Water Security Initiative: Interim Guidance on Developing an Operational Strategy for Contamination Warning Systems

Office of Water (MC 140) EPA 817-R-08-002 September 2008 www.epa.gov/safewater

Office of Water (MC 140)
EPA 817-R-08-002
September 2008
www.epa.gov/safewater

Foreword

The Water Security initiative is a U.S. Environmental Protection Agency (EPA) program that addresses the risk of intentional contamination of drinking water distribution systems. Initiated in response to Homeland Security Presidential Directive 9, the overall goal is to design and deploy contamination warning systems for drinking water utilities. EPA is implementing the Water Security initiative in three phases: (1) development of a conceptual design that achieves timely detection and appropriate response to drinking water contamination incidents; (2) demonstration and evaluation of the conceptual design in full-scale pilots at drinking water utilities; and (3) issuance of guidance and conduct outreach to promote voluntary national adoption of effective and sustainable drinking water contamination warning systems. **Figure F-1** summarizes this process.

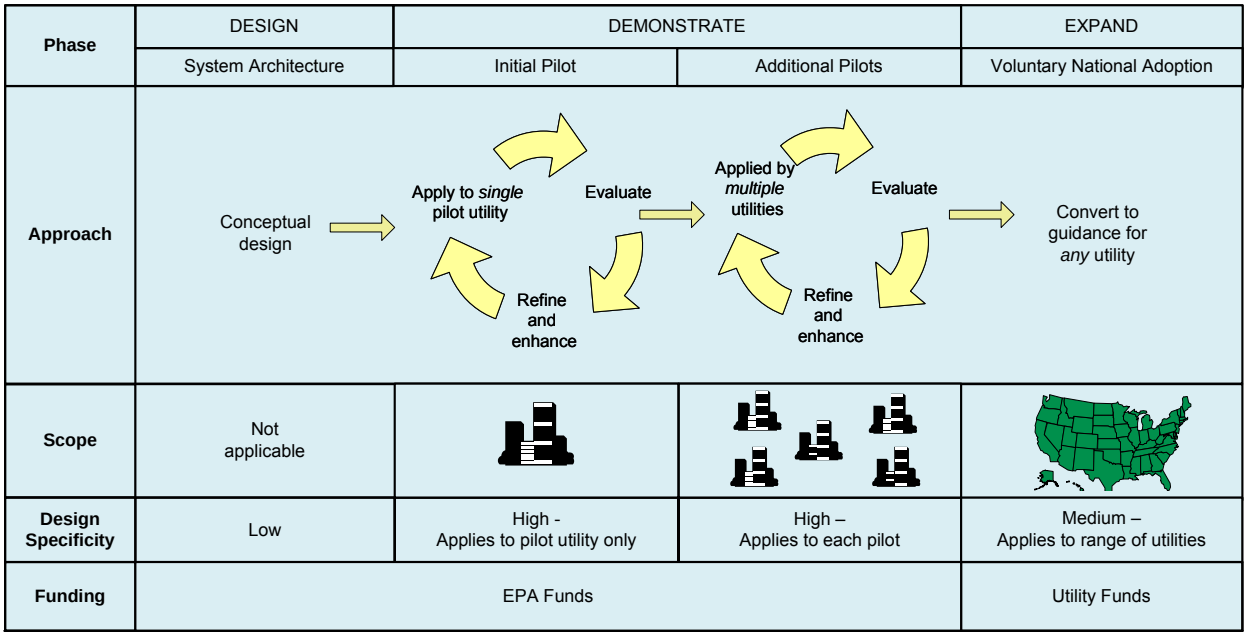

Figure F-1. Overview of EPA's Water Security Initiative

A contamination warning system should be a proactive approach to managing threat warnings that uses advanced monitoring technologies/strategies and enhanced surveillance activities to collect, integrate, analyze, and communicate information. However, it should not be merely a collection of monitors and equipment placed throughout a water distribution system to alert of intrusion or contamination, but rather an exercise in information acquisition and management. Different information streams are captured, managed, analyzed, and interpreted to recognize potential contamination incidents in time to respond effectively. While the contamination warning system should be designed by the drinking water utility, some data sources may be outside of the utility, and in this case, cooperation with partners would likely be important to the success of a contamination warning system. **Figure F-2** illustrates the recommended components of a contamination warning system, as briefly described below:

- **Online water quality monitoring** involves monitoring for typical water quality parameters throughout the distribution system, and comparison with an established base-state to detect possible contamination incidents.
- **Sampling and analysis** involves the collection of distribution system samples that are analyzed for various contaminants and contaminant classes for the purpose of establishing a baseline of contaminant occurrence (contaminants detected, levels detected, and frequency of detections) and method performance, as well as for the purpose of investigating suspected contamination incidents triggered by other monitoring and surveillance components.

