response partner agency protocols for detecting and responding to a drinking water contamination incident. More than 50 people from 10 agencies participated in this large-scale exercise.

PRE-EXERCISE TRAINING

Typically, not all participants in a tabletop exercise have the same level of background knowledge. For example, emergency planners and public safety personnel are often better trained in topics such as NIMS and ICS than are utility personnel. Utility personnel can familiarize themselves with NIMS and ICS through online courses offered on the FEMA Web site at www.fema.gov/emergency/nims/. However, emergency planners and public safety

personnel have usually never received any orientation on the workings of wastewater or drinking water systems. To remedy this imbalance, it is useful to devote some time prior to the exercise to background briefings on topics such as the USEPA Response Protocol Toolbox, ICS, and the basics of drinking water treatment and distribution, as well as wastewater collection and treatment. Information should also be provided to the group beforehand on the roles that would be played by the various agencies responding to a water emergency. Each participating agency, such as the FBI, National Guard Civil Support Team, and health department can give short presentations on their roles. These presentations also provide everyone with an opportunity to get to know their counterparts in the other organizations prior to an actual emergency situation.

CONDUCTING THE EXERCISE

Prior to the actual start of tabletop or full-scale exercises, the facilitator should provide background scenario information to the players. This may include information on the real or hypothetical community in which the event occurs, such as details concerning the drinking water and wastewater systems, medical and public health resources of the community, and capabilities of various response agencies in the area.

Scenario-driven tabletop exercises usually run for several hours. To increase the amount of play, time is often condensed. For example, a three-hour exercise can cover a 12-hour scenario period if every 15 minutes of real-world time represents one hour of scenario time.

Scenario-driven exercises usually begin with initial injects provided to appropriate player cells by the exercise facilitator. These could include reports to the health department of unusually large numbers of patients being seen in local hospital emergency rooms, reports to the utility of gasoline-like odors emanating from sewer manholes, or calls to police concerning trespassers on utility property. Following the initial inject, the various player cells must analyze the information, contact and consult with other agencies, and take appropriate response actions.

Response actions for a contamination event can include isolation of reservoirs or tanks suspected of being contaminated, notification of the public, requesting information or assistance from other response agencies, and issuance of public advisories. Players should be encouraged to treat the artificial scenario as if it were a real event occurring in their community. They should also be encouraged to use their organization's ERP to test its suitability for the scenario. Additional injects can be provided to various players by the exercise facilitators as the flow of the exercise dictates. Players should be advised to document events, communications, and response actions throughout the exercise. USEPA's Response Protocol Toolboxes contain a number of example documentation forms that can be used in an imaginary or real-world emergency situation.

A number of appropriate scenarios for tabletop exercises involving drinking water and wastewater utilities have been developed by USEPA (USEPA, 2005). Manmade emergencies may include, among others, physical or cyber attacks on utilities, intentional release of harmful treatment chemicals such as gaseous chlorine or ammonia, the addition of toxins or pathogens to drinking water distribution systems, or the discharge of flammable liquids into wastewater collection systems. However, scenarios do not have to be restricted to malevolent acts. There is excellent training value in scenarios involving accidental events such as fires at utilities, tractor-trailer spills of hazardous materials in the watershed, and natural disasters such as floods or hurricanes. These events are undoubtedly more likely to occur in water utilities than are acts of terrorism.

Throughout the exercise, facilitators should distance themselves from the actual play but make themselves available for procedural questions. In a real-world emergency, facilitators will not be available to offer advice on the best response.

A critical component of crisis response is communications with the public. Especially now, in the age of 24-hour news reporting, the media and public are likely to become aware of situations earlier rather than later. Once aware of a problem, the media will be requesting additional information. Responders from all agencies need to discuss ahead of time how information will be disseminated to the public. A tabletop exercise is an excellent setting for practicing this aspect of emergency response.

An important consideration in the conduct of exercises is how to handle sensitive information. If an exercise involves multiple water utilities, it may not be prudent to discuss details of an individual utility's ERP because it may reveal specific vulnerabilities of the system. In this case, participants on a utility player team can discuss possible utility responses based on their collective experience and judgment. Additionally, facilitators should stress to all participants that while classified information will probably not be used during an exercise, discussions of water system vulnerabilities in general may still involve industry sensitive information and should be handled with professional discretion and kept within professional circles. If revealed publicly, such information could be used to enhance the believability of a hoax threat or provide ideas to individuals contemplating a malevolent act.

The majority of tabletop exercises during the past several years have been training opportunities rather than tests. In these exercises, as in real-world incidents, more than one response may be appropriate. In most cases, an effective response will depend on the execution of a well thought-out ERP guided by informed professional judgment. A suitable response in one city or state may not be appropriate in another section of the country where regulations, SOPs, and resources may be different.

ADDITIONAL TRAINING DURING THE EXERCISE

The objective of tabletop and full-scale exercises is to rehearse utility and agency responses to an emergency situation. An important aspect of the multi-agency response is the coordination of efforts of the various organizations that will participate in the response to a major event. The basic mechanism for coordinating multi-agency response at the actual site of the event is the ICS. The accepted structure for coordinating multi-agency support for the overall response is the EOC. While detailed ICS and EOC training is available through FEMA and other sources, basic ICS and EOC principles can be reviewed before the start of a tabletop exercise.

In the series of tabletop exercises conducted throughout the nation by USEPA during the past several years (Whelton et al. 2006), both a Unified Command and an EOC were activated as part of each exercise. The Unified Command, an important structure within the ICS, included representatives of the major organizations participating in the exercise and was responsible for overall decision making during the scenario response exercise. At the end of the exercise, the Unified Command team presented a situation briefing and incident objectives to the other participants in the exercise. Similarly during the exercise, the EOC was responsible for coordinating support for the Unified Command's efforts.

The EOC was also tasked with presenting a mock press conference to the other players. Participants in the EOC included elected officials and representatives from the emergency support functions typically present at a city or county EOC (e.g., public safety, public works, medical staff). While implementation of a Unified Command and EOC during tabletop exercises is certainly no substitute for formal training on the subjects, their inclusion in the utility tabletop exercise provides an introduction to participants who may not have been previously exposed to these concepts and a review for participants who have already received formal training.

HOT WASH

Another key component of exercises, especially scenario-driven exercises, is an after-action review or "Hot Wash." Throughout the course of a long exercise, many participants will not be aware of event interpretations and responses made by other participating agencies. An open discussion session following the end of the exercise, in which the progress of the exercise is discussed, inject by inject, gives all of the players an opportunity to see the big picture. It also gives all of the participants a chance to discuss the responses taken by the various organizations participating in the exercise. The Hot Wash is often the best opportunity for a useful exchange of information between responding agencies. The discussion is enhanced if it is conducted in a positive manner without criticism of the actions of any specific group. The exercise facilitator can play an important role in moderating this exchange.

The Hot Wash discussion works best if it closely examines what went right and what went wrong during the exercise. In particular, the group should try to determine if and when communications broke down and how this can be prevented in the future. Poor communications is a common problem in managing real-world emergencies. If participants disagree about how a situation or a response was handled, the facilitator should encourage group discussion in an attempt to reach a consensus on what the best course of action should have been. The participating agencies should try to identify any weaknesses in their organizations' ERPs and discuss how these shortfalls can be eliminated. The group should also try to identify additional procedures, interagency agreements, or policies that may be needed to deal with real-world emergencies.

GUIDANCE MATERIALS

Guidance materials are available to assist utilities in planning for and conducting exercises. Moyer (2005) has described exercises that have been conducted for drinking water utilities and has provided a sample intentional contamination scenario that can be adapted and used in exercises. The Washington State Department of Health has published a planning guide on tabletop exercises for public drinking water systems (Washington Department of Health 2005). Bromberg (2006) described a drinking water tabletop exercise, based on a ricin contamination scenario that was conducted at an annual conference of the Wisconsin Water Association. USEPA released a CD containing six separate scenarios that utilities can use for tabletop exercises within their organizations and with outside response agencies (USEPA 2005). This CD not only contains the scenarios, but also includes briefing slides on topics, such as the ICS, that can be used for refresher training prior to the exercise. USEPA has indicated that they will be releasing another CD focusing on 'All Hazards' scenarios in the near future. The DHS offers training guidance through its Homeland Security Exercise and Evaluation Program (hseep.dhs.gov/pages/1001_HSEEP7.aspx). Additionally, USEPA lists available water security training courses, meetings, workshops, and webcasts at cfpub.epa.gov/safewater/watersecurity/outreach.cfm.

REFERENCES

- Bromberg, E. 2006. Contamination Events Testing Realistic Threat Scenarios. *Opflow*, 32(2):1.
- Fencil, J., and D. Hartman. 2009. Cincinnati's Drinking Water Contamination Warning System Goes Through Full-Scale Exercise. *Jour. AWWA*, 101(2):52.
- Moyer, J. 2005. Tabletop Exercises: How You Can Use Them to Prepare for Water System Incidents. *Jour. AWWA*, 97(8):52.
- US Environmental Protection Agency. 2005. *Emergency Response Tabletop Exercises for Drinking Water and Wastewater Systems*. USEPA 817-C-05-001. Washington, D.C.: Office of Drinking Water and Groundwater. www.epa.gov/safewater/watersecurity/tools/trainingcd.

- U.S. Public Law 107-188. 2002. *Public Health Security and Bioterrorism Preparedness and Response Act. Title IV: Drinking Water Security and Safety.* Washington, D.C. www.fda.gov/oc/bioterrorism/PL107-188.html#title4.
- Washington Department of Health. 2005. *Tabletop Exercise Planning Guide for Public Drinking Water Systems.* DOH 331-279. Olympia, Wash.: Office of Drinking Water. www.doh.wa.gov/ehp/dw/Security/Training.htm.
- Whelton, A.J., P.K. Wisniewski, S. States, S.E. Birkmire, and M.K. Brown. 2006. Lessons Learned From Drinking Water Disaster and Terrorism Exercises. *Jour. AWWA*, 98(8):63.

REMEDIATION AND RECOVERY

As discussed in earlier chapters, any number of intentional acts, natural disasters, or accidents could negatively affect public water systems. Given the importance of drinking water and wastewater services to a community, it is critical that damages be repaired and a utility be brought back into full operation as soon as possible following an event that disrupts service. In fact, in a community devastated by a major disaster such as a hurricane, tornado, or flood, rapid restoration of water and wastewater services can be a key element in restoring hope to people.

An excellent account of the experiences of the Cleveland Division of Water in recovering from the Northeast Blackout of 2003, and the experiences of New Orleans and Pensacola, Fla. utilities, in recovering from the hurricanes of 2005 and 2006 is presented in a DVD produced by AWWA (2009).

DECONTAMINATION OF WATER SYSTEMS

While many drinking water and wastewater utilities have had experience in recovering from damages inflicted by major mechanical failures, accidents, or natural disaster, fewer have had to recover from an accidental or intentional contamination event.

Decontamination is an important aspect of recovery from a contamination event. For drinking water systems, this could include decontamination of contaminated raw water that may be present in source water impoundments, partially treated water within the treatment plant, or finished water in reservoirs, tanks, or transmission lines within the distribution grid. In the case of wastewater systems, this may include decontamination of untreated

sewage in the collection network or partially treated wastewater within the POTW. Decontamination of the infrastructure itself (pipes, storage tanks, reservoirs, pumping stations) is also important.

A number of critical questions arise when remediation and recovery of contaminated water systems must be considered. Some of these have to do with the fate and transport characteristics of specific contaminants. For example, is a particular contaminant soluble enough in water to have been transported throughout a drinking water distribution or wastewater collection system? Is a specific contaminant stable or does it spontaneously hydrolyze in water, or oxidize, or in the case of pathogens, become inactivated in the presence of chlorine? Does a certain contaminant adhere to pipe surfaces, especially those encrusted with corrosion products, scale, and biofilm?

Still other issues concern the effects of the decontamination process itself. Specifically, are the breakdown products of some contaminants more toxic than the original contaminant, and could certain decontamination procedures actually produce an even more dangerous condition? Many of these questions remain unanswered for a majority of the contaminants that may intentionally or accidentally contaminate drinking water and wastewater systems.

A source of information on contaminant-specific decontamination is the USEPA Water Contaminant Information Tool (WCIT) database (Weisman and Jayasundera 2006). At the time this handbook was published, WCIT contained decontamination recommendations for 102 chemical, biological, and radiological contaminants, gathered from peer-reviewed sources such as USEPA's NHSRC, the US Department of Defense, and open literature journal articles.

WCIT contains decontamination information for microbial contaminants, biotoxins, inorganic and organic chemicals, chemical warfare agents, and radionuclides. The contaminant-specific decontamination section of the database includes information on decontamination techniques (e.g., flushing, sand blasting, use of surfactants and chelating agents); effectiveness of removal from specific types of materials (e.g., ductile iron, concrete, copper); and residuals generated by the decontamination process.

The decontamination procedures chosen must factor in infrastructure that may be highly tuberculated with scale, corrosion, or biofilm. Internal pipe surfaces with these characteristics may be particularly difficult to decontaminate. WCIT also contains information on the fate and transport characteristics, health effects, toxicity, and infectivity of various contaminants.

Research during the past several years has increased the body of knowledge on decontamination issues. A number of reports in the open literature suggest the types of treatment processes that might be effective for decontamination of water systems, and how effective these treatments might be. For example, Burrows and Renner (1999) reported that botulinum toxins are more than 99.7 percent inactivated by 3 mg/L free chlorine in 20 minutes, and 84 percent inactivated by 0.4 mg/L free chlorine in 20 minutes. They

reported the results of one military-sponsored study that demonstrated more than 99.988 percent removal of botulinum toxins from spiked raw water using the process of reverse osmosis (RO). The authors also suggested that treatment systems utilizing charcoal filtration should be effective in removing botulinum toxins.

Burrows and Renner indicated that ricin is more than 99.4 percent inactivated after 20-minute contact with free chlorine at 100 mg/L, but is essentially unchanged at 10 mg/L. They also stated that RO is more than 99.8 percent effective in removing ricin from water, but coagulation–flocculation is relatively ineffective. They further speculated that carbon filtration should effectively absorb ricin, but presented no experimental data.

In the same report, the authors noted that the *B. anthracis* spore is stable in pond water for periods of at least two years. The spore is highly resistant to inactivation by chlorine, but could be removed by filters having a pore size smaller than 1 µm, which is the typical diameter of anthrax spores.

A practical approach to decontaminating water during an emergency is the use of portable field units. A unit currently undergoing testing is the expeditionary unit water purifier (EUWP). This skid-mounted device is readily transportable. Treatment includes UF, RO, and chemical feed for pre- and posttreatment. Daily treatment production goals are 100,000 gallons of water per unit. The EUWP was initially designed for military use and is fashioned after the RO water purification units that the US military has used in the field for a number of years.

While the EUWP was initially intended for military applications to meet Tri-Service Field Water Quality Standards (Army, Navy, Air Force) for short-term consumption by healthy soldiers, the technology is expected to be capable of meeting USEPA National Primary Drinking Water Regulations. Such a unit could be deployed by federal or state agencies to provide potable water to a community following a disaster, and could be used to treat water that contains high dissolved solids, turbidity, or even hazardous substances. This device might also be used for treating contaminated drinking water contained in a municipal distribution system prior to disposal, or wash water produced during decontamination of contaminated buildings and equipment.

DECONTAMINATION OF INFRASTRUCTURE

How well pathogens survive in municipal distribution systems, and what decontamination measures are required to reclaim the water supply infrastructure, are additional issues that need to be considered following an accidental or intentional biological contamination event. Infrastructure that may have been affected includes water mains, pumping stations, reservoirs, and storage tanks that are part of the public water system, as well as the plumbing systems within individual homes and buildings.

In a study conducted at the US Air Force Research Laboratory (Aberdeen Proving Ground, Maryland), Calomiris (2006) investigated the ability of

anthrax spores to survive passage through a plumbing system, resist traditional drinking water disinfection methods, and adhere to and contaminate pipes. In this study, *B. anthracis* spores suspended in municipal chlorinated tap water were circulated through a model plumbing system. The investigators observed minimal inactivation of spores during a 15-hour period of passage through the pipe loops. Susceptibility to traditional drinking water disinfection levels was further studied by exposing spores to various concentrations of chlorine for different periods of time. Calomiris found that following 60 minutes exposure to 1 mg/L chlorine (a residual greater than that found in most municipal distribution systems), there was no significant decrease in the number of viable spores. Under these same conditions, one minute exposure typically inactivates 99.99 percent of other waterborne pathogens that do not exist as spores in the environment. Higher concentrations of chlorine were more effective. At 5 mg/L, 97 percent of spores were inactivated after one hour exposure, while at 10 mg/L, 99.99 percent of spores were inactivated.