- **Enhanced security monitoring** includes the equipment and procedures that detect and respond to security breaches at distribution system facilities.
- **Consumer complaint surveillance** enhances and automates the collection and analysis of consumer calls reporting unusual water quality concerns and compares trends against an established base-state to detect possible contamination incidents.
- **Public health surveillance** involves the analysis of health-related data sources to identify illness in the community that may stem from drinking water contamination.

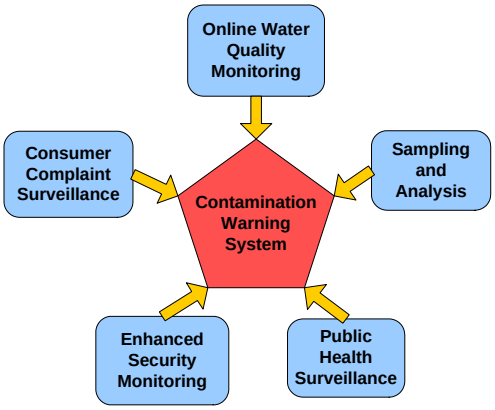

Figure F-2. Multi-Component Approach to a Contamination Warning System

Developing a contamination warning system should also include extensive consequence management planning to develop procedures for investigating and responding to possible contamination incidents detected through the recommended routine monitoring and surveillance components. Once a possible contamination incident has been identified, the consequence management plan should define a process for establishing the credibility of the suspected incident, the response actions that may be taken to minimize public health and economic consequences, and a strategy to ultimately restore the system to normal operations.

In the context of the Water Security initiative, the deployment of a contamination warning system should include the six phases illustrated in **Figure F-3**. EPA is developing a suite of guidance to assist utilities through this process, all of which will be available at EPA's Water Security initiative website (http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm) upon publication.

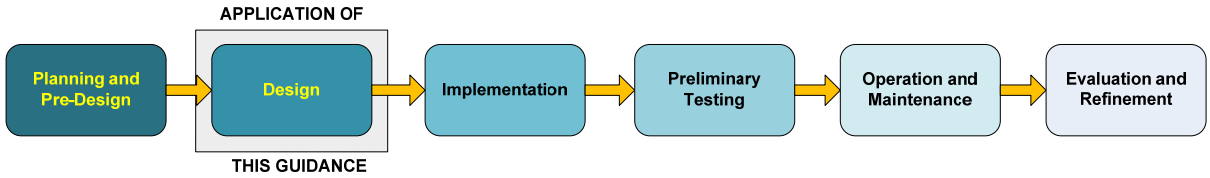

Figure F-3. Recommended Stages of Contamination Warning System Deployment

The document that follows, *Interim Guidance on Developing an Operational Strategy for Contamination Warning Systems*, was written to assist utilities with the development of recommended standard operating procedures for day-to-day operations of the monitoring and surveillance components of a contamination warning system. This interim guidance manual will be revised as needed based on findings of the demonstration pilots and public comment prior to being issued in final form. The guidance emphasizes development of an operational strategy in a manner that integrates the monitoring and surveillance components to provide a timely indication of a possible contamination incident in the distribution system. Development of an operational strategy would typically begin in the design phase of contamination warning system deployment, as indicated in Figure F-3. Once the components of the contamination warning system have been designed and implemented, the preliminary operational strategy developed during the design phase should be refined through subsequent phases of deployment. The ultimate use of the operational strategy developed according to this guidance is to guide day-to-day operation of the contamination warning system during the operation and maintenance phase. A companion document, *Interim Guidance on the Development of a Consequence Management Plan*, was written to assist utilities with the development of plans to guide the utility and partner agencies through the processes of validating, responding to, and recovering from a contamination incident in the distribution system (USEPA, 2008a). Together, the operational strategy and the consequence management plan should comprehensively document the procedures that guide operation of the contamination warning system.