Calomiris also examined the tendency for anthrax spores to attach to the inside of pipes by running contaminated water in a continuous loop through sections of pipe made of either copper, PVC, or galvanized iron. After six hours of recirculation, 20 to 40 percent of spores had attached to the surface of the copper and PVC pipes, while 95 percent attached to the iron pipes. When biofilms were present on the interior of copper pipes, attachment increased to 80 percent.

The results of this study suggest that anthrax spores can survive passage through a plumbing system and therefore most likely a municipal distribution system, and can tolerate typical drinking water chlorine residuals. A portion of the spores would be expected to attach to pipe surfaces or biofilms within pipes, while the rest could pass through the pipe system to reach the consumer tap.

Welter and colleagues (2005) conducted a bench-scale study of decontamination of drinking water system infrastructure. The study investigated the effectiveness of a number of decontamination methods in removal of several types of contaminants from drinking water distribution system pipe surfaces. Contaminants included: inorganic chemicals (cyanide, mercury, arsenic, and surrogates of radioactive isotopes such as cesium, strontium, cobalt, and thallium), organic compounds (chlordan and *para*-dichlorobenzene), and microbes (*Bacillus thuringiensis* and MS2 bacteriophage). In these experiments, the researchers used 12-inch lengths of pipe sections of various materials.

In studying the adherence of contaminants on various pipes, the researchers observed no significant adsorption of cyanide, arsenic, mercury, or MS2 bacteriophage on any of the pipe materials tested. They found greater than 5 percent of cesium, strontium, cobalt, and thallium attached to iron, new galvanized pipe, and galvanized iron already containing a biofilm. They also reported that chlordan, and to a lesser extent para-dichlorobenzene, adsorbed to all pipe surfaces except cement-lined ductile iron, and epoxy-coated steel pipe.

When examining the effectiveness of chlorine decontamination on *Bacillus* spores at various contact times (CT values), the investigators observed poor inactivation of spores attached to tuberculated galvanized pipe. The highest removal efficiency obtained was only 84 percent with a very high CT application of 30,000 mg/L-min. These results clearly demonstrate the difficulties associated with removal of microbes from complicated pipe surfaces as compared with inactivation of microorganisms in bulk water.

Welter and colleagues also reported a number of observations on removal of inorganic and organic contaminants from pipe surfaces. These included removal efficiencies ranging between 18 percent and 56 percent for strontium and cesium using Simple Green, a commercially available decontamination agent, and highly variable removals of organic compounds by several commercially available surfactants.

In addition to removal efficiencies for various contaminants and decontaminating agents, another practical question is: how can officials be sure, and be able to convince the public, that all contaminants have been removed and the plumbing system is now clean enough to convey safe, potable water? Public perception is an important aspect of what is safe. Following the anthrax attacks on the US Postal System in 2001, the criterion used to determine that a building had been successfully decontaminated was the presence of no culturable spores. Existing data certainly suggest that more than just a few spores are required to cause an anthrax infection. However, the public fear generated by the intentional anthrax attacks led to the adoption of extremely low tolerance levels for the presence of this contaminant. It is likely that a similar public reaction would occur following a chemical, radiological, or biological attack on a public or building water system.

DECONTAMINATION PROCEDURES

Should it become necessary to decontaminate pipes, storage tanks, reservoirs, pumps, or treatment plants; plumbing systems within homes or buildings; or contaminated drinking water or wastewater, a number of approaches are currently available. For the most part, these techniques have been used for years for routine refurbishment of drinking water and wastewater infrastructure, as well as for routine treatment of drinking water and wastewater.

Several procedures can be used for contaminated pipes in the distributions system.

- *Flushing.* Large volumes of water are flushed through the contaminated pipe and water, sediment, and contaminants are discharged through open fire hydrants or blowoffs.
- *Air scouring.* Surges of air and water through the pipes combine to dislodge more recalcitrant contaminants.
- *Chemical cleaning.* Various chemicals dissolve or desorb contaminants from the inner surfaces of pipes and associated tuberculation. Chemical decontaminants may include disinfectants, oxidants, acids, sequestering agents, and surfactants.

Denver Water has devised a trailer-mounted ozone system for disinfecting water mains (Dahm 2009). While this device is routinely used in the Denver distribution system for disinfecting mains following installation or repair, the designers believe that it would also be useful for decontamination following an accidental or intentional contamination event.

- *Pigging or swabbing.* Water pressure is used to force a plastic scouring device or swab through a section of pipe to remove contaminants as well as biofilm, scale, and corrosion products.

A number of decontamination techniques could be utilized for contaminated storage tanks, reservoirs, and equipment:

- *Grit blasting.* Sand, metal shot, or dry ice is propelled against a contaminated surface using compressed air.
- *High-pressure spray.* A high-pressure stream of water is directed toward the contaminated surface. The spray is forceful enough that it can remove encrustation as well as contaminants adhering to the surface.
- *Chemical cleaning.* Chemicals, such as oxidants, acids, bases, and surfactants can be used to decontaminate surfaces. Foams may be applied to increase contact time with the contaminated surface.

In a worst-case scenario, portions of a contaminated infrastructure may actually have to be abandoned and replaced. This may be required if the previously discussed techniques cannot remove the contaminant or if contaminant removal poses an unacceptable risk to the workers performing the decontamination or to the public.

In the case of contaminated drinking water, sewage, or the wash water resulting from the decontamination processes described for drinking water or wastewater infrastructure, a number of conventional and emerging water treatment techniques can be used to treat the water prior to disposal. These include

- Chlorination
- Coagulation and sedimentation
- Adsorption
- Ion exchange
- Distillation
- Conventional filtration
- Membrane filtration
- Oxidation
- Air stripping
- Reverse osmosis

REMEDIATION AND RECOVERY RESEARCH

A number of research projects are being carried out to develop improved techniques for decontaminating water as well as pumping, storage, and transmission structures. These projects are being sponsored by the National Institute of Standards and Technology (NIST), the Water Research Foundation (formerly the Awwa Research Foundation) and others. USEPA's NHSRC is conducting decontamination research in five areas:

- Decontamination and treatment protocols and technologies
- Agent fate and transport
- Persistence of contaminants in pipes and infrastructure (including transformation by-products)
- Development of appropriate cleanup levels and verification methodologies
- Disposition of contaminated water or wastewater associated with the decontamination process (including drainage from personnel decontamination showers)

The Critical Infrastructure Partnership Advisory Council (CIPAC) formed a Water Sector Decontamination Working Group, consisting of government agency and utility representatives, to identify key issues for decontamination of water systems. The group considered decontamination challenges ranging from the treatment plant to finished water storage tanks and distribution system, to residential and nonresidential property water systems. They also considered decontamination problems for wastewater systems, including both the collection system and the treatment process. CIPAC issued a report in 2008, *Recommendations and Proposed Strategic Plan: Water Sector Decontamination Priorities*, which listed the following priority decontamination issues that need to be addressed through additional research and other efforts:

- Containing and disposing of large amounts of contaminated water
- Near-term practical solutions
- Decontamination procedures for treatment plant infrastructure
- Decision-making frameworks for decontamination
- Decontamination procedures for distribution and collection systems
- Training and outreach to utilities, partners, and stakeholders
- Utility communications to public officials, responders, and the public regarding decontamination
- Clean-up levels
- Treatment procedures for contaminated drinking water and wastewater
- Agent fate and transport
- Clarifying roles and responsibilities for decontamination and treatment
- Process for regulatory waivers and suspensions
- Resources and assets for decontamination and treatment
- Laboratory analysis

- Health and safety assessment for drinking water and wastewater treatment plant and field staff
- Overarching decontamination needs

DECONTAMINATION OF WASTEWATER SYSTEMS

A special scenario of concern for wastewater system operators is the possibility that should people, buildings, or other structures in the community become contaminated as a result of a chemical, biological, or radiochemical (CBR) incident, wastewater from subsequent decontamination efforts may find its way into the municipal sanitary or stormwater collection and treatment systems. Such an event could affect wastewater utility employees, the public, the infrastructure, wastewater treatment, and the environment. The National Association of Clean Water Agencies (NACWA) has published a guidance manual for response to such an event (NACWA 2005). Some of their recommendations are described here.

Several types of decontamination may be required, depending on the extent of the attack. If victims need to be decontaminated, this would obviously receive the highest priority and should begin as soon as practical and as close to the incident site as safety concerns permit. Decontamination would involve removal of clothing and washing the body with or without soap. Victims may walk through a decontamination shower, some of which are designed as portable units. Some victims may be decontaminated using equipment installed at hospital sites.

Alternatively, decontamination might be improvised using water spray from fire hoses or garden hoses. Decontamination units designed for this purpose are often equipped with a pool or sump to collect the spent wash water, which can then be transferred to a holding tank prior to being decontaminated and disposed of properly. However, in the case of improvised decontamination facilities, and even some hospital decontamination stations, wastewater may drain directly to the sanitary or stormwater sewer system.

Decontamination of structures, vehicles, equipment, and other items exposed to CBR agents will usually be conducted after victims have been cared for, and should be carried out with more deliberate planning. Methods used may include water (with and without detergents), high-pressure steam, surfactants, oxidizing chemicals, caustic chemicals, or emulsions. Wastewater generated by these processes should be contained using dikes or sorbents. Subsequent treatment and disposal of this wash water should be carried out in a safe and planned manner.

Measures to contain decontamination wastewater will always be secondary to the protection of life and safety, as noted in a FEMA publication (2003): "In a mass casualty setting, life safety takes precedence over containing runoff." Furthermore, where CBR attacks result in numerous victims, over a widespread geographic area, or ignite fires, containment of

decontamination wastewater may be impossible. USEPA has stated that runoff from a decontamination event is not considered an act of negligence when emergency responders undertake the necessary actions to save lives or protect the public. However, USEPA's position on contaminated runoff does not eliminate the responsibility to control the flow of water into the local environment. After the imminent threats to human health and safety are addressed, all reasonable efforts to contain the contamination or mitigate the contamination should then be taken (USEPA 2000).

Still another major source of contaminated wastewater could result from intentional or accidental contamination of a municipal drinking water system. Large quantities of water may have to be drained from the drinking water distribution system or storage tanks and reservoirs. Because of the urgency of returning drinking water systems to service for fire protection, this water may be directed to sanitary or stormwater sewers, along with any other drinking water inadvertently released from the public water supply. In such an event, drinking water and wastewater officials should coordinate their efforts to reduce the impact on the wastewater system, its employees, the public, and the environment.

Wastewater utilities should include in their ERPs measures for handling decontamination wastewater discharged to their systems. This includes decisions concerning the management of contaminated biosolids, such as cessation of land application of CBR contaminated biosolids. Additionally, wastewater utility officials should coordinate with emergency management agencies and first responders in advance to ensure that wash water containment equipment will be available and that responders are aware of the importance of preventing as much untreated discharge as possible from ending up in the municipal wastewater collection system.

Wastewater utilities should also maintain and distribute supplies and equipment, such as drain seals for stormwater inlets, which can be used to contain decontamination wastewater and reduce its impact on the public wastewater system. Personal protective equipment (PPE) also should be provided for appropriately trained utility employees who assist emergency personnel.

If wastewater contaminated with CBR agents has entered the public wastewater collection system, it may be necessary to protect utility employees from exposure until the scope of the problem is ascertained and remediation steps have been taken. Appropriate steps may include:

- Preventing personnel from entering manholes
- Preventing personnel from entering wet wells of pump stations
- Suspending manual cleaning of bar screens and removal of grit
- Restricting access to aeration basins, trickling filters, and other treatment plant locations where aerosols may be generated
- Suspending manual handling of biosolids

MUTUAL AID AMONG UTILITIES

When a natural or manmade disaster strikes a drinking water or wastewater utility, their capabilities can be overwhelmed. The expectation has been that in such an event, local, state, and ultimately the federal government will provide the necessary assistance to the utility to recover and resume service to the public. However, the experiences of Hurricane Katrina in 2005 demonstrated that government aid doesn't arrive immediately. Emergency response and recovery must begin at the utility level.

One approach to ensuring an effective response and recovery capability is the development of intrastate mutual aid agreements among drinking water and wastewater utilities. The initiative has been labeled WARN. This initiative began in 1992 with the formation of CalWARN in California where utilities were forced to deal with a variety of emergencies including earthquakes, freezes, and firestorms. Florida and Texas, two states frequently besieged by devastating hurricanes, developed FlaWARN and TxWARN agreements in 2001 and 2005, respectively. Following the mass destruction of Hurricane Katrina a concerted effort emerged among all states to develop WARN programs to assist utilities in dealing with hazards ranging from natural disasters to major accidents and malevolent acts.

The theme of the WARN initiative is "Utilities Helping Utilities." Specifically, WARN involves drinking water and wastewater utilities within a state assisting each other with personnel, equipment, and supplies in time of crisis. WARN programs can help restore critical drinking water and wastewater services to a community, especially when the community is trying to respond to catastrophic damage caused by disasters. By partnering with like-service providers with the same types of personnel and equipment, water and wastewater utilities can quickly obtain the specialized assistance that they require during an emergency.

Establishment of a signed, statewide WARN mutual aid agreement prior to an emergency provides an immediate call list for utilities seeking critical resources. The agreement also addresses difficult issues concerning legal liability and reimbursement of assisting utilities following an emergency, and facilitates subsequent reimbursement by federal agencies such as FEMA.

WARN membership is voluntary, as is the provision of specific resources by any member utility during an incident. While the primary participants in a WARN agreement are the utilities themselves, this initiative is widely supported by state and federal regulatory agencies, state and federal emergency management and homeland security agencies, and all of the major drinking water and wastewater industry associations (e.g., AWWA, WEF). AWWA, with support from USEPA, published a white paper providing guidance on formation of WARN programs (Morley and Riordan 2006). Additional information on WARN can be found at www.nationalwarn.org.

The water sector is also evaluating mechanisms to establish a national mutual aid network to connect the intrastate programs (Whitler 2007). The goal is to link existing WARN programs with the Emergency Management

Assistance Compact (EMAC) to form interstate mutual aid agreements. EMAC is an interstate mutual aid compact that has been signed by all 50 states and provides procedures for interstate mutual assistance.

REMEDIATION CASE STUDY

The most significant intentional contamination event to occur in a US drinking water system occurred in the Beechview neighborhood of Pittsburgh in 1980 (Moser 2005). In this event, a perpetrator, most likely an insider involved in an ongoing labor strike occurring at the suburban water utility, injected between 1 and 10 gallons of a solution of the pesticide chlordane, dissolved in a kerosene carrier, into an 18-inch transmission main in the distribution system. The contaminant was pumped into the transmission main, against pressure greater than 200 psi, via a pitometer tap within a curb box located in a wooded area about 800 feet upstream of the first customer tap.

While 150 people were reported to have become ill, fortunately no one was hospitalized and nobody died. However, the chlordane–kerosene mixture adhered to the pipe walls of the municipal and domestic water distribution systems and required an extensive cleanup effort. The affected distribution service zone included 15 miles of pipe containing 218,000 gallons of contaminated water.

The average concentration of chlordane measured at taps during the initial phase of the contamination event was approximately 100 µg/L with several extremely high slugs (69 mg/L and 144 mg/L) also detected. In addition to chlordane, traces of several hundred other organic compounds, associated with the kerosene carrier, were detected in various water samples collected from the distribution network.

Although this incident occurred 30 years ago, details of the remediation and recovery effort following the event provide an indication of the scale of cleanup effort that might be required to respond to a variety of accidental or intentional contamination incidents.

Water utility and public health officials first became aware of the contamination of the public water system when consumers phoned the utility and health department complaining of a kerosene–insecticide smell and taste in the tap water. Steps were quickly taken to isolate the contaminated pressure zone. Once officials confirmed that the contaminant was a mixture of chlordane and kerosene, they attempted to remove the contaminant by flushing the municipal distribution system with large volumes of finished drinking water.

Because not all pipe segments were configured so that they could be flushed, a total of 34 blowoffs were installed in the affected distribution network. Utility customers were asked to flush their domestic plumping systems with large volumes of tap water and the utility did not charge for the water. The initial public advisory instructed customers not to use the water for drinking, cooking, or bathing.

The authorities decided that once the system had been flushed to the point where chlordane concentrations reached levels less than 10 µg/L, customers would be allowed to resume use of the water for bathing. Chlordane concentrations in water samples were measured using gas chromatographic analysis. When chlordane levels were demonstrated to be less than 3 µg/L, health and utility officials advised customers that they could once again use the water for ingestion, at least for a period not to exceed one month in order to minimize customer exposure. All restrictions on water usage were finally lifted when chlordane concentrations in the water were shown to be lower than 0.05 µg/L, the detection limit for chlordane using GC.

State environmental regulatory officials decided that the flushed tap water during the remediation and recovery effort could be discharged, without prior treatment, to the combined stormwater–sanitary sewage collection system. Flushing was able to restore water use to consumers in approximately one month. However, nine months were required to eliminate all traces of chlordane from the distribution system. Samples of finished tap water continued to be tested in parts of the distribution system for the next two years. Because of the documented effectiveness of flushing, neither replacement of water pipes, nor pigging and swabbing, nor chemical cleaning were given serious consideration as decontamination options. The total cost of remediation for this episode amounted to \$469,000 (1980 dollars). This equated to \$234 per customer account.

The USEPA has developed an example hypothetical case study on decontamination and recovery (USEPA 2008). The purpose of the case study is to document the planning and experiences of a water and wastewater utility's activities related to decontamination and recovery. The utility described in the study is a large combined water and wastewater utility, located in the southeastern coastal United States.

ALTERNATE WATER SUPPLIES AND SANITARY SERVICES

A number of questions remain concerning remediation and recovery following accidental or intentional contamination of a drinking water or wastewater system. For example, what is the capability for providing an alternative water supply for both a short-term loss of service (one or two weeks) and a long-term loss of service such as one or two months? And, what measures are being taken to improve this response and recovery capability (Roberson and Morley 2005)? In the Pittsburgh chlordane contamination incident previously described, potable water was supplied to the public using water tanker trucks during the initial response and extended recovery phases. Because this contamination event occurred in the winter, the trucks had to be heated or located within heated garages.

The same question can be posed concerning short-term and long-term provision of alternative sanitation services should a public wastewater system

be put out of commission. One approach would be to provide temporary sanitary facilities in the form of portable toilets. Another approach could be to develop mutual aid agreements with nearby wastewater utilities and contracts with hauling companies to collect unaffected wastewater.

USEPA REMEDIATION AND RECOVERY GUIDANCE

Module 6 of both the *Drinking Water and Wastewater Response Protocol Toolboxes* presents guidance on the remediation and recovery process that could be applied when a drinking water or wastewater contamination incident has been confirmed.

As indicated in the Toolboxes, the purpose of the remediation and recovery process is to address extensive contamination at levels that pose immediate or long-term risks to health and the environment. The overall objective of the process is to return the water or wastewater system to service as quickly as possible while protecting public health and minimizing disruption to everyday life. The remediation and recovery protocols discussed in USEPA's Toolboxes are applicable to remediation of source water, treatment plant infrastructure, and the drinking water distribution or wastewater collection systems.

The remediation and recovery approach outlined in the Response Protocol Toolboxes is modeled on the Superfund remedial response program. The nine general steps in the remediation and recovery program are:

1. *Long-term alternate water supply or sanitary services.* During the remedial process for a drinking water system, a long-term alternate supply of potable water may need to be secured. This could include bottled water or delivery of bulk water from a neighboring utility. During remediation of a contaminated wastewater system, alternative sanitary service, such as deployment of a large number of portable toilets, may be required for an extended period of time. The need for long-term alternative water supplies or sanitary services will depend on the nature and severity of the contamination event and the length of time required to return the system to normal operation. If utility and local authorities do not have the resources to provide long-term alternative services, assistance will be required from state and federal government.
2. *System characterization–feasibility study.* After a contamination incident has been confirmed, additional information will be required to support remediation/recovery actions. A system characterization–feasibility study will provide a detailed assessment of the nature and extent of contamination and preliminarily screen candidate treatment options.
3. *Risk assessment.* On confirmation of a contamination incident, the lead agency for consequence management (e.g., DHS, FEMA, USEPA) will quickly assess the risk posed to onsite workers and the public. This rapid risk assessment will help guide response actions.

During the remedial response phase, additional risk assessments may be required to

- evaluate risk reduction achieved by the immediate operational response actions,
 - aid in establishing preliminary remediation goals, and
 - assess potential risk reduction from implementation of long-term remedial actions.
4. *Detailed analysis of alternatives for remediation.* This step involves the evaluation of various remediation approaches based on their effectiveness and technical feasibility. Remedial actions may include any of the following steps, or a combination of steps:
 - No action (human health and environmental risks will be reduced through natural attenuation and/or degradation of the contaminant)
 - Containment of contaminated water
 - Treatment of contaminated water
 - Disposal of contaminated water
 - Rehabilitation of contaminated system components
 - Replacement of contaminated system components
 5. *Remediation technology selection.* A comparative analysis is performed to identify the advantages and disadvantages of each alternate remediation technology. The criteria for technology selection include:
 - Protection of human health
 - Protection of the environment
 - Compliance with applicable regulations (e.g., SDWA, CWA)
 - Implementability
 - Cost
 6. *Remedial design.* After a final remedy is selected, remedial design is the next step. This is an engineering phase involving preparation of a series of documents, specifications, and drawings that detail the steps to be taken during the remedial action.
 7. *Remedial action.* This is the implementation of the chosen remediation approach and includes both treatment of contaminated water and rehabilitation of system components.
 8. *Postremediation monitoring.* After site actions are complete, the system must be monitored to ensure that the remediation was effective.
 9. *Communication to restore public confidence.* During remediation and prior to return of the water system to normal operations, the water utility and other agencies must provide outreach to the community to restore public confidence in the drinking water or wastewater system. This could be the most challenging step.

GOVERNMENT ASSISTANCE

Following a natural disaster, major accident, or intentional act, should the remediation and recovery of a utility require the assistance of the federal

government, a number of agencies are authorized to act (Travers 2007). According to ESF #3, the Public Works and Engineering Annex of the NRF, the US Army Corps of Engineers coordinates response and recovery activities related to water and wastewater infrastructure. USEPA is a support agency and will likely assist the Corp of Engineers in this effort. This could include USEPA performing functions such as damage assessments of affected utilities. The NRF can be downloaded from www.fema.gov/nrf.

FEMA also has responsibilities under ESF #3 to coordinate the public assistance program. Through this initiative, FEMA awards grants to assist state and local governments, and certain private, nonprofit entities (PNP), with response and recovery efforts for major disasters or emergencies declared by the President of the United States. These efforts include the repair, replacement, and restoration of disaster-damaged, publicly owned facilities and certain PNP facilities.

Utilities are encouraged to become familiar with the public assistance program to understand the grant process and eligible reimbursement activities. Training on the public assistance grant program is available at <http://training.fema.gov/emiweb/IS/is630.asp>.

BUSINESS CONTINUITY PLANS (BCP)

A BCP helps a utility continue to function in the aftermath of an emergency (Warren et al. 2008). Unlike an ERP, which focuses on the direct response to a disaster, a BCP describes how a utility continues its everyday business functions following the initial response and incident stabilization period. The BCP includes procedures for dealing with the financial effects of a crisis, adapting company policies to meet the changing needs of employees and the utility, resuming normal operations, paying employees, billing customers, and staying in business. Specific goals of a BCP include

- Defining business impacts, risks, and vulnerabilities
- Providing for continuation of the utility's core mission
- Ensuring performance of essential services
- Protecting critical resources needed to perform essential functions
- Reducing operational disruptions

As with an ERP, a BCP will be most effective if, prior to an emergency, the utility develops the plan, ensures that critical employees are familiar with it, and exercises the plan.

The National Fire Protection Agency has issued a standard that is designed to be a description of the basic criteria for a comprehensive program that addresses disaster recovery, emergency management, and business continuity (NFPA 2007).

REFERENCES

- American Water Works Association (AWWA). 2009. *Disaster Response and Recovery DVD*. Denver, Colo.: AWWA.
- Burrows, W.D., and S.E. Renner. 1999. Biological Warfare Agents as Threats to Potable Water. *Environ. Hlth. Perspectives*, 107(12):975.
- Calomiris, J.J. 2006. *Bacillus anthracis* Spores in a Model Drinking Water Pipe System. Abst. 226(H). Amer. Soc. Microbial. Biodefense Research Meeting. Washington, D.C.
- Dahm, B. 2009. Disinfecting Water Mains Using a Trailer Mounted Ozone System. *Proc. 2009 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Federal Emergency Management Agency (FEMA). 2003. *Emergency Response to Terrorism, Job Aid*, ed. 2.0. US Department of Homeland Security. Washington, D.C.: Federal Emergency Management Agency.
- Morley, K., and R. Riordan. 2006. *Utilities Helping Utilities: An Action Plan for Mutual Aid and Assistance Networks for Water and Wastewater Utilities*. Denver, Colo.: AWWA. www.awwa.org/files/Advocacy/Govtaff/Documents/Utilities_Helping_Utilities.pdf#Whitepaper.
- Moser, R.M. 2005. Purposeful Contamination of Distribution System with Chlordane Affecting 10,000 People. *Proc. 2005 AWWA Water Security Congress*. Denver, Colo.: AWWA.
- National Association of Clean Water Agencies (NACWA). 2005. *Planning for Decontamination Wastewater: A Guide for Utilities*. Washington, D.C.: NACWA.
- National Fire Protection Agency (NFPA). 2007. *NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs*. Quincy, Mass.: NFPA. <http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf>.
- Roberson, A., and K. Morley. 2005. We Need to Get Strategic on Water Security. *Jour. AWWA*, 97(10):42.
- Travers, D. 2007. Preparing for an Emergency. *Jour. AWWA*, 99(8):36.
- US Environmental Protection Agency (USEPA). 2000. *First Responders' Liability Due to Mass Decontamination Runoff*. USEPA 550-F-00-009. Washington, D.C.: USEPA.
- USEPA. 2008. *Decontamination and Recovery Planning: Water and Wastewater Utility Case Study*. Office of Water 817-F-08-004. Washington, D.C. www.epa.gov/safewater/watersecurity/pubs/report_decon_casestudy.pdf.
- Warren, L., J. Moyer, and C. Cyr. 2008. Sidestep Disaster with a Business Continuity Plan. *Opflow*, 34(7):16.
- Weisman, R., and S. Jayasundera. 2006. Infrastructure Decontamination Information Added to EPA Water Contaminant Database. *Water World*. Tulsa, Okla.
- Welter, G., J. Cotruvo, M. Lecheyvallier, R. Moser, and S. Spangler. 2005. Decontamination of Water System Infrastructure. *Proc. AWWA Water Security Congress*. Denver, Colo.: AWWA.
- Whitler, J. 2007. Emergency Preparedness for Drinking Water and Wastewater Systems. *Jour. AWWA*, 99(3):36.

PANDEMIC FLU

Influenza viruses are found in many species, including humans, birds, swine, horses, and dogs. In mammalian species, these viruses cause respiratory disease.

A pandemic is an infectious disease epidemic that affects people worldwide. Influenza pandemics are rare but recurrent events. Ten influenza pandemics have been documented in the past 300 years (Osterholm 2005), three of which occurred during the 20th century. The most significant was the Spanish Flu in 1918, when as many as 100 million people perished around the globe and more than 500,000 died in the United States. The Asian Flu in 1957 claimed 1 to 2 million lives globally and 70,000 in the United States, and the 1968 Hong Kong Flu was responsible for approximately 1 million deaths worldwide and 34,000 in the United States. Many public health specialists believe that another influenza pandemic is inevitable and could occur at any time (Patriarca and Cox 1997, Osterholm 2005, Fauci 2006). Because such an event could significantly affect the operations of drinking water and wastewater utilities, water companies are encouraged to plan for this contingency.

BACKGROUND

Viruses survive and reproduce by latching onto a cell in a bacterial, plant, or animal host. The virus manipulates the receptor cell causing the cell to engulf the virus. The virus releases its nucleic acid material (genes) from within its protein coat. The viral nucleic acid material (DNA or RNA) enters the nucleus of the host cell and directs it to synthesize viral genes and proteins that spontaneously assemble into new viruses that subsequently break out of the host cell. Once free, the newly formed viruses can infect other cells in the same host or move to a different host.

Viruses in the family Orthomyxoviridae cause influenza. There are three genera of influenza viruses: *Influenzavirus A*, *Influenzavirus B*, and *Influenzavirus C*. These are also referred to as type A, type B, and type C influenza viruses. Influenza A viruses include avian, swine, equine, and canine influenza viruses, as well as the human influenza A viruses. Influenza A viruses have caused a number of human flu epidemic and pandemic disease outbreaks. Influenza B viruses are mainly found in humans. They can cause epidemics in human populations but have not so far been responsible for pandemics. Influenza C viruses are mainly associated with disease in humans and only rarely are associated with large-scale epidemics.

Influenza A viruses are classified into subtypes based on two surface antigens, the hemagglutinin (H or HA) proteins and the neuraminidase (N or NA) proteins. Subtypes are distinguished by differences in their genetic sequences, which translate into differences in their antigenic structure. There are 16 hemagglutinin antigens (H1 to H16) and nine neuraminidase antigens (N1 to N9). The hemagglutinin proteins allow the flu virus to bind to host cell walls and penetrate them. The neuraminidase proteins allow newly formed viruses to break free from the host cell. The hemagglutinin proteins are the major target for the immune response.

Influenza A viruses are also classified into strains. The strains are categorized by type (e.g., A); host (e.g., avian); place of first isolation; strain number (if any); year of isolation; and antigenic subtype (e.g., H1N1). For example, the H1N1 swine flu virus that caused a limited outbreak of swine flu among soldiers at Fort Dix, N.J., in 1976 is termed *A/sw/New Jersey/76 (H1N1)*.

Influenza viruses are single-stranded RNA viruses with a genome composed of eight separate segments (chromosomes) of the nucleic acid RNA, rather than one long, single molecule. The eight influenza chromosomes contain a total of 10 genes, compared with approximately 20,000 genes in people. Each gene is responsible for the ultimate synthesis of one type of protein. Influenza A viruses change much more frequently than other viruses.

This is why lifelong vaccinations can protect people against polio and measles indefinitely, while yearly vaccinations are needed to provide protection against seasonal and emerging flus. Strains evolve as they accumulate point mutations during virus replication (*antigenic drift*). A more abrupt change occurs during genetic reassortment (*antigenic shift*). Reassortment occurs when two different influenza viruses infect a single cell simultaneously. When the new viruses are assembled, they may contain one or more of the eight RNA segments (chromosomes) from one parent virus as well as segments from the other. Reassortment between different strains can result in the emergence of novel strains.

Reassortment can also occur between avian, swine, equine, canine, and human influenza A viruses. For example, if a pig is infected with a human influenza A virus and an avian influenza A virus at the same time, the new replicating viruses could mix existing genetic information (reassortment) and

produce a novel virus that had most of the genes from the human virus but a hemagglutinin and/or a neuraminidase gene from the avian virus. The resulting new virus might then be able to infect humans and spread from person to person, but it would have surface proteins (hemagglutinin and/or neuraminidase) not previously seen in influenza viruses that infect humans. If this new virus causes illness in humans and can be transmitted easily between people, an influenza pandemic can occur.

Human influenza A viruses are found mainly in people, but they can also infect swine and birds. Human influenza viruses regularly circulate throughout the world, and in the winter, they typically cause disease epidemics in the human population. Seasonal outbreaks are caused by subtypes of influenza virus that already circulate among people.

Approximately 36,000 Americans and 500,000 people worldwide die each year of seasonal flu. While there is some acquired immunity in most populations resulting from prior exposures and vaccinations, strains mutate in small but important ways from year to year (antigenic drift) and more virulent strains appear in certain seasons. Flu vaccinations are usually prepared between active flu seasons based on prevalent strains from the most recent flu season.

Pandemic influenza is caused by a virus that is dramatically different from those that have occurred previously, which can occur through antigenic shift. These novel viruses cause pandemics because few people or none at all have had prior immunologic exposure to the surface proteins of these viruses. The new strains may also have a greater impact on human health if they are inherently more virulent. The flu pandemics of 1918, 1957, and 1968 resulted from antigenic shifts. Once a new pandemic influenza virus emerges and spreads, it usually becomes established among people and circulates for many years as seasonal epidemics of influenza.

The existence of influenza viruses in birds was recognized more than 120 years ago and was referred to as *fowl plague* or *fowl pest*. Avian influenza viruses circulate worldwide and affect wild birds as well as domestic poultry. Waterfowl and shorebirds appear to be the natural reservoir hosts. In wild birds, the influenza viruses are usually, though not always, carried asymptotically. Outbreaks in domestic bird flocks have often been linked to direct or indirect contact with wild waterfowl.

In poultry, there are two forms of disease. Low pathogenicity avian influenza viruses generally cause asymptomatic infections, mild respiratory disease, or decreased egg production. High pathogenicity avian influenza (HPAI) viruses cause severe disease that can kill up to 90–100 percent of a poultry flock. Some avian influenza viruses can also infect mammals, including humans and swine. Normally, avian influenza viruses do not spread efficiently in mammals and infections are limited to individual animals or small groups.

Swine influenza viruses were first isolated in the United States in 1930. Swine flus are mainly found in pigs, but they have also been found in other

species. Swine influenza infections may occur in people who have contact with pigs. Twelve cases of human infection with swine influenza were reported to the CDC in the period from December 2005 through February 2009 (CDC 2009a).

Swine are distinct from other animals because their cells possess receptors for influenza A viruses of swine, human, and avian origin. This phenomenon enhances the possibility of reassortment of genetic material when more than one virus of a different strain infects swine, resulting in new strains with different genetic components. For this reason, swine have been referred to as *mixing vessels* for the formation of new flu viruses.