Disclaimer

Note to Readers: The U.S. Environmental Protection Agency (EPA) prepared this guidance to help you enhance the security of your water system. This document does not impose legally binding requirements on EPA, states, tribes, or the regulated community, and it may or may not apply to a particular situation, depending on the circumstances. EPA, state decision-makers, and drinking water utilities retain the discretion to adopt approaches that may differ from this guidance. Any decisions regarding a particular community water system should be made based on applicable statutes and regulations. Therefore, interested parties are free to raise questions and objections about the appropriateness of the application of this guide to a particular situation, and EPA will consider whether the recommendations or interpretations in the guidance are appropriate in that situation based on the law and regulations. EPA may change this guidance in the future. To determine whether EPA has revised this guide or to obtain additional copies, contact the Safe Drinking Water Hotline at 1-800-426-4791 or visit the EPA's Water Security website at www.epa.gov/watersecurity.

Any mention of trade names, companies, products, or services in this guidance does not constitute an endorsement by the Environmental Protection Agency of any non-federal entity, its products, or its services.

Questions concerning this document should be addressed to:

Steve Allgeier
U.S. EPA Water Security Division
26 West Martin Luther King Drive
Mail Code 140
Cincinnati, OH 45268
(513) 569-7131
Allgeier.Steve@epa.gov

or

Jessica Pulz
U.S. EPA Water Security Division
26 West Martin Luther King Drive
Mail Code 140
Cincinnati, OH 45268
(513) 569-7918
Pulz.Jessica@epa.gov

Request for Comments

EPA is soliciting suggestions and recommendations to make this interim guidance manual more complete and user-friendly. Commenters are encouraged to be as specific as possible and to provide references where appropriate. Submit suggestions by e-mail to: watersecurity@epa.gov and indicate that the message relates to the "Interim Guidance on Developing an Operational Strategy for Contamination Warning Systems."

Acknowledgements

EPA's Office of Ground Water and Drinking Water would like to recognize the following individuals and organizations for their assistance and contributions in development of this document:

City of Cincinnati – Greater Cincinnati Water Works

- Steve Allen
- Verna Arnette
- Faye Cossins
- Bill Fromme
- David Hartman
- Jim Holly
- Yeongho Lee
- Mark Menkhaus
- Jeff Pieper
- Jeff Swertfeger
- Mike Tyree

U.S. Environmental Protection Agency – Office of General Counsel

- Leslie Darman

U.S. Environmental Protection Agency – Water Security Division

- Steve Allgeier
- Jeffrey Fencil
- David Harvey
- Elizabeth Hedrick
- Mike Henrie
- Tanya Mottley
- Nancy Muzzy
- Brian Pickard
- Jessica Pulz
- Dan Schmelling
- David Travers
- Katie Umberg

U.S. Environmental Protection Agency – National Homeland Security Research Center

- Hiba Ernst
- John Hall
- Robert Janke
- Matthew Magnuson
- Regan Murray
- Benjamin Packard
- Jeff Szabo
- Cynthia Yund

Contractor Support

- Victoria Blackschleger
- John Chandler
- Kevin Connell
- Mike Denison
- Bill Desing
- Darcy Gibbons
- Adam Haas
- Adrian Hanley
- Yakir Hasit
- Gary Jacobson
- Reese Johnson
- Dan Joy
- Alan Lai
- Greg Meiners
- Bill Phillips
- Curtis Robbins
- Doron Shalvi
- David Watson
- Scott Weinfeld
- Nick Winnike

Utility Reviewers

- Manouchehr Boozarpour, San Francisco Public Utilities Commission
- Don Christie, Los Angeles Department of Water and Power
- Ricardo DeLeon, Metropolitan Water District of Southern California
- Ron Hunsinger, East Bay Municipal Utility District
- Bart Koch, Metropolitan Water District of Southern California
- David Lipsky, New York City Department of Environmental Protection
- Dan Quintanar, Tucson Water
- Steve Rhode, Massachusetts Water Resources Authority
- Stanley States, Pittsburgh Water and Sewer Authority