On rare occasions an avian or swine influenza virus adapts into a strain that is contagious among humans. Generally, this requires a novel hemagglutinin and/or neuraminidase protein to evade the human immune response, together with viral proteins that are well adapted to the new host's cells (Reid and Taubenberger 2003). These new influenza strains can be dangerous for human populations because there is no acquired immunity from previous human infections. In this case, the influenza may spread more rapidly, may infect more people, and may cause more serious disease than normal seasonal epidemics of human influenza.

The appearance of a novel strain may cause a widespread epidemic in a specific country. With the frequent and rapid travel that occurs between countries, an epidemic affecting a single country can quickly become a pandemic, affecting countries around the globe. All three influenza pandemics that occurred in the 1900s appear to have had an avian origin.

A strain of avian influenza virus, categorized as HPAI H5N1 virus, has created a great deal of concern during the past decade because it has shown the ability to occasionally be transmitted from birds to people. This strain was first isolated from a farmed goose in China in 1996. In 1997, outbreaks of H5N1 avian influenza were reported in poultry farms and live markets in Hong Kong. A total of 18 cases (six fatal) were reported in the first known instance of human infection with this virus.

The more recent (2003–2009) HPAI H5N1 outbreak began in poultry in Southeast Asia in 2003. Since 2003, H5N1 avian influenza viruses have killed millions of domestic fowl in Asia, parts of Europe, the Pacific, the Middle East, and Africa, and tens of millions more have been culled. HPAI (H5N1) has been isolated from more than 50 different wild avian species (National Wildlife Health Center 2006). Numerous deaths have been reported in wild birds, which typically carry avian influenza viruses asymptotically. As of May 2009, this virus had infected 429 people, with about two-thirds of these cases being fatal (WHO 2009).

Human infections have occurred in Azerbaijan, Bangladesh, Cambodia, China, Djibouti, Egypt, Indonesia, Iraq, Lao People's Democratic Republic, Myanmar, Nigeria, Pakistan, Thailand, Turkey, and Vietnam. Most of the human infections resulted from close contact with poultry. A few cases of limited person-to-person spread have been documented after prolonged

contact. However, sustained human-to-human contact has not been reported (WHO 2006a, CDC 2007). As of May 2009, HPA1 H5N1 has not been found in birds or people anywhere in the United States, nor in the rest of North America, Central America, or South America (USEPA 2009).

While some countries have eradicated the virus from poultry, this epidemic is ongoing and worldwide eradication is not expected in the short term (Spickler 2009). Although most cases of human infection have involved transmission from infected birds to people, if this virulent strain becomes adept at passing from person to person, a dangerous influenza pandemic could result with the potential to kill millions of people (WHO 2005).

An outbreak of swine flu in people was documented in 1976. Approximately 500 military recruits at Fort Dix were infected with a swine influenza virus, but the outbreak did not spread to the surrounding community. One of the recruits died of pneumonia (CDC 2009a). In the spring of 2009, a flu strain caused by a novel A virus of H1N1 subtype emerged in Mexico, rapidly crossed the US border, and quickly spread around the world (MMWR 2009). The epidemic caused relatively mild illness in a large number of patients and some deaths and continued to spread through the summer and autumn of 2009. A large scale vaccination program was mounted in the US and other countries to control the pandemic.

The virus was characterized as swine influenza because it showed characteristics of A viruses circulating in swine. This strain is actually believed to contain a combination of genes from human, bird, and North American and Eurasian swine flu viruses. The public health threat presented by this virus was closely monitored worldwide since it became a global influenza pandemic (Pitchers and Nichols 2009).

EFFECTS OF PANDEMICS ON WATER UTILITIES

As pointed out by Michael Chertoff, the former secretary of the US DHS, a severe pandemic influenza presents a tremendous challenge because it may affect the lives of millions of Americans, cause significant numbers of illnesses and fatalities, and substantially disrupt economic and social stability (DHS 2006). A flu pandemic will last much longer than most other public health emergencies and may include waves of influenza activity separated by several months (CDC 2005).

An influenza epidemic or pandemic could significantly affect drinking water and wastewater utilities. Based on records from previous pandemics, 20 to 40 percent of the workforce could be unavailable for an extended period of time. Some individuals may be absent because of their own illnesses, while others may be absent while caring for sick family members or looking after children who are home because of school and day-care closings. Still other employees may not report to work for fear of becoming infected.

Absenteeism may be particularly critical for small utilities because staffing levels are already low. Treatment chemicals, supplies, and equipment may

be difficult to obtain because of workforce shortages and business closings in other industries, as well as gasoline shortages needed to ship these goods. If these resources are available, the prices may increase rapidly for the same reasons. Because flu outbreaks may occur simultaneously throughout the country, the reallocation of resources may be more difficult than in other disaster or emergency situations. Therefore, drinking water and wastewater utilities, along with other critical infrastructures, must rely on their own internal resources.

During the outbreak of H1N1 swine flu in 2009, the CDC acknowledged the key role played by water utilities and other key infrastructures during a potential pandemic. Anne Schuchat, M.D., the acting deputy director for the CDC testified before Congress and made the following statement (Schuchat 2009):

“During public health emergencies like the current novel influenza A (H1N1) epidemic, protecting workers is a top priority, both as members of the community, and as workers with special roles in ensuring the functioning of critical infrastructures.... They keep society functioning by maintaining utilities, public safety, and food and water supply.”

A failure to maintain water services could significantly affect a community’s ability to deal with an epidemic because hospitals—a critical element in community response—rely on potable water and sanitary services to function effectively. Therefore, it is important for water utilities to prepare and maintain pandemic flu contingency plans as well as business continuity or COOPs.

PREPARING FOR, RESPONDING TO, AND RECOVERING FROM A PANDEMIC

Utilities can improve their ability to deal with the effects of epidemics or pandemics in a number of ways.

- prepare a pandemic emergency plan. This can be an addendum to an existing utility ERP.
- Identify employee positions that are critical for keeping the utility operating.
- Cross-train personnel to serve as backups.
- Maintain a roster of recently retired employees to fill in for absent employees.
- Use contract labor to fill-in for absent employees (e.g., consulting firms and plumbing contractors).
- Prepare detailed SOPs to assist replacement personnel.
- Establish a clear chain of command for the utility and prepare a succession plan should key supervisors be unavailable during an epidemic.

-
- Determine ahead of time which functions of the utility's operations are essential and which functions could be postponed during an emergency lasting several weeks or several months.
 - Identify critical resources needed to maintain operations (e.g., chlorine and electricity).
 - Formalize agreements with other water and wastewater utilities to share critical resources and provide mutual aid. The WARN is an effective mechanism for establishing this type of agreement before an emergency occurs.
 - Evaluate potential insurance costs for increased medical expenses.
 - If possible, establish a rainy-day fund so there will be additional money available for emergency or routine purchases at increased prices.
 - Prepare a business plan for operating on reduced revenues that might occur during a prolonged disease outbreak.
 - Consider the need and conditions for extreme measures such as sequestering onsite critical staff during an epidemic.
 - Encourage employees to obtain annual flu vaccinations.
 - Investigate the possibility of water utility personnel receiving vaccinations and antiviral medications on a priority basis during a disease outbreak. This would involve coordination with public health authorities.

Public utility personnel have already been assigned priority for vaccinations and for antiviral drugs in the US Department of Health and Human Services Pandemic Influenza Plan. For vaccinations, public utility personnel are included in tier 2, subtier B along with public safety personnel. For distribution of antiviral medications, critical infrastructure employees are included in tier 8 (USDHHS 2005).

A particular challenge during a flu emergency will be to balance the need to have utility employees on the job, perhaps for extended hours, and ensure they can still care for their families. This may require the utility to review existing personnel policies to determine whether changes need to be made for a pandemic. Sick leave policy may need to be more liberal. Personnel leave policy may need to be revised to permit employees to care for ill family members. The utility may consider enacting or modifying work-at-home policies to allow employees to spend less time at the worksite. The employer must ensure that the company's IT infrastructure could support this action. Utilities should also encourage employees to have family ERPs in place.

Potential Labor and Legal Issues During a Flu Emergency

An epidemic or pandemic flu situation may raise a number of labor issues that should be addressed.

- Employees may refuse to report to work because of fears of becoming infected.
- One employee reports that another employee appears to be sick and wants the company to do something about it.

- Employees may complain about fellow employees not practicing good hygiene.
- Should the company pay employees who were told to stay home?
- Should antiviral drugs be issued to all employees?
- Should the company check the temperatures of employees?

Potential legal questions include the following:

- Can an employer lawfully demand that employees provide proof of vaccination?
- Can an employer bar sick workers from the worksite?
- Can a utility compel healthy, but fearful, employees to report to work?
- Can an employer restrict nonwork-related employee travel abroad?

INFECTION CONTROL IN THE WORKPLACE

Should an epidemic or pandemic flu situation develop, companies, including utilities, can take steps to help control the spread of disease in the workplace, protect employees, and ensure the utility can continue to function. These steps will also reinforce the idea that the utility is concerned about worker safety and may encourage employees to continue reporting to the worksite.

Some suggestions include:

- Place alcohol-based sanitizers throughout utility facilities, especially in the entrances to dining areas, copy rooms, and computer rooms.
- Place tissue boxes and trash cans throughout buildings to encourage proper hygiene.
- Place disinfectants and cleaning supplies in restrooms and work areas.
- Limit face-to-face meetings involving large numbers of people. If possible, substitute these with teleconferences and video conferences.
- Post signs throughout the facilities reminding employees of proper hygiene to reduce disease transmission.
- Limit the sharing of equipment by employees.
- Sanitize shared work areas.
- Restrict or discourage visitors to facilities and tours.
- In extreme situations, face masks can be issued to personnel who interact with the public.
- Discourage handshaking.

INFLUENZA TRANSMISSION VIA WATER

In mammals, including humans, influenza viruses are transmitted in aerosols created by coughing and sneezing and by contact with nasal discharges either directly or on environmental surfaces. Mammalian influenza viruses can survive for several hours in the environment.

A question that arises in the water industry is whether influenza can be transmitted to people by ingestion or contact with drinking water contaminated with flu virus. Furthermore, if during a disease outbreak, drinking water treatment systems and domestic wastewater treatment systems became contaminated with virus, could this exacerbate the spread of disease and pose a threat to treatment plant operators and the general public (Lucio-Forster et al. 2007)?

In contrast to human influenza virus, which replicates in humans primarily in the respiratory tract, the gut is the main replication site for avian influenza viruses in birds. Infected birds shed moderate to large quantities of avian flu virus in their feces, saliva, and nasal secretions, and fecal–oral transmission via water is the predominant means of spread among wild birds (Sturm-Ramirez et al. 2004). Open bodies of water, including drinking water reservoirs, can become contaminated by birds that are actively shedding virus and by waterfowl carcasses (Hoffbuhr et al. 2006). Fecal waste from duck and chicken farms may also spread to bodies of water by surface runoff or possibly enter groundwater through disposal and composting of waste on poultry farms.

Several cases have been reported of people contracting H5N1 avian influenza by contact with contaminated waters (CRC 2005; Hoffbuhr et al. 2006). An adult woman and an unrelated young boy in Vietnam were reported to have developed the disease after swimming in water bodies used for disposal of dead poultry. The boy developed a severe H5N1 infection including involvement of the brain. The origin of the infection appeared to be the gastrointestinal route, suggesting ingestion of contaminated water as a possible cause. Because these data represent only a few cases, the question of whether humans can become infected by ingestion, or direct intranasal or conjunctival inoculation of influenza viruses in contaminated water is not fully resolved.

It should be noted that fecal shedding of avian H5N1 virus may be possible in humans. The virus was recovered from an infected child with diarrhea (de Jong et al. 2005). The potential presence of influenza virus in human feces may have implications for occupational exposure of wastewater system workers, possibly via aerosol generation, during future flu epidemics (WHO 2006b). Should this be the case, measures could be needed to reduce aerosol generation and exposure of individuals to aerosols (e.g., use of protective clothing and masks).

Lucio-Forster and colleagues (2007) studied the susceptibility of H5N2 avian influenza virus (used as a safer surrogate for H5N1) to chlorine and to UV irradiation. Infectious H5N2 was exposed to the disinfectants immersed in phosphate buffer and in wastewater effluent. The results indicated that the virus was inactivated by UV at fluences of 10 mJ/cm^2 .

Typical design fluences for water treatment vary from 40 mJ/cm^2 to 170 mJ/cm^2 . Chlorine trials indicated that the virus was completely inactivated at a CT value of $8\text{ mg/L} \times \text{minutes}$. This CT value is substantially less than that used in US drinking water and wastewater plants.

USEPA, in conjunction with the US Department of Agriculture, investigated the susceptibility of several avian influenza viruses to chlorine (Rice et al. 2007). These viruses were the highly pathogenic avian influenza virus H5N1. The results of the study indicated that two strains of bird flu virus, one isolated from domestic poultry and one isolated from a wild swan, were rapidly inactivated by chlorine. Exposure of the viruses to 0.5 to 1.0 mg/L free chlorine for a period of one minute resulted in greater than 99.9 percent inactivation.

The study suggests that chlorine inactivation of avian influenza virus may actually be more rapid than that observed for typical enteric viruses of concern (e.g., Hepatitis A virus and Norovirus). Influenza viruses have an outer lipid envelope that is highly susceptible to damage by oxidants such as chlorine and ozone (WHO 2006a). These viruses require an intact lipid envelope to attach to and infect host cells. Influenza viruses are more susceptible to chlorine than nonenveloped enteric viruses. Therefore, water disinfection processes that are designed to inactivate the more resistant enteric viruses would be expected to provide a higher degree of protection against influenza viruses (CRC 2005).

Conventional filtration of surface waters is also expected to be effective in partial removal of influenza viruses (USEPA 2007). The influenza viruses (50–120 nm in diameter) are somewhat larger than the enteric viruses (25–41 nm in diameter), so they should be expected to be removed at least as efficiently by coagulation and filtration processes (CRC 2005).

A Netherlands study (Schijven et al. 2005) and an Australian study (CRC 2005) of avian influenza concluded that the risk of transmission in treated drinking water is negligible. Similarly, both the CDC (2009b) and USEPA (2009) have issued statements on their Web sites indicating that the risk of flu transmission via properly treated drinking water is insignificant. Additionally, maintenance of free chlorine levels of 1 to 3 parts per million (ppm or mg/L) for pools and 2 to 5 ppm for spas, recommended by CDC, is protective against water transmission of influenza viruses (CDC 2009).

Surface runoff represents a potential source of contamination for groundwater. While some states require that all groundwater-based public systems use disinfection as a treatment, this is not always the case. In addition, the vast majority of private wells are not equipped with chlorinators. Some specialists believe that it would be difficult for influenza virus to contaminate most groundwater sources that have not been disinfected. Virus particles become diluted by the large volume of groundwater with which they mix, become inactivated with time, and are removed from groundwater flow during passage through subsurface groundwater systems (PandemicFlu.gov 2009).

ADDITIONAL INFORMATION

DHS has published a guidance document on pandemic flu planning for water utilities (DHS 2006) entitled *Pandemic Influenza: Preparedness, Response,*

and Recovery—Guide for Critical Infrastructure and Key Resources. The document contains a downloadable template for COOPs and a separate document for government agencies. The core component of the DHS guidance document is section 5, “The Continuity of Operations—Essential (COP-E) Guide.” This section provides critical infrastructures such as the water industry with a practical tool to facilitate their pandemic planning and response efforts. It emphasizes the importance of a shift from conventional business continuity planning to pandemic specific planning and helps planners identify essential functions, people, and material within and across sectors. This section also proposes methods to protect and sustain these resources at each phase from preparation through recovery.

Additional information on pandemic flu, as well as further guidance on flu planning is available from the US government official flu Web site, www.pandemicflu.gov. The site provides downloadable planning documents and checklists for businesses.

AMWA developed a pandemic influenza reference guide and checklist for member water utilities (AMWA 2007), which can be downloaded from AMWA’s web site, www.amwa.net.

Van Atta and Newsad (2009) modified a checklist for pandemic influenza planning that was originally published by the CDC. The checklist includes information from regulatory agencies, water agencies, and critical infrastructure documents that can be used to verify that a pandemic plan is effective. They also developed a template that water utilities can use for pandemic influenza planning that can be downloaded from the Operator Training Committee of Ohio Web site at www.ohiowater.org/OTCO/pages/downloads.htm.