Table of Contents

SECTION 1.0: INTRODUCTION 1

1.1 KEY CONCEPTS AND DEFINITIONS 1
1.2 DOCUMENT OVERVIEW 3

SECTION 2.0: CONSTRUCTING THE OPERATIONAL STRATEGY 5

2.1 STEP 1: SYSTEM-WIDE ASSESSMENT OF RESOURCES 6
2.2 STEP 2: COMPONENT-LEVEL ANALYSIS – STANDARD OPERATING PROCEDURES 8
2.3 STEP 3: SYSTEM–WIDE INTEGRATION 9

SECTION 3.0: STANDARD OPERATING PROCEDURES 12

3.1 COMPONENT DESCRIPTION 12
3.2 ROLES AND RESPONSIBILITIES 13
3.3 PROCESS FLOW 14
3.4 USER-SPECIFIC CHECKLISTS 15

SECTION 4.0: IMPLEMENTATION AND MAINTENANCE 16

4.1 BASELINE AND PRELIMINARY TESTING 16
4.2 FULL DEPLOYMENT 17
4.3 EVALUATION AND REFINEMENT 18

SECTION 5.0: REFERENCES 20

APPENDIX CASE STUDY: OPERATIONAL STRATEGY FOR THE CINCINNATI CONTAMINATION WARNING SYSTEM 21

A.1 OVERVIEW AND OBJECTIVES 22

OVERVIEW 22
OBJECTIVES 23
OVERVIEW OF ROLES AND RESPONSIBILITIES 23
OVERVIEW OF TRIGGER INVESTIGATION PROCESS FLOWS 24

A.2: ONLINE WATER QUALITY MONITORING STANDARD OPERATING PROCEDURES 26

COMPONENT DESCRIPTION 26
ROLES AND RESPONSIBILITIES 27
PROCESS FLOW 27
CHECKLISTS 31

A.3: SAMPLING AND ANALYSIS STANDARD OPERATING PROCEDURES 32

COMPONENT DESCRIPTION 32
ROLES AND RESPONSIBILITIES 33
PROCESS FLOW 33
CHECKLISTS 38

A.4: ENHANCED SECURITY MONITORING STANDARD OPERATING PROCEDURES 39

COMPONENT DESCRIPTION 39
ROLES AND RESPONSIBILITIES 40
PROCESS FLOW 40
CHECKLISTS 45

A.5: CONSUMER COMPLAINT SURVEILLANCE STANDARD OPERATING PROCEDURES 46

COMPONENT DESCRIPTION 46
ROLES AND RESPONSIBILITIES 47
PROCESS FLOW 48
CHECKLISTS 54

A.6: PUBLIC HEALTH SURVEILLANCE STANDARD OPERATING PROCEDURES 56

COMPONENT DESCRIPTION 56
ROLES AND RESPONSIBILITIES 56
PROCESS FLOWS 57
CHECKLISTS 62

A.7: EXAMPLES OF CONTAMINATION WARNING SYSTEM, TRIGGER INVESTIGATION CHECKLISTS 63

CHECKLIST A-1: CONTAMINATION WARNING SYSTEM TRIGGER INVESTIGATION 64
CHECKLIST A-2: DISTRIBUTION SYSTEM SITE INVESTIGATION 67
CHECKLIST A-3: DISTRIBUTION SYSTEM OPERATIONS REVIEW 69
CHECKLIST A-4: DISTRIBUTION SYSTEM WORK ORDER REVIEW 70
CHECKLIST A-5: SECURITY INCIDENT INVESTIGATION 71
CHECKLIST A-6: WATER QUALITY CONSUMER COMPLAINT INVESTIGATION 74
CHECKLIST A-7: PUBLIC HEALTH SURVEILLANCE TRIGGER INVESTIGATION 76