REFERENCES

- Association of Metropolitan Water Agencies (AMWA). 2007. *Business Continuity Planning in the Event of an Influenza Pandemic: A Reference Guide*. Washington, D.C.: AMWA.
- Centers for Disease Control and Prevention (CDC). 2005. *Information about Influenza Pandemics*. Atlanta, Ga. www.cdc.gov/flu.
- CDC. 2007. *Avian Flu*. Atlanta, Ga. [www.cdc.gov/avian/index.htm](http://www.cdc.gov/flu/avian/index.htm).
- CDC. 2009a. *Key Facts about Swine Influenza (Swine Flu)*. Atlanta, Ga. www.cdc.gov/swineflu/key-facts.htm.
- CDC. 2009b. *H1N1 Flu (Swine Flu) and You: Questions and Answers*. Atlanta, Ga. www.cdc.gov/h1n1flu/qa.htm.
- Cooperative Research Centre for Water Quality and Treatment—Australia (CRC). 2005. Avian Influenza: Is There a Risk to Water Supplies? *Health Stream*, 40:12.
- de Jong, M.D., V.C. Bach, T.Q. Phan, M.H. Vo, T.T. Tran, B.H. Nguyen, M. Beld, T.P. Le, H.K. Truong, V.V. Nguyen, T.H. Tran, Q.H. Do, and J. Farrar. 2005. Fatal Avian Influenza A (H5N1) in a Child Presenting with Diarrhea Followed by Coma. *New Engl. Jour. Med.*, 352:686.
- DHS (Department of Homeland Security). 2006. *Pandemic Influenza: Preparedness, Response, and Recovery (Guide for Critical Infrastructures and Key Resources)*. Washington, D.C.: DHS. www.fema.gov/government/coop/index.shtml.
- Fauci, A.S. 2006. Pandemic Influenza Threat and Preparedness. *Emerg. Infect. Dis.*, 12(1):73.
- Gertig, K.R. 2006. Taken Down by Disease: Can Bird Flu Halt Operations. *Opflow*, 32(7):14.
- Hoffbuhr, J. et al., 2006. Utilities Prepare for Potential Pandemic. *Jour. AWWA*, 98(6):48.

- Lucio-Forster, A., D.D. Bowman, B. Lucio-Martinez, M.P. Labare, and M.S. Butkus. 2007. Assessing the Effects of Chlorination and UV Irradiation on Avian Influenza Virus (H5N2) in Water and Wastewater. *Proc. of 2007 Water Environment Federation Disinfection Conference*, Pittsburgh, Pa.
- Morbidity and Mortality Weekly Report*. 2009. Outbreak of Swine-Origin Influenza A (H1N1) virus infection—Mexico, March–April 2009. *Morb. Mortal. Wkly. Rep.*, 58:467.
- National Wildlife Health Center. 2006. List of Species Affected by H5N1 (Avian Influenza). Madison, Wis. www.nwhc.usgs.gov/disease_information/avian_influenza/affected_species_chart.jsp.
- Osterholm, M.T. 2005. Preparing for the Next Pandemic. *N. Engl. Jour. Med.*, 352(18):1839.
- PandemicFlu.gov. 2009. Can the Avian Influenza Contaminate Water Sources? www.pandemicflu.gov/faq/foodsafety/fws-0002.html.
- Patriarca, P.A., and N.J. Cox. 1997. Influenza Pandemic Preparedness Plan for the United States. *Jour. Infect. Dis.*, 176(Suppl 1):S4-7.
- Pitchers, R., and G. Nichols. 2009. *UK Briefing Note on Newly Emergent Influenza A (H1N1)*. United Kingdom Industry Research Limited, May 6, 2009. London.
- Reid, A.H., and J.K. Taubenberger. 2003. The Origin of the 1918 Pandemic Influenza Virus: A Continuing Enigma. *Jour. Gen. Virol.*, 84:2285.
- Schijven, J., P.F.M. Teunis, and A.M. de Roda Husman. 2005. Quantitative Risk Assessment of Avian Influenza Virus Infection via Water. Netherlands Environmental Inspectorate M/703719/05/BD, RIVM, Bilthoven, the Netherlands.
- Schuchat, A. 2009. *CDC's Response to a Novel 2009 H1N1 Influenza Virus*. Testimony before the Committee on Education and Labor, US House of Representatives, May 7, 2009.
- Spickler, A.R. 2009. *Technical Factsheet on Influenza*. The Center for Food Security and Public Health, Iowa State University. <http://www.cfsph.iastate.edu/Factsheets/pdfs/influenza.pdf>.
- Sturm-Ramirez, K.M., T. Ellis, B. Bousfield, L. Bissett, K. Dyrting, J.E. Rehg, L. Poon, Y. Guan, M. Peiris, and R.G. Webster. 2004. Reemerging H5N1 Influenza Viruses in Hong Kong in 2002 are Highly Pathogenic to Ducks. *Jour.. Virol.*, 78:4892.
- US Department of Health and Human Services (USDHHS). 2005. *HHS Pandemic Influenza Plan*. Washington, D.C. www.hhs.gov/pandemicflu/plan/pdf/HHSPandemicInfluenzaPlan.pdf.
- USEPA. 2007. *Avian Flu (Pandemic Flu)*. Washington, D.C. www.epa.gov/avianflu/faq.htm.
- USEPA. 2009. *Can the Avian Influenza Contaminate Air or Water and What Disposal Options Are Recommended? Food, Water, and Air Safety Questions*. Washington, D.C. www.pandemicflu.gov/faq/foodsafety/fws-0001.html.
- Van Atta, P., and R. Newsad. 2009. Water System Preparedness and Best Practices for Pandemic Influenza. *Jour. AWWA*, 101(1):40.
- World Health Organization (WHO). 2005. *Avian Influenza: Assessing the Pandemic Threat*. Geneva, Switzerland. www.who.int/csr/disease/influenza/WHO_CDS_2005_29/en/.
- WHO. 2006a. *Avian Influenza (Bird Flu) Fact Sheet*. Geneva, Switzerland. http://www.who.int/media-centre/factsheets/avian_influenza/en/index.html#humans.
- WHO. 2006b. *Review of Latest Available Evidence on Potential Transmission of Avian Influenza (H5N1) Through Water and Sewage and Ways to Reduce the Risks to Human Health*. Geneva, Switzerland: WHO.
- WHO. 2009. *Cumulative Number of Confirmed Human Cases of Avian Influenza A/(H5N1) Reported to WHO*. Geneva, Switzerland. http://who.int/csr/disease/avian_influenza/country/cases_table_2009_05_22/en/print.



CONCLUSIONS

Concern about the possibility of drinking water and wastewater systems becoming the target of terrorism began with the terrorist attacks of Sept. 11, 2001. Prior to that event, the water industry had dealt infrequently with vandalism and isolated malevolent acts.

This handbook has attempted to provide a comprehensive examination of the recent research, government guidance, and industry approaches dealing with this concern. From this effort, and years of first-hand experience with water security and emergency preparedness, the author offers the following conclusions and opinions.

Because drinking water and wastewater systems are such an important part of the infrastructure of this country and directly affect the health and well-being of the entire population on a daily basis, it seems reasonable to conclude that they are a potential target for domestic or transnational terrorism. The magnitude of this risk is certainly an open question.

As described in chapters 2 and 3 of this handbook, terrorists have attacked water infrastructure in Iraq, and intentional contamination events and threats have occurred in several countries in recent years. Fortunately, no incidents on a par with the 9/11 airline hijackings in the United States, the train attacks in Madrid, the subway attacks in London, or any of the other large-scale terrorist incidents have occurred at utilities. However, because the elements of surprise and unpredictability are salient features of terrorism, it would be imprudent to dismiss the threat to the water and wastewater industries. The chance of a terrorist act occurring at any specific utility is remote. However, the possibility that a utility somewhere may be targeted is real.

In addition to the possibility of terrorism, utilities must be prepared to deal with isolated instances of nonterrorist malevolent attacks, such as the intentional chlordane contamination of drinking water in Pittsburgh in 1980

and the series of cyber attacks on an Australian wastewater system in 2000, described in chapters 2 and 3. These attacks were initiated by insiders for reasons other than terrorism. However, with the advantages of insider access and knowledge, this type of incident may be more likely to occur and perhaps more difficult to prevent than vandalism and attacks perpetrated by outsiders. Given the nature of malevolent acts in general, the water industry needs to prepare for what appear to be low probability, but potentially high impact, events. As articulated by Ben Grumbles, former assistant administrator for USEPA, "We need to look not only at what is probable but what is possible" (Grumbles 2006).

Another practical reason why water utilities must protect against the possibility of malevolent acts, and be prepared to respond to their consequences, is that the events of 9/11 have altered the public's expectation of the water industry's response. Prior to 9/11, the discovery of a cut fence surrounding a drinking water storage reservoir would have caused no serious alarm. The incident would have quickly been labeled as vandalism, with plans made to repair the breach at some point in the future. Now, the public expects a measured, sensible, and timely response that ensures their safety without unduly disturbing them with false alarms. The possibility that the cut fence may be indicative of a more serious event must be investigated before the incident is discounted as mere vandalism. An effective response of this kind requires prior preparation and training.

Of course, accidents and natural events are more likely to occur than intentional threats and acts. Power grid failures such as that affecting the northeastern United States in 2003, and disastrous hurricanes like Katrina that severely damaged New Orleans have illustrated the vulnerability of the water sector to nature and happenstance.

The most sensible program for protecting utilities is to adopt an all-hazards, multiple-benefits approach. Efforts to decrease vulnerability and increase emergency preparedness for one set of threats (natural disasters, accidents, pandemics, or deliberate acts) should help protect utilities against the others. Similarly, efforts made to improve online monitoring of water quality to detect accidental or intentional contamination events should also assist the utility with regulatory compliance and process control. Taking an all-hazards, multiple-benefits approach to emergency preparedness should provide utilities with the best all-around benefit in the most economical manner.

Security and emergency preparedness are just two of a number of competing requirements for water utilities that include compliance with increasingly stringent regulations, replacement of aging infrastructure, and dealing with newly recognized unintentional contaminants such as trace pharmaceuticals and endocrine disruptors. However, just as with most other activities involving the public, such as air travel, food protection, and high-profile public gatherings, post 9/11 the public expects drinking water and wastewater utilities to exercise due diligence in terms of security and preparedness. This expectation will likely remain for years to come.



LIST OF ABBREVIATIONS/ACRONYMS

| ABB/ ACRON | TERM |
|-----------------------|--|
| ALF | Animal Liberation Front |
| AMSA | Association of Metropolitan Sewerage Agencies |
| AMWA | Association of Metropolitan Water Agencies |
| APHL | Association of Public Health Laboratories |
| ASCE | American Society of Civil Engineers |
| ASDWA | Association of State Drinking Water Administrators |
| ASSET | Automated Security Survey and Evaluation Tool |
| ATCC | American Type Culture Collection |
| AWWA | American Water Works Association |
| AwwaRF | Awwa Research Foundation |
| BCP | business continuity plan |
| BSL | Biosafety Level |
| BTEX | benzene, toluene, ethylene, xylene |
| CAMAL Net | California Mutual Aid Laboratory Network |
| CAS | Chemical Abstract Service |
| CBR | chemical, biological, and radiochemical/radiological |
| CCTV | close-circuit television |
| CDC | Centers for Disease Control and Prevention |
| CFATS | Chemical Facility Anti-Terrorism Standards |
| CIPAC | Critical Infrastructure Partnership Advisory Council |
| COI | chemicals of interest |

| | |
|---------------------|--|
| COOP | continuity of operation(s) plan |
| CS ² SAT | Control System Cyber Security Self-Assessment Tool |
| CST | civil support team |
| CT | contact time |
| CWA | Clean Water Act |
| CWS | contaminant warning system |
| DBP | disinfection by-product |
| DCS | distributed control system |
| DHS | Department of Homeland Security |
| DO | dissolved oxygen |
| DOC | department operations center |
| DOT | Department of Transportation |
| DPD | N-N-diethyl-p-phenylenediamine |
| DSS | distribution system simulator |
| ECD | electron capture detector |
| ELF | Earth Liberation Front |
| EMAC | Emergency Management Assistance Compact |
| EMS | emergency medical services |
| EOC | emergency operations center |
| EPANET | USEPA software that models water distribution piping systems |
| EPR | emergency response plan |
| eRLN | Environmental Response Laboratory Network |
| ESF | emergency support function |
| ESRI | GIS software |
| ETA | Basque ETA |
| ETV | Environmental Technology Verification |
| EUWP | expeditionary unit water purifier |
| EWQSK | Emergency Water Quality Sampling Kit |
| EWS | early warning system |
| FBI | Federal Bureau of Investigation |
| FDA | Food and Drug Administration |
| FEMA | Federal Emergency Management Agency |
| FERN | Food Emergency Response Network |
| FIRESCOPE | Firefighting Resources of California Organized for Potential Emergencies |
| FOIA | Freedom of Information Act |
| GAO | Government Accountability Office |
| GC | gas chromatography (not chromatograph[s][ic]) |
| GCC | Government Coordinating Council |

| | |
|------------------|--|
| GC–MS | gas chromatography–mass spectrometry (not ...graph[s][ic] [meter]) |
| GETS | Government Emergency Telecommunications Service |
| GIS | geographic information system |
| G–M | Geiger–Müller (counter) |
| | |
| HAS | Homeland Security Act |
| HazMat | hazardous material |
| HMO | health maintenance organization |
| HPAI | high pathogenicity avian influenza |
| HSOC | Homeland Security Operations Center |
| HSPD | Homeland Security Presidential Directive |
| | |
| IAP | incident action plan |
| IC Water | Incident Command Water |
| ICP | incident command post |
| ICS | Incident Command System |
| ID ₅₀ | infectious dose-50 percent |
| IED | improvised explosive device |
| IID | improvised incendiary device |
| IRA | Irish Republican Army |
| ISAC | Information Sharing and Analysis Center |
| IT | information technology |
| LD ₅₀ | lethal dose-50 percent |
| LEL | lower exposure limit |
| LPAI | low pathogenicity avian influenza |
| LRN | Laboratory Response Network |
| LT2ESWTR | Long-Term 2 Enhanced Surface Water Treatment Rule |
| | |
| MALS | multi-age light-scattering (technique) |
| MCL | maximum contaminant level |
| | |
| NACWA | National Association of Clean Water Agencies |
| NASA | National Aeronautics and Space Administration |
| NBC | nuclear, biological, chemical |
| NCS | National Communications System |
| NDWAC | National Drinking Water Advisory Council |
| NEMI | National Environmental Methods Index |
| NEMI–CBR | National Environmental Methods Index for Chemical, Bio- logical, and Radiological Methods |
| NESHTA | National Environmental, Safety, and Health Training Association |
| NEWWA | New England Water Works Association |
| NHSRC | National Homeland Security Research Center |
| NIAC | National Infrastructure Advisory Council |

| | |
|---------|--|
| NIMS | National Incident Management System |
| NIPC | National Infrastructure Protection Center |
| NIPP | National Infrastructure Protection Plan |
| NIST | National Institute of Standards and Technology |
| NMRC | Naval Medical Research Center |
| NOAEL | no observed adverse effect limit |
| NOC | National Operations Center |
| NPDES | National Pollutant Discharge Elimination System |
| NRC | National Research Council |
| NRC | National Response Center |
| NRF | National Response Framework |
| NRP | National Response Plan |
| NRWA | National Rural Water Association |
| O&M | operations and maintenance |
| ORP | oxidation-reduction potential |
| PADEP | Pennsylvania Department of Environmental Protection |
| PCR | polymerase chain reaction |
| PDD | Presidential Decision Directive (with number) |
| PFO | principal federal official |
| PI | photoionization (appears 1x, deleted) |
| PID | photoionization detector |
| PIJ | Palestine Islamic Jihad |
| PIN | personal identification number |
| PKK | Kurdish Worker's Party |
| PLO | Palestine Liberation Organization |
| PN Rule | Public Notification (Rule) |
| PNP | private, nonprofit |
| POTW | publicly owned treatment works |
| PPE | personal protective equipment |
| ppm | parts per million |
| PPS | physical protection system |
| PTZ | pan–tilt–zoom (camera) |
| PVC | polyvinyl chloride pipe |
| RAMCAP | Risk (Analysis and) Management for Critical Asset Protection |
| RAM-W | Risk assessment Methodology for Water |
| RO | reverse osmosis |
| RO WPU | reverse-osmosis water purifier unit |
| RPTB | Response Protocol Toolboxes |
| RTU | remote telemetry unit (appears 1x, deleted) |

| | |
|-----------|---|
| SAIC | Science Applications International Corporation |
| SAM | Standardized Analytical Methods |
| SCADA | supervisory control and data acquisition |
| SDWA | Safe Drinking Water Act |
| SEB | staphylococcal enterotoxin B |
| SEMS | Security and Emergency Management System |
| SOP | standard operating procedure |
| SSA | sector-specific agency |
| SSP | sector-specific plan |
| SSP | site security plan |
| SVA | site vulnerability assessment |
| SWMM | Sewer and Water Management Model |
| TATP | triacetone triperoxide |
| TEVA | Threat Ensemble Vulnerability Assessment |
| TEVA-SPOT | TEVA Sensor Placement Optimization Tool |
| TOC | total organic carbon |
| TTEP | Technology Testing and Evaluation Program |
| UF | ultrafiltration |
| UHF | ultra high frequency |
| UPS | uninterruptible power supply |
| USACE | US Army Corps of Engineers |
| USAMRIID | US Army Medical Research Institute for Infection Diseases |
| USEPA | US Environmental Protection Agency |
| UV-Vis | ultraviolet-visible |
| UWS | unattended water sensor |
| VA | vulnerability assessment |
| VBIED | vehicle-borne improvised explosive device |
| VHF | very high frequency |
| VOC | volatile organic compound |
| VSAT | Vulnerability Self-Assessment Tool |
| WARN | Water and Wastewater Agency Response Network |
| Water SSP | Water Sector-Specific Plan |
| WATERS | Water Assessment Technology Evaluation Research and Security Center |
| WCIT | Water Contaminant Information Tool |
| WEF | Water Environment Federation |
| WERF | Water Environment Research Foundation |
| WHO | World Health Organization |
| WISE | Water Infrastructure Standards Enhancement (Committee) |
| WLA | Water Laboratory Alliance |
| WMD | weapons of mass destruction |
| WPS | Wireless Priority Service |

| | |
|-------|--|
| WSCC | Water Sector Coordinating Council |
| WSGCC | Water Sector Government Coordinating Council |
| WSI | Water Security Initiative |
| WSWG | Water Security Working Group |
| WUERM | water utility emergency response manager |
| Y2K | Year 2000 |



ABOUT THE AUTHOR

Stanley States received a master's degree in Forensic Chemistry and a doctorate in Environmental Biology from the University of Pittsburgh. For the past 33 years, he has worked for the Pittsburgh Water and Sewer Authority and currently serves as Director of Water Quality and Production. In this capacity, he has worked on a daily basis with treatment, laboratory analysis, operations, and regulatory compliance for a large water utility. He has served as an adjunct professor at the University of Pittsburgh and has published a number of papers and book chapters on waterborne pathogens and their removal through water treatment processes.

For the past eight years, Dr. States has been very involved with homeland security and emergency preparedness issues for drinking water and wastewater utilities. He has authored a number of articles and chapters on rapid field analysis and online monitoring. He has also written and delivered a number of courses and webcasts, throughout the United States and overseas, dealing with utility security and preparedness. Sponsors of this training have included the US Justice Department, the Department of Homeland Security, the US Environmental Protection Agency, the Centers for Disease Control and Prevention, the US Army, the American Water Works Association, and the Water Environment Federation.



INDEX

Note: *f.* indicates figure; *t.* indicates table.

- Access control, 103–104
Active and effective security programs, 75–77
Acute toxicity screening, 203–205
Aden, and Arab terrorist movement, 4
Adversarial assimilation, 9
Afghanistan, and possible al-Qaida plot to sabotage American drinking water systems, 46
al-Banna, Hassan. *See* Banna, Hassan al-
al-Qaida. *See* Qaida, al-
Alfred P. Murrah Federal Building (Oklahoma City, Okla.), 2, 9, 21
Allen, Thad, 190
American Civil War, 43
American Society of Civil Engineers (ASCE), 89
American Type Culture Collection (ATCC), 34, 37
American Water Works Association (AWWA), 89
emergency planning and response publications, ix, x, 176, 184
and National Water Sector Cyber Security Committee, 143–144
AMSA. *See* Association of Metropolitan Sewerage Agencies
AMWA. *See* Association of Metropolitan Water Agencies
Analytical response, 185, 199
commercial laboratories, 218
definitive laboratory analysis, 214–216, 215*t.*
field safety screening, 200–201
gas detectors, 200
LRN laboratories (Centers for Disease Control), 216–217
mobile laboratories, 219
National Environmental Methods Index for Chemical, Biological, and Radiological Methods (NEMI-CBR), 220
national laboratories (Centers for Disease Control), 216
online analytical probes, 153–154
rapid field testing of water, 201–211
reference laboratories, 217
Response Protocol Toolbox Module 4 (Analytical Guide), 185
sample collection, 213–214
sample concentration in the field, 211–213, 213*f.*
SCT screen for radioactivity, 200
sentinel laboratories, 217
Standardized Analytical Methods (SAM) document, 220
USEPA Environmental Laboratory Compendium, 219
USEPA Environmental Response Laboratory Network (eRLN), 218

- USEPA Regional Laboratory Networks, 217
- Water Laboratory Alliance (WLA), 217–218
- WCIT database, 218–219, 246
- See also* Information Security Analysis Center; RAMCAP; Response Protocol Toolbox; Security Analysis and Response for Water Utilities; Water Information Sharing and Analysis Center
- Angola, well contamination incidents (1999), 46
- Anthrax, 35–36
- attacks (US, 2001), 5–6, 15, 35
 - and decontamination, 247–248
- Arkansas, and plot to poison big city water supplies, 45
- Aryan Nations, 37
- ASSET (Automated Security Survey and Evaluation Tool), 97
- Asset-Based Vulnerability Checklist for Wastewater Utilities, 97
- Association of Metropolitan Sewerage Agencies (AMSA), 97
- Association of Metropolitan Water Agencies (AMWA), 98
- pandemic flu reference guide, 271
- Association of Public Health Laboratories, 216
- Association of State Drinking Water Administrators (ASDWA), 96
- Assyria, ancient, 43
- Ataturk, Kemal, 12–13
- Athens, ancient, 43
- ATCC. *See* American Type Culture Collection
- Australia
- cyber attack on wastewater utility (Queensland, 2000), 58–59
 - hacker attack on SCADA system (Maroochy), 138–139
- Awwa Research Foundation (AwwaRF), 93
- Bacillus*, and decontamination, 248–249
- Backflow prevention for hydrants, 113–114 programs, 122
- al-Banna, Hassan, 13
- Barriers (perimeter security), 105–106
- Baseline Threat Information for Vulnerability Assessment of Community Water*, 79–80
- Basque ETA, 8, 21
- bin Laden, Osama, 7, 13–15
- Bio-Sensor fish sentinel system, 159–160
- BioCapture BT-550, 206
- Biological and Toxin Weapons Convention, 44
- Biological warfare, 36, 37, 43–44
- Bioterrorism Act of 2002, 64–65, 79–80, 91
- on emergency response plans, 176
 - and FOIA exemption for security-related information, 127
- Biotoxins, 33–34. *See also* Biological warfare
- Bollards, 105
- Botulinum toxins, 33–34
- BTA (Bio Threat Alert) test strips, 205–206
- Bush, George W., 79, 91, 191
- Business continuity plans, 259
- Calcium hypochlorite, 120
- California
- benzene contamination of sewer system (Visalia, 2006), 60
 - Mutual Aid Laboratory Network (CAMAL Net), 216
 - planned bombing of LA International Airport (1999), 8
 - thefts of or tampering with chlorine gas containers from treatment plants, 47
- Cambodia, and pesticide contamination of village water by Khmer Rouge, 46
- CANARY software, 168
- Canberra On-Line Liquid Monitoring system, 161
- Cap locks, 113
- Castor beans, 34
- CBR (radiochemical) incidents, 220, 252–253
- CCTV. *See* Visual surveillance
- Ceausescu, Nicolae, 41
- Censar Multiparameter Water Quality/Security Sensor, 156

- Centers for Disease Control (CDC)
 LRN laboratories, 216, 216–217
 on swine flu and water utilities, 266
- Chains, 105
- Chemical Facility Anti-Terrorism Standards (CFATS), 70
- Chemicals
 DOT hazardous chemical regulations, 26
 industrial, 38–40
 releases of hazardous treatment chemicals, 22
 spills, 25–26
 weaponized, 40–42, 216
See also NPC (nuclear, biological, chemical) weapons
- Chertoff, Michael, 129, 265
- China
 and anthrax contamination by Japanese Army (WWII), 36
 Cultural Revolution, 7
 and Japanese use of biological agents (WWII), 43–44
 pesticide poisoning of water supply by water purification device salesman, 47
 petrochemical spill contaminating source waters, 25–26
 and plague contamination by Japanese Army (WWII), 37
 and *Salmonella* contamination by Japanese Army (WWII), 37
- Chloramines and chloramination, 121 and contaminant monitoring, 150–151
- Chlorine
 inactivation of avian influenza virus, 270
 liquid or solid rather than gas, 120
 online measurement systems, 151
 portable pumping and injection systems, 121
 residual as mitigation measure, 121
 temporary increases in levels of, 121
- Chlorine analyzers, 100
- Chlorine gas
 attacks and releases, 22
 decision tool, 120
 delivery security, 134
 risk management, 120
- thefts of or tampering with containers from treatment plants, 47
- The Chlorine Institute Security Management Plan, 134
- CIPAC. *See* Critical Infrastructure Partnership Advisory Council
- Clean Water Act of 1972, 64
- Commercial laboratories, 218
- Computers. *See* Cyber measures; SCADA systems
- Concrete planters, 105
- Contaminants, 31–32, 32t.
 biotoxins, 33–34
 industrial chemicals, 38–40
 infectious dose 50 percent (ID_{50}), 31
 lethal dose 50 percent (LD_{50}), 31–32
 pathogenic microbes, 34–38
 pesticides, 40
 radionuclides, 42
 weaponized chemicals, 40–42
See also Decontamination
- Contamination, 23–25
 Contamination Threat Management Guide (USEPA Response Protocol Toolbox, Module 2), 184–185
 and delayed detection, 24
 in distribution systems, 27
 at fire hydrants, 29
 in individual buildings, 30–31
 in source waters, 25–26
 in storage tanks and reservoirs, 27–29
 potential sites for, 25–31
 at service connections, 29–30
- Site Characterization and Sampling Guide (USEPA Response Protocol Toolbox, Module 3), 185, 202
 at treatment plants, 26–27
See also Decontamination
- “Contamination Threat Management Guide,” 184
- Contamination warning systems (CWSs), 147–148
- algae toximeters, 159
 automatic sample archiving, 169
 bacteria-based biosensors, 157–158
 biosensors, 156–161
 cities developing, 171
 comprehensive approach, 169–170

- continuous, online monitoring networks as main component of, 147
- daphnia toximeters, 158
- and data acquisition software, 167
- and data analysis software, 168
- and data management centers, 167
- fish sentinel systems, 159–160, 160f.
- fluorometers, 153
- gas chromatography (GC), 161–162
- gas chromatography-mass spectrometry (GC-MS), 161–162
- gene probes, 165
- gross measurement of organic chemical load, 152–153, 152f.
- and hydraulic modeling, 168
- ideal characteristics, 148
- immunoassay, 165
- integrated systems, 167–168
- light scattering devices, 153, 163–164, 164f.
- limited commercial development of online monitoring technology, 165–166
- monitoring basic chemical parameters as surrogates for contaminants, 149–151
- multi-angle light-scattering (MALS) technique, 163
- multi-array sensors, 156
- multi-parameter panels, 154–156, 154f., 155f.
- mussel monitors, 158
- oil and petroleum detection, 153
- online analytical probes, 153–154
- online chlorine measurement systems, 151
- protein signatures in pathogen monitoring, 164–165
- questions to ask before establishing, 148
- radiation monitoring to detect radionuclides, 160–161
- sensor placement, 166–167
- and signal authentication equipment, 167–168
- signature patterns, 154–156
- for specific chemical contaminants, 161–162
- for specific pathogens, 162–165
- tiered approach, 169
- total organic carbon (TOC) measurement, 149, 150, 151, 152, 209
- and UV-Vis absorbance, 153
- and Water Security Initiative (WSI), 171
- See also* Decontamination
- Continuity of operations plans (COOPs), 63
- Control System Cyber Security Self-Assessment Tool (CS²SAT), 142–143
- Covello, Vincent, 228
- Crisis communications, 223–224, 234
- acknowledging people's fears, 229
- acknowledging uncertainty, 229
- anticipating questions (95 percent rule), 228–229
- avoiding over-reassuring, 229
- citing third parties or sources, 228
- consistent messages, 224
- establishing your own humanity, 229
- information needed by public, 224–225
- and media relations, 225–228
- and mental noise theory, 230
- message mapping, 230–231, 231t., 232t.
- objectives, 224
- plan, 224, 229–230
- primacy-recency (first-last) principle, 228
- and public health responsibility, 224
- public notification, 231–233
- and remediation efforts, 258
- sound bites (27/9/3 rule), 228
- suggesting self-protective actions, 229
- telling what to expect, 229
- See also* National Communications System
- Critical Infrastructure Information Act of 2002, 66
- Critical Infrastructure Partnership Advisory Council (CIPAC), 76
- and security performance measurement, 77–78
- and ten features of water sector specific plan, 76–77
- Water Sector Decontamination Working Group, 251

- Critical Infrastructure Protection Board, 79
- Cryptosporidium*, 10–11, 24, 36, 121 monitoring, 163, 164
- CS²SAT. *See* Control System Cyber Security Self-Assessment Tool
- CWSs. *See* Contamination warning systems
- Cyanide, 38–40, 202
- Cyber attacks, 22–23
- Cyber measures, 144 access control, 141 authentication protocols for vendor or contractor access rights, 143 authentication technologies for remote sensors, 143 formal security program, 143
- Internet as mode of attack (hacking), 137–140
- National Institute of Standards and Technology (NIST) guidelines, 144 risk reduction recommendations, 140–143 and *Roadmap to Security Control Systems in the Water Sector*, 143
- SCADA system security, 141–143 VAs for computerized systems, 140 and Web-based propagation of terrorism, 137
- Cyprus, and Greek terrorist movement, 4
- Decontamination air scouring, 249 and anthrax, 247–248 and Bacillus, 248–249 B chemical cleaning, 249, 250 flushing, 249 grit blasting, 250 high-pressure spray, 250 of infrastructure, 247–249 of water systems, 245–247 of water systems, 252–253 pigging or swabbing, 250 procedures, 249–250 WCIT database on, 246
- See also* Contaminants; Contamination; Contamination warning systems (CWSs)
- Defense in depth, 100
- Deliveries and security, 133–134
- Denver Water, 250
- Department of Homeland Security (DHS). *See* US Department of Homeland Security
- Department of Transportation DOT. *See* US Department of Transportation
- Departmental operations centers (DOCs), 197
- Deterrence or defeat of adversaries, 102
- Domestic terrorist groups and individuals, 9–10
- Doors, 103
- E. coli*, 29–30, 121 monitoring, 164
- Early Warning Inc. Nanotech Biosensor, 165
- Earth Liberation Front (ELF), 9, 21
- Eclox, 203, 204
- Electrical power failure (Northeastern states, 2003), 21–22, 56, 245
- Emergency management, 189–190, 197–198 departmental operations centers (DOCs), 197 emergency operations centers, 195–196 incident command posts, 194, 196–197
- See also* Federal Emergency Management Agency; Incident Command System; National Incident Management System; National Response Framework; National Response Plan
- Emergency Management Assistance Compact (EMAC), 135
- Emergency notifications, 178 to law enforcement, 178–179 to National Response Center (NRC), 180 to neighboring water utilities, 18 to public, 231–233 to state regulatory agencies, 179–180
- Emergency operations centers (EOCs), 195–196 and incident command posts, 196–197 and training, 242

- Emergency Planning for Water Utilities* (M19), ix, 176
- Emergency preparedness. *See* Security and emergency preparedness
- Emergency Response Plan Guidance for Small and Medium Community Water Systems to Comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, 176–177
- Emergency response plans (ERPs), 177–178
- Bioterrorism Act on, 176
- EPA guidelines, 82
- essential components of, 178
- publications, 176–177
- site specificity, 63
- video, 177
- Emergency services contracts, 134
- Emergency Water Quality Sampling Kit, 214
- Employees
- background checks, 128–129
 - as official first responders, 182–183
 - role in emergency response, 182–183
 - security and emergency preparedness among, 129
 - security training, 132
- See also* Insiders (disgruntled employees)
- Entamoeba histolytica*, 30–31
- Environmental Protection Agency (EPA). *See* US Environmental Protection Agency
- Environmental Response Laboratory Network (eRLN), 218
- Environmental Technology Verification (ETV) program, 83–84
- EOCs. *See* Emergency operations centers
- EPANET, 166
- eRLN. *See* Environmental Response Laboratory Network
- ERPs. *See* Emergency response plans
- Executive Order 13231 (President's Critical Infrastructure Protection Board), 138
- Expeditionary unit water purifier (EUWP), 247
- External asset protection, 112–113
- FBI
- on attacks against water utilities, 18
 - and emergency notifications, 178–179
 - InfraGard program, 87–88
 - and LRN laboratories, 216
- Fecal contamination, 24
- Federal Emergency Management Agency (FEMA), 65
- assistance to remediation and recovery efforts, 259
- online course on EOC, 196
- online courses on ICS, 195
- See also* Incident Command System
- Federal regulations and directives, 63–70
- relative scarcity of mandates to water industry, 70–71
- Fences, 99, 106–107
- Filtration, in inactivation of influenza viruses, 270
- Finished water reservoir covers, 114
- Fire hydrants
- backflow-prevention devices, 113–114
 - locks, 113
 - protecting, 113–114
- Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE), 192
- Flu. *See* Pandemic flu
- France
- intentional chemical spill into river, 26
 - plot by al-Qaida to attack water supply network, 47
- Freedom of Information Act, 126–127
- exemption for security-related information, 127
- Gas detectors, 200
- Gates, 106–107
- GCC. *See* Government Coordinating Council
- Geiger–Müller counter, 200
- Geo Centers, Inc., 157
- Gerberding, Julie, 234
- Germany
- post-WWII poisoning of SS soldiers by Jewish retaliators (1946), 44
 - use of biological agents in World War I, 43