List of Tables

Table 2-1. Example IT System Inventory 7
Table A-1. Summary of Primary Roles in Routine Contamination Warning System Operations 24
Table A-2. Summary of Process Flows and Trigger Validation Process for Contamination Warning System Components 25
Table A-3. Summary of the Example Online Water Quality Monitoring Network 26
Table A-4. Roles and Responsibilities for Routine Operation of Online Water Quality Monitoring 27
Table A-5. Example Timeline for Validation of a Water Quality Trigger in the Context of an Operational Contamination Warning System 31
Table A-6. Example Checklists used During Investigation of a Water Quality Monitoring Trigger 31
Table A-7. Local Laboratory Network and Sampling Frequency for Maintenance Monitoring 32
Table A-8. Field Methods for Safety and Contaminant Screening 32
Table A-9. Roles and Responsibilities for Routine Operation of Sampling and Analysis 33
Table A-10. Example Timeline for Validation of a Sampling and Analysis Trigger in the Context of an Operational Contamination Warning System 37
Table A-11. Example Checklists used During Investigation of a Sampling and Analysis Trigger 38
Table A-12. Summary of Enhanced Security Monitoring Equipment per Location 39
Table A-13. Roles and Responsibilities for Routine Operation of Enhanced Security Monitoring 40
Table A-14. Example Timeline for Validation of a Security Trigger in the Context of an Operational Contamination Warning System 44
Table A-15. Example Checklists used During Investigation of an Enhanced Security Trigger 45
Table A-16. Summary of the Algorithms used in the Consumer Complaint Surveillance Event Detection System 46
Table A-17. Roles and Responsibilities for Routine Operation of Consumer Complaint Surveillance 47
Table A-18. Example Timeline for Validation of a Consumer Complaint Surveillance Trigger in the Context of an Operational Contamination Warning System 54
Table A-19. Example Checklists used During Investigation of a Consumer Complaint Surveillance Trigger 55
Table A-20. Data Streams, Public Health Partners, and Detection Capabilities 56
Table A-21. Roles and Responsibilities for Routine Operation of Public Health Surveillance 57
Table A-22. Example Timeline for Validation of a Public Health Surveillance Trigger in the Context of an Operational Contamination Warning System 62
Table A-23. Example Checklists used During Trigger Investigation for the Public Health Surveillance Component 62
Table A-24: Example Checklists used During Investigation of Contamination Warning System Triggers 63

List of Figures

Figure F-1. Overview of EPA's Water Security Initiative i
Figure F-2. Multi-Component Approach to a Contamination Warning System ii
Figure F-3. Stages of Contamination Warning System Deployment ii
Figure 1-1. Contamination Warning System Architecture 1
Figure 1-2. Overarching Structure of EPA's Recommended Operational Strategy 2
Figure 2-1. Operational Strategy Development Process 6
Figure 3-1. Roles within a Generic Utility Organizational Hierarchy 13
Figure 3-2. Generic Process Flow and Initial Trigger Validation Process 15
Figure A-1. Process Flow for Online Water Quality Monitoring: Routine Monitoring and Initial Trigger Validation 28
Figure A-2. Process Flow for Sampling and Analysis: Routine Monitoring and Initial Trigger Validation 34
Figure A-3. Process Flow for Enhanced Security Monitoring: Routine Monitoring and Initial Trigger Validation 41
Figure A-4. Process Flow for Consumer Complaint Surveillance: Routine Monitoring 49
Figure A-5. Process Flow for Consumer Complaint Surveillance: Initial Trigger Validation 52
Figure A-6. Process Flow for Public Health Surveillance: Routine Monitoring and Initial Trigger Validation 58

List of Acronyms

The list below includes acronyms approved for use in the Operational Strategy Guidance. Acronyms are defined at first use in the document.

BT	Bioterror (Agent)
CSR	Customer Service Representative
EPA	Environmental Protection Agency
ER	Emergency Room
GIS	Geographic Information System
GUI	Graphical User Interface
IT	Information Technology
IVR	Interactive Voice Response
LAN	Local Area Network
LRN	Laboratory Response Network
ORP	Oxidation-reduction potential
PCB	Polychlorinated Biphenyl
QA	Quality Assurance
QC	Quality Control
SCADA	Supervisory Control and Data Acquisition
SVOC	Semi-volatile Organic Compound
TOC	Total Organic Carbon
VOC	Volatile Organic Compound
WS	Water Security (initiative)
WUERM	Water Utility Emergency Response Manager

Section 1.0: Introduction

This document is part of a series of guidance documents developed to support EPA's Water Security (WS) initiative (formerly known as WaterSentinel). Initiated in response to Homeland Security Presidential Directive 9, the overall goal of the Water Security initiative is to design, deploy, and evaluate contamination warning systems for drinking water utilities. Additional information on the objectives of the Water Security initiative and contamination warning systems can be found in *Water Sentinel System Architecture* (USEPA, 2005). Additional information is also available on the Water Security initiative website at: http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm.