- use of biological agents in World War II, 44
- Giardia*, 10–11, 24
- and intentional contamination of Scottish building, 31
 - monitoring, 164
- Giuliani, Rudolph, 234
- Goetz, Bernard, 45
- Government Accountability Office (GAO), on federal funding in security improvement, 83
- Government Coordinating Council (GCC), 76
- Government Emergency Telecommunications Service (GETS), 233
- Greater Cincinnati Water Works, 239
- Grumbles, Ben, 274
- Guidelines for the Physical Security of Wastewater/Storm Water Utilities*, 89
- Guidelines for the Physical Security of Water Utilities*, 89
- Hach
- Guardian Blue System, 154–156
 - Inspector Alert Handheld Nuclear Radiations Monitor, 203
 - Radalert 50 Handheld Nuclear Radiation Monitor, 203
- Hamas, 8
- Harris, Larry Wayne, 37
- Hepatitis A, 38
- Hereth, Larry, 190
- Hezbollah, 8
- Homeland Security Act of 2002 (HSA), 65–66
- Homeland Security Presidential Directives (HSPDs)
- HSPD 5—Management of Domestic Incidents, 67–68, 189
 - HSPD 7—Critical Infrastructure Identification, Prioritization, and Protection, 68
 - HSPD 8—National Preparedness, 68–69, 182–183
 - HSPD 9—Defense of United States Agriculture and Food, 69, 85, 171
 - HSPD 10—Biodefense for the 21st Century, 69
- Homeland Security. *See US Department of Homeland Security*
- Hoover, J. Edgar, 18
- Hurricanes (Katrina et al.), 245
- Hydrants. *See Fire hydrants*
- Hydraulic lift barriers, 105
- Hydraulic modeling, 122–123
- and contamination warning systems, 168
- IAP. *See Incident Action Plan*
- IC Water (Incident Command Water), 85–86, 168
- ICPs. *See Incident command posts*
- ICS. *See Incident Command System*
- ID₅₀. *See Infectious dose 50 percent*
- Idaho National Laboratory, 138
- Idaho Technology, 208–209
- Identification badges and cards, 127–128
- Illinois
- Entamoeba histolytica* event at Chicago hotel, 30–31
 - plot to infect Chicago and St. Louis water with *S. typhi*, 44
- Improvised explosive devices (IEDs), 20–21
- in potential attacks on wastewater systems, 54
- See also* Vehicle-borne improvised explosive devices
- Incendiary devices and flammable substances, 54–55
- Incident action plans (IAPs), 193, 194
- Incident command posts (ICPs), 194
- and emergency operations centers, 196–197
- Incident Command System (ICS), 190, 192
- advisors, 193, 193f.
 - and agency administrators, 193
 - basic structure, 192, 193f.
 - and chief elected officials, 193
 - and chief executive officers, 193
 - command staff, 193–194, 193f.
 - finance and administration section, 193f., 194
 - and incident action plan (IAP), 194
 - incident commander, 193, 193f.
 - logistics section, 193f., 194
 - officers, 193, 193f.

- operations section, 193f., 194
planning section, 193f., 194
single command, 194
and training, 242
unified command, 194, 195, 242
- Infectious dose 50 percent (ID₅₀), 31
- INFICON
HAPSITE GC–MS, 162, 210
Scentograph, 162, 210
- Influenza. *See* Pandemic flu
- Information management
confidential information, 126
FOIA exemption for security-related information, 127
and Freedom of Information Act, 126–127
public information, 126
release of sensitive information, 125–127
restricted information, 126
See also Media relations
- Information Security Analysis Center (ISAC), 77
- InfraGard program, 87–88
- Insiders (disgruntled employees), 10, 46, 129
identifying and helping troubled insiders, 127
and physical protection systems, 102
- See also* Employee background checks; Identification badges and cards
- Intelligent Aquatic Biomonitoring System, 160
- Interdependencies among infrastructures, 23, 55–56
- Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*, 89
- Interim Voluntary Guidelines for Developing an Online Contaminant Monitoring System*, 172
- Interim Voluntary Security Guidance for Wastewater/Storm Water Utilities*, 89
- Interim Voluntary Security Guidance for Water Utilities*, 89
- International (transnational) terrorist groups, 8–9
- Internet. *See* Cyber measures
- Intrusion detection, 107–108
- and automatic shutdown of facilities, 110
exterior sensors, 108–109
interior sensors, 109–110
- IQ Toxicity Test, 203, 204–205
- Iraq
attacks involving IEDs and chlorine tanks, 47
Baghdad pipeline destroyed by VBIED, 21
chlorine gas attacks, 22
and terrorist attacks, 5
- Irish Republican Army (IRA), 8, 21
- ISAC. *See* Information Security Analysis Center
- ISAC. *See* Water Information Sharing and Analysis Center
- Islamic fundamentalism and jihadism, 9–10, 12–16
history of, 12–13
- Israel, attempted contamination of hospital, 31
- Italy
injection of contaminants into bottled water stocks (2003), 47
and Moroccan men's plot to poison water with cyanide, 39
- IVins, Bruce, 5, 7
- Japan
deliberate contamination of hospitals by microbiologist, 37
sarın attack (1995), 12, 40–41
use of biological agents in World War II, 36, 37, 43–44
- Jersey barriers, 105
- JMAR BioSentry System, 163–164, 164f.
- Jordan, and Iraqi plot to poison US troops' water tank, 47
- Kaczynski, Theodore, 9
- Kaffa (1346), 43
- Kentucky
explosion resulting from flammable substance in Louisville sewage system (1981), 57–58, 58f.
- illegal discharge of toxic compounds into Louisville wastewater system (1977), 57

- Kenya, and American embassy bombing (1998), 8
- Keys, control of, 104, 132–133
- Kosovo, well contamination by Yugoslav federal forces, 46
- Ku Klux Klan, 1
- Kurdish Workers' Party, 8
- Large Water System Emergency Response Outline*, 176–177
- Lashkar-e-Taiba, 8
- Lavy, Thomas Lewis, 34
- Lebanon, and US Marines, 4, 8
- Lethal dose 50 percent (LD_{50}), 31–32
- Lighting, 104–105
- Locks, 103–104
- Louisiana, and attempted theft of anhydrous ammonia from wastewater facility (2003), 59
- LRN laboratories (Centers for Disease Control), 216–217
- Ludlum Model 2241-3RK Response Kit, 203
- Making the Nation Safer, 66–67
- Manhole covers, securing, 114
- Mao Tse-tung, 7
- Markov, Georgi, 34
- Maryland
- chemical intrusion destroying biological treatment process at wastewater plant (Hagerstown, 2002), 60
 - and emergency notifications, 179–180
- Massachusetts, accidental contamination at treatment plant, 27
- McVeigh, Timothy, 6, 9, 21
- Medaka Sensor, 160
- Media relations, 225
- and “ambush interviews,” 227
 - anticipating public perceptions and fears, 226
 - and assigning blame, 227
 - avoiding conjecture or speculation, 227
 - avoiding discussion of costs prematurely, 227
 - avoiding speaking on behalf of other organizations, 227
- developing working relationship prior to emergencies, 225
- and executives, 226
- fact sheets, 226
- and honesty, 228
- and hypothetical questions, 227
- keeping the message simple, 227
- and media deadlines, 227–228
- and “no comment,” 227
- objectives for interviews or press conferences, 226
- and off-the-record comments, 227
- one person as point-of-contact, 226
- and open body language, 227
- and personal emotions, 228
- preparation before meeting with media, 226
- press conferences away from emergency command centers, 226
- press release templates, 226
- and public information officers, 226
- repeating question before answering, 226–227
- and sensational or irrelevant questions, 227
- stating utility's priorities, 226
- and training, 241
- and utility specialists, 226
- See also Crisis communications; Information management*
- Mexico, explosions resulting from gasoline leak into sewer system (Guadalajara, 1992), 59–60, 60f.
- Michigan, and ELF incident, 21
- Microtox, 203–204
- Militia groups, 1
- Missouri
- distribution system contamination incident, 29–30
 - salmonellosis incident in storage tanks, 27–28, 37
- Mitigation measures, 99
- backflow-prevention program, 122
 - chlorine and chloramine management, 120–121
 - cyber measures, 137–144
 - defense (or protection) in depth, 100
 - and hydraulic modeling, 122–123
 - and multiple benefits, 100, 274
 - operational, 117–123
 - paying for, 101

- physical protection systems, 101–116
policies, procedures, and training, 125–135
and system plans, 122
system redundancy, 100, 117–120
trident approach (short-term, long-term, future), 100–101
- Mohammed, Khalid Sheikh, 7
- Moldaenke daphnia toximeter, 158
- Mongolia, and Japanese use of biological agents (WWII), 43–44
- Monongahela River diesel spill (1988), 26
- MosselMonitor, 158
- “Mother of Satan.” *See* Triacetone triperoxide
- Motion detectors, 110
- MSA Orion Multi-Gas Detector, 200
- MSA Passport PID II Portable Gas Detector, 210
- Mueller, Robert, 18
- MultiRAE Plus One to Five Gas Monitor with VOC Detection, 200
- Mumbai, India, attacks of 2008, 15
- Muslim Brotherhood, 13
- Mutual aid agreements, 134–135
and remediation and recovery, 253–254
- National Communications System (NCS), 233–234
- National Drinking Water Advisory Council (NDWAC)
14 security features for water and wastewater utilities, 76
Water Security Working Group (WSWG), 75
- National Environmental Methods Index for Chemical, Biological, and Radiological Methods (NEMI-CBR), 220
- National Environmental Training Center, 97
- National Environmental, Safety, and Health Training Association (NESHTA), 97
ERP guidance video, 177
- National Homeland Security Research Center (NHSRC), 81, 84, 166
decontamination research, 251
- Standardized Analytical Methods (SAM) document, 219–220
- TEVA contamination monitoring research project, 166
- National Incident Management System (NIMS), 190, 192
and National Response Plan, 191
- National Infrastructure Advisory Council (NIAC), 129
- National Infrastructure Protection Center (NIPC), 64
InfraGard program, 87–88
- National Infrastructure Protection Plan (NIPP), 70
critical infrastructures and related agencies, 70, 71t.
sector specific plans, 73
- National Institute of Standards and Technology (NIST)
cyber security guidelines, 144
remediation and recovery research, 250
- National laboratories (Centers for Disease Control), 216
- National Operations Center, 191
- National Pollutant Discharge Elimination System (NPDES), 157
- National Response Center (NRC), 66, 180
- National Response Framework (NRF), 191, 258
- National Response Plan (NRP), 190–191
and NIMS, 191
- National Rural Water Association (NRWA), 96, 97
- National Water Sector Cyber Security Committee, 143–144
- NCS. *See* National Communications System
- NDWAC. *See* National Drinking Water Advisory Council
- Neo-Nazi groups
Germany, 8
US, 1
- Nepal, water system attack, 21 (2006)
- Nerve agents, 40–41
- NESHTA. *See* National Environmental, Safety, and Health Training Association

- New England Water Works Association (NEWWA), 97
- New York
- contamination of NYC water with plutonium, 45–46
 - NYC Office of Emergency Management Headquarters, 196
- NHSRC. *See* National Homeland Security Research Center
- NIAC. *See* National Infrastructure Advisory Council
- NIMS. *See* National Incident Management System
- 9/11, 5, 8, 12, 15, 196
- and increased concern about terrorism, 1, 273
 - effect on security approach, ix–x, 79, 273–274
- NIPC. *See* National Infrastructure Protection Center
- NIPP. *See* National Infrastructure Protection Plan
- NIST. *See* National Institute of Standards and Technology
- North Carolina, fire hydrant contamination incident, 29
- NPC (nuclear, biological, chemical) weapons, 11–12
- use in war, 12
- NRC. *See* National Response Center
- NRF. *See* National Response Framework
- NRP. *See* National Response Plan
- NRWA. *See* National Rural Water Association
- Ohio
- explosions resulting from flammable substance in wastewater system (Akron, 1977), 58
 - insider contamination of Canton municipal wells with trichloroethylene, 46
- Ohio River diesel spill (1988), 26
- The One Percent Doctrine*, 39
- One-way teeth, 106
- Ontario, bottled water tampering case (2007), 47
- Operational responses
- continuity of operations plans (COOPs), 63
- to drinking water contamination threats, 182
- mitigation measures, 117–123
- to wastewater contamination threats, 181
- Order of the Rising Sun, 44
- Oregon, and *Salmonella* contamination by religious cult, 37, 45
- Pakistan, and Sunni militants' plot to poison Karachi water with cyanide, 47
- Palestine
- and Jewish terrorist movement (1940s), 4
 - and state-sponsored terrorism, 8
- Palestine Islamic Jihad, 8
- Palestinian Liberation Organization (PLO), 5, 8
- Pandemic flu, 261
- and antigenic drift, 262
 - and antigenic shifts, 262, 263
 - avian viruses, 263
 - deaths from flu, 263
 - effects on water utilities, 265–266
 - and employees' family responsibilities, 267
 - H1N1 swine flu virus, 262, 265
 - H5N1 avian virus, 264–265, 269
 - H5N2 avian virus, 269
 - infection control in workplace, 268
 - Influenza A viruses, 262–263
 - influenza transmission via water, 268–270
 - information resources, 270–271
 - and novel virus strains, 263, 264
 - and potential labor and legal issues, 267–268
 - preparing for, 266–267
 - species susceptible to influenza viruses, 261
 - swine viruses, 273–274
- twentieth-century occurrences, 261
- and vaccinations, 262, 263
 - and vaccinations for public utility personnel, 267
 - virus behavior, 261
 - virus genera, 261
 - virus reassortment, 262–263
- Pandemic Influenza: Preparedness, Response, and Recovery*, 270–271
- Pathogenic microbes, 34–38

- field detection and identification, 207–209
monitoring, 162–165
See also Biological warfare
Patriot Act of 2001, 66, 67t.
PCR, 207
Pennsylvania
accidental discharge of potassium thiocyanate into sewer system (Philadelphia, 2006), 60
and emergency notifications, 179
hacker attack on SCADA system, 139
insider contamination of Duquesne water plant, 46
and intentional pesticide contamination of Pittsburgh water line, 40, 44–45
smallpox blanket incident (1763), 43
Pentagon, and attack of 9/11, 2, 6, 55
People's Temple incident, 38
Pesticides, 40
Philippines, and pesticide contamination of police department's water containers, 46
Physical attacks, 17, 20–21
Physical protection systems, 101–103, 115–116
access control, 103–104
barriers (perimeter security), 105–106
defeat of adversaries, 102
deterrence of adversaries, 102
external asset protection, 112–113
fences, walls, and gates, 99, 106–107
and insiders, 102
intrusion detection, 107–110
lighting, 104–105
security guards and patrols, 114–115
site and building design, 106
steps in philosophy of, 101–102
visual surveillance (CCTV), 110–112
PipelineNet, 86, 122, 168
Pittsburgh (Pa.) Water and Sewer Authority, ix
chlordane–kerosene injection incident (remediation and recovery case study), 255–256, 273–274
field concentration method, 211
Plutonium, 45–46
Policies and procedures, 125
community awareness of security issues, 129–130
controlled access to key facilities, 131
crisis management human resources program, 127–129
deliveries, 133–134
emergency notifications, 133
emergency services contracts, 134
employee background checks, 128–129
identification badges and cards, 127–128
information and records management, 125–127
key security, 132–133
mutual aid agreements, 134–135
public access to storage and treatment facilities, 130–131
regarding weapons, 129
release of sensitive information, 125–126
security and emergency preparedness among employees, 129
See also Cyber measures; Information management
Portland (Ore.) Water Bureau, 130–131
ppbRAE Plus Monitor, 209–210
PPSs. *See* Physical protection systems
Preparedness. *See* Security and emergency preparedness
President's Commission on Critical Infrastructure, 64
President's Critical Infrastructure Assurance Office, 17–18, 23–24
President's Critical Infrastructure Protection Board, 138
Presidential Decision Directive 63 (PDD 63, 1998), 64, 75
Principal federal officials (PFOs), 189–190
Protecting Your Community's Assets: A Guide for Small Wastewater Systems, 97
Protection in depth, 100
Public health, 185–187
Public Health Security and Bioterrorism Preparedness and Response Act of 2002. *See* Bioterrorism Act of 2002
Public information. *See* Crisis communications; Media relations
Public Notification Rule, 232
Public participation

- access to reservoirs, 130–131
 citizens' observation and reporting of suspicious activity, 129–130
 treatment facility tours, 131
- Q**adhafi, Mu'ammar, 8
Qaida, al-, 1, 4, 8, 12–15
 and media, 5
 plot to attack Paris water supply network, 47
 possible plot to sabotage American drinking water systems in Afghanistan, 46
 threat to poison US water systems, 47
 and VBIEDs, 21
Qutb, Sayyid, 13
- R.A.P.I.D. LT PCR systems, 208–209
Radiation
 monitoring, 160–161
 screening, 202–203
Radionuclides, 42
RAMCAP (risk analysis management for critical asset protection), 98
RAM-W. *See* Risk Assessment Methodology for Water
Rapid field enzyme test, 207
Rapid field testing of water, 201–202, 208t., 212t.
 acute toxicity screening, 203–205
 core testing, 202
 organic compound detection and identification, 209–211
 pathogen detection and identification, 207–209
 radiation screening, 202–203
 rapid enzyme test, 207
 rapid immunoassay, 205–207
Rassam, Ahmed, 8
Recommendations and Proposed Strategic Plan: Water Sector Decontamination Priorities, 251
 Records management, 126–127
Recovery. *See* Remediation and recovery
Red Army Faction, 8
 and botulinum toxins, 24
Reference laboratories, 217
Regional Laboratory Networks, 217
Remediation and recovery, 76, 245
 alternative water supplies and sanitary services, 256, 257
 analysis of alternatives, 258
 business continuity plans, 259
 case study (Pittsburgh chlordane–kerosene injection incident), 255–256, 273–274
 communication to restore public confidence, 258
 decontamination of infrastructure, 247–249
 decontamination of wastewater systems, 252–253
 decontamination of water systems, 245–247
 decontamination procedures, 249–250
 government assistance, 258–259
 postremediation monitoring, 258
 remedial design and action, 258
Remediation and Recovery Guide (USEPA Response Protocol Toolbox, Module 6), 187, 257–258
 research, 250–251
 risk assessment, 257
 system characterization–feasibility study, 257
 technology selection, 258
 USEPA guidance, 257–258
Reservoir covers, 114
Response Guidelines, 184
Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents, 81, 82, 183–187, 186f., 199
 Module 1 (Water-Utility Planning Guide), 184
 Module 2 (Contamination Threat Management Guide), 184–185
 Module 3 (Site Characterization and Sampling Guide), 185, 202
 Module 4 (Analytical Guide), 185
 Module 5 (Public Health Response Guide), 185–187
 Module 6 (Remediation and Recovery Guide), 187, 257–258
 threat management decision tree, 185, 186f.
Response to incidents and threats, 175–176

- emergency notifications, 178–180
operational responses, 181–182
role of utility personnel, 182–183
USEPA Response Protocol Toolboxes, 183–187, 186f.
See also Analytical response; Emergency management; Emergency response plans
- Ricin, 34
- Ridge, Tom, 190
- Risk Assessment Methodology for Water (RAM-W), 93, 95
steps in, 93–95
- Risk
defined, 92
See also Mitigation measures
- RiverSpill. *See* IC Water Roadmap to Security Control Systems in the Water Sector, 143
- Romania, alleged nerve agent attack by secret police, 41–42, 46
- Rome, ancient, 43
- Rotavirus, 24
- Rudolph, Eric, 9
- Safe Drinking Water Act (SDWA), 63, 91, 176. *See also* Bioterrorism Act of 2002
- Safety Act of 2002, 66
- Salmonella* and salmonellosis, 27–28, 37–38, 44, 121
- Sampling
automatic sample archiving, 169
Response Protocol Toolbox Module 3 (Site Characterization and Sampling Guide), 185, 202, 214
sample collection, 213–214
sample concentration in the field, 211–213, 213f.
- USEPA Sampling Guidance for Unknown Contaminants in Drinking Water, 199
- Sandia National Laboratories, 93, 164–165
and CANARY software, 168
- Sandman, Peter, 229
- Sarin, 12, 40–41
- Saudi Arabia
al-Qaida threat to poison US water systems, 47
- truck bombing (1996), 8
- SCADA systems
avoidance of remote terminals, 142
and CS²SAT for assessing security, 142–143
data logs, 142
and hacker attacks, 137–140
interference with, 22–23, 55
isolation from Internet and other networks, 141–142
shutting down in event of security threat, 142
vulnerabilities in, 139
- Schuchat, Anne, 266
- Scotland, and intentional *Giardia* contamination at apartment complex, 31
- SDWA. *See* Safe Drinking Water Act
- Sector specific plans (SSPs), 73. *See also* Water sector specific plan
- Security
all-hazards approach, x, 274
four pillars of (prevention, detection, response, recovery), 76
performance measurement, 77–78
reports and tools, 79–90
threat-based guidelines, 89
- Security Analysis and Response for Water Utilities*, x, 176
- Security and emergency preparedness, 273–274
among employees, 129
and community awareness, 129–130
- Security guards and patrols, 114–115
- Security Product Guide*, 80–81, 202
- Security Self Assessment Guide for Small and Very Small Systems, 96–97
- SEMS (Security and Emergency Management System), 97
- Sensor Placement Optimization Tool (TEVA-SPOT), 166
- Sentinel laboratories, 217
- September 11, 2001. *See* 9/11
- Service connections, protecting, 113
- Sewer lines, as conduits for terrorists, 55
- SewerNet, 86, 122, 168
- Shigella* and shigellosis, 24, 37–38, 121
- Sievers 900 Portable TOC Analyzer, 209
- Site and building design, 106

- Small water and wastewater systems
 ERP guidance publications and video, 177
 security guides, 96–97
SMART (Sensitive Membrane Antigen Rapid Test) Ticket, 206–207
 Small utilities, security tools for, 96–97
 Sodium hypochlorite, 120
 Somalia, and US troops, 4, 8
 Soman, 40, 41
 South Carolina
 chlorine gas release, 22
 ricin incident at postal facility, 34
 Soviet Union
 anthrax release, 35
 and biological weapons, 44
 and Japanese use of biological agents (WWII), 43–44
 Spain, and Madrid bombings (2004), 4, 9, 15, 137
 Sri Lanka, water system attack, 21
 SSPs. *See* Sector specific plans
 Standardized Analytical Methods (SAM) document, 220
 State terrorism, 7
 State-sponsored terrorist groups, 7–8
Strategic Plan for Homeland Security, 82
 Support Anti-Terrorism by Fostering Effective Technologies Act. *See* Safety Act of 2002
 System plans, 122
 System redundancy, 117
 alternate raw water sources and intakes, 117
 backup electrical generators, 119
 backup mains, 100
 backup pumping facilities, 117–118
 backup treatment facilities, 117–118
 chemicals on hand for 30 days of treatment, 119
 contingency storage of possibly contaminated wastewater, 118
 critical spare parts, 118
 dual storage sources for each service area or pressure zone, 118
 interconnection water supply agreements, 119
 isolation of finished water storage, 118
 multiple parallel treatment trains for wastewater systems, 118–119
 online chlorine analyzers throughout distribution system, 100
 standby storage, equipment, and electrical components, 118
 storage of one or more days' supply of finished water, 119–120
 uninterruptible power supplies for electrically powered systems, 119
 Tabun, 40, 41
 Tajikistan, cyanide poisoning incident, 38–39
 Tamil Tigers, 21
 Tanzania, and American embassy bombing (1998), 8
 Technical Associates radiation monitor, 161
Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality, 172
 Technology Testing and Evaluation Program (TTEP), 83–84
 Tenix Corp., 164–165
 Terrorism, 1–2
 as adversaries' response to US power, 2
 and casualties, 5–6
 and coercion of government decisions, 6
 defined, 3–4
 and deniability, 5
 by domestic groups and individuals, 9–10
 general failure of, 4
 goals of, 5–6
 history of, 1
 and innocent third parties, 3–4
 by insiders (disgruntled employees), 10
 by international (transnational) groups, 8–9
 and Islamic fundamentalism and jihadism, 9–10, 12–16
 and lone wolves, 7, 9
 occasional successes of, 4
 perpetrator categories, 7–11
 and perpetrator's motive, 3
 and perspective of observer, 3

- as political statement, 5
and public protection issues, 6
and publicity, 5
reasons for choice of, 4–5
and selection of targets, 6
as show of strength, 6
socioeconomic and psychological profiles, 7
state terrorism, 7
by state-sponsored groups, 7–8
and timing of attacks, 6
in US, 1, 2–3
vandalism as, 10–11
and weapons of mass destruction, 3, 11–12
and widespread economic loss, 6
- TEVA. *See Threat Ensemble Vulnerability Assessment*
- TEVA-SPOT. *See Sensor Placement Optimization Tool*
- Texas, and diversion of gasoline into wastewater system (Conroe, 1994), 60
- Threat Ensemble Vulnerability Assessment (TEVA), 84
- Threat management decision tree, 185, 186f.
- Total organic carbon (TOC) measurement, 149, 150, 151, 152, 209
- Toxic substances, in potential attacks on wastewater systems, 55
- Training, 125, 237
conducting exercises, 240–241
enhanced functional exercises, 238
full-scale exercises, 239
guidance materials, 243
“Hot Wash” (post-exercise review), 242–243
and media relations, 241
and multi-agency response, 242
pre-exercise, 239–240
roundtable discussions, 238
scenario-driven exercises, 240–241
and sensitive information, 241
simple functional exercises, 238
tabletop exercises, 238–239
Top-Off series, 239
for utility employees and contractors, 132
value of exercises, 237–238
- videos for public safety personnel, 130
- Triacetone triperoxide (TATP), 20–21
- Trichloroethylene, 46
- Triple fencing, 99
- Truck or car bombs
in potential attacks on wastewater systems, 54
- Saudi Arabia (1996), 8
- TTEP. *See Technology Testing and Evaluation Program*
- Turkey, and plot to poison air force water supply by Kurdish terrorists, 46
- US Army Corps of Engineers, 258
- US Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, 12
- US Department of Homeland Security (DHS), 6, 65–66, 70
color-coded threat levels and water treatment facility tours, 131
- Control System Cyber Security Self-Assessment Tool (CS²SAT), 142–143
- establishment of, 79
- Joint Field Office, 91
- National Cyber Security Division, 143
- National Operations Center, 191
- Pandemic Influenza: Preparedness, Response, and Recovery*, 270–271
- principal federal officials (PFOs), 189–190
- US Department of Transportation (DOT), hazardous chemical regulations, 26
- US Environmental Protection Agency (USEPA), 63, 65
assistance to remediation and recovery efforts, 258
- Baseline Threat Information for Vulnerability Assessment of Community Water*, 79–80
- and CANARY software, 168
- contaminant models, 122
- and CWSs, 171
- and directive on water quality surveillance and monitoring, 69

- Environmental Laboratory Compendium, 82, 219
- Environmental Response Laboratory Network (eRLN), 218
- Environmental Technology Verification (ETV) program, 83–84
- EPANET, 166
- ERP guidance publications and video, 176–177
- ERP guidelines, 82
- and ERPs, 91
- hydraulic models, 85–86
- National Homeland Security Research Center (NHSRC), 81, 84, 166, 219–220
- published reports on, 172
- Regional Laboratory Networks, 217
- Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents*, 81, 82, 183–187, 186f.
- Sampling Guidance for Unknown Contaminants in Drinking Water, 199
- and sector specific plan for water sector, 73
- Security Product Guide*, 80–81, 202
- Sensor Placement Optimization Tool (TEVA-SPOT), 166
- Strategic Plan for Homeland Security*, 82
- Technology Testing and Evaluation Program (TTEP), 83–84
- Threat Ensemble Vulnerability Assessment (TEVA), 84
- and VAs, 91, 93, 97
- Wastewater Response Protocol Toolbox*, 81–82, 183–187, 186f.
- Wastewater Threat Document*, 79–80
- Water Assessment Technology Evaluation Research and Security (WATERS) Center, 150–151
- Water Contaminant Information Tool (WCIT), 86–87
- Water Laboratory Alliance (WLA), 217–218
- Water Protection Task Force, 79
- Water Security Division, 79, 85
- Water Security Initiative (WSI), 85, 168, 171
- Water Security Research and Technical Support Action Plan*, 82–83
- water security Web site, 80
- and Water Security Working Group, 79
- WCIT database, 218–219, 246
- See also* National Environmental Methods Index for Chemical, Biological, and Radiological Methods
- US Geological Survey, 220
- Vandals, 10–11
- VAs. *See* Vulnerability assessments
- Vehicle-borne improvised explosive devices (VBIEDs), 20, 21
- Visual surveillance (CCTV), 110–111
- archiving of images, 112
 - and lighting, 111
 - monitoring, 111–112
- Volatile organic compounds (VOCs), 200
- field screening, 200, 209–210
- Vulnerability, defined, 92
- Vulnerability assessments (VAs), 18, 91–92
- for computerized systems, 140
 - elements of, 92–93
 - and FOIA exemption for security-related information, 127
 - and protection of sensitive information, 98–98
 - site specificity, 63
 - videos, 97
- Vulnerability Self-Assessment Tool (VSAT), 95
- key steps, 95–96
- VX, 40, 41
- Walls, 106–107
- WARN program, 134–135, 254
- Wastewater Response Protocol Toolbox, 81–82, 183–187, 186f., 199, 214
- Wastewater systems, 61
- and cascading effects from interdependencies with other infrastructures, 55–56
 - contamination endpoints of concern, 56

- documented incidents of accidents and sabotage, 56–60
- scenarios of concern, 54–56
- USEPA Response Protocol Toolbox, 81–82, 183–187, 186f.
- why they could be targets, 53–54
- See also* Small water and wastewater systems
- Wastewater Threat Document*, 79–80
- Water Contaminant Information Tool (WCIT), 86–87
- Water Environment Federation (WEF), 89, 91
- Water Information Sharing and Analysis Center (ISAC), 18
- Water Information Sharing and Analysis Center (WaterISAC), 88–89
- Water Infrastructure Standards Enhancement Committee, 89
- Water Laboratory Alliance (WLA), 217–218
- Water Protection Task Force, 75
- Water Research Foundation, 250
- Water sector, defined, 73
- Water Sector Coordinating Council (WSCC), 73, 76
- member organizations, 73–74
- Roadmap to Security Control Systems in the Water Sector*, 143
- Water Sector Government Coordinating Council (WSGCC), 73
- Water sector specific plan, 73, 78
- four goals and 10 features, 76–77
- four goals and supporting objectives, 74–75
- Goal 1: Sustain protection of public health and the environment, 74, 76
- Goal 2: Recognize and reduce risks in the water sector, 74, 76
- Goal 3: Maintain a resilient infrastructure, 74–75, 76–77
- Goal 4: Increase communication, outreach, and public confidence, 75, 77
- organizations involved in developing, 73–74
- Water Security Handbook*, 184
- Water Security Initiative (WSI), 85, 168, 171
- Water Security Research and Technical Support Action Plan*, 82–83
- Water Security Working Group (WSWG), 75, 79
- Water SSP. *See* Water sector specific plan
- Water System Security: A Field Guide*, x
- Water systems
- and adequate quantities of water, 17–18
- and adequate water pressure, 17–18
- and cascading effects from interdependencies with other infrastructures, 23
- and contamination events, 17, 23–42
- contamination incidents and threats that have occurred, 42–47
- crucial attributes of, 17–18
- and cyber attacks, 22–23
- effects of attacks on, 17
- likelihood of attacks on, 17–19
- numbers in US, 17
- physical assaults on, 17, 20–21
- and release of hazardous treatment chemicals, 22
- and safety of water, 17–18
- why they could be targets, 19
- WCIT. *See* Water Contaminant Information Tool
- WCIT database, 219
- on decontamination, 246
- Weapons of mass destruction (WMD)
- defined, 11
- detecting, 11
- and Islamic jihadists, 15
- NPC (nuclear, biological, chemical), 11–12
- and question of terrorism, 3
- Weathermen, 7
- White House Office of Homeland Security, 79
- White supremacists, 45. *See also* Aryan Nations; Neo-Nazi groups
- Windows, 104
- Wireless Priority Service (WPS), 233–234
- Wisconsin, and Milwaukee cryptosporidiosis outbreak, 25, 170
- World Trade Center
- attack of 1993, 6, 8
- attack of 2001, 2, 6

- See also* 9/11
World War I biological warfare, 43
World War II biological warfare, 43–44
World Wide Web. *See* Cyber measures
WSCC. *See* Water Sector Coordinating Council
WSGCC. *See* Water Sector Government Coordinating Council
WSI. *See* Water Security Initiative
WSWG. *See* Water Security Working Group
- Yemen, and USS Cole bombing (2000), 8
Yersinia pestis, 36–37
Zambia, water pipeline destroyed by bomb, 21
Zyklon B, 38