1.1 Key Concepts and Definitions

Figure 1-1 provides an overview of EPA's recommended contamination warning system architecture. It illustrates the role of the operational strategy in guiding routine operation of the monitoring and surveillance components, and the transition to a credibility determination process in the event a contamination threat is deemed possible. Typically, this aspect of the contamination warning system is guided by a consequence management plan, which provides a decision-making framework that should be used to establish credibility, implement response actions, minimize public health and economic impacts, and ultimately return the system to normal operations. (See *Interim Guidance for Developing a Consequence Management Plan*, USEPA, 2008a.)

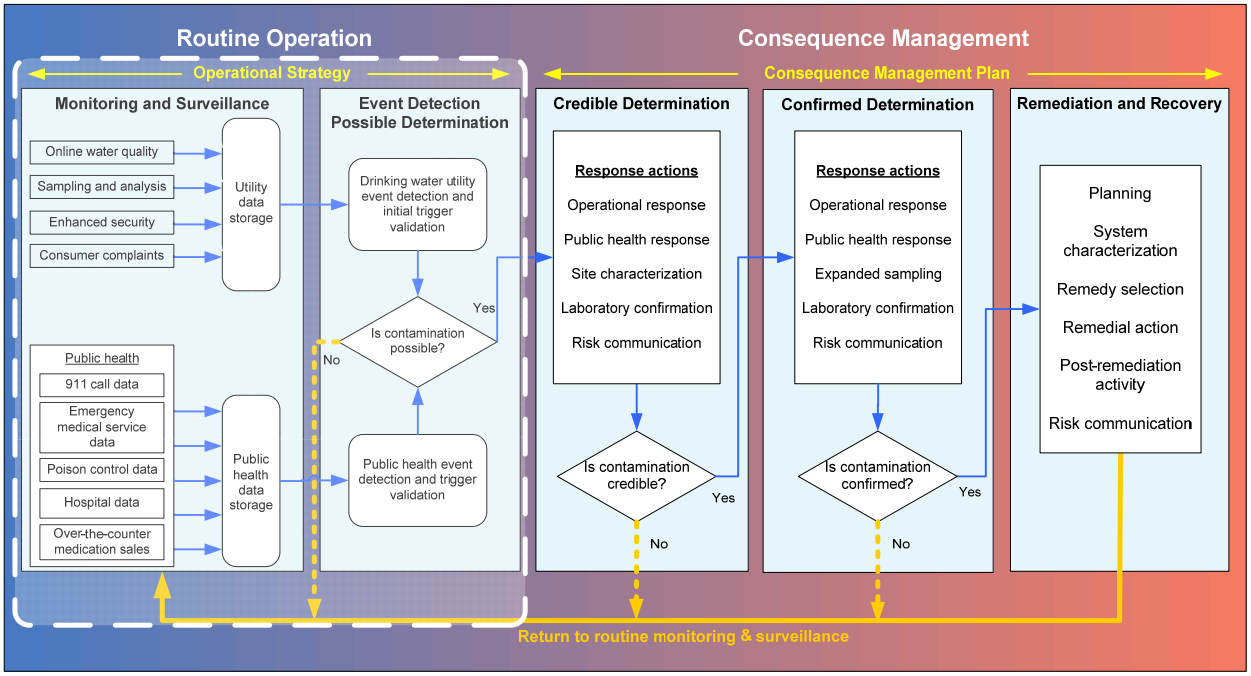

Figure 1-1. Contamination Warning System Architecture

In the context of this guidance, an *operational strategy* is the system-wide integration of the *standard operating procedures* that guide routine operation of the monitoring and surveillance components of a drinking water contamination warning system. Generally, the standard operating procedures establish specific roles and responsibilities, process flows, and procedural activities for each component and the processes for investigating a *trigger* and determining whether or not an anomaly is indicative of a *possible contamination threat*, as described in the EPA's *Response Protocol Toolbox* (USEPA, 2003). An operational strategy may also include checklists that support specific users in the implementation of the standard operating procedures. **Figure 1-2** illustrates the high-level structure of an operational strategy, which is made up of component-level standard operating procedures that in turn are supported by user-

specific checklists. The purpose of this document is to assist drinking water utilities in development of EPA's recommended operational strategy for a contamination warning system based on the high-level structure shown in this figure.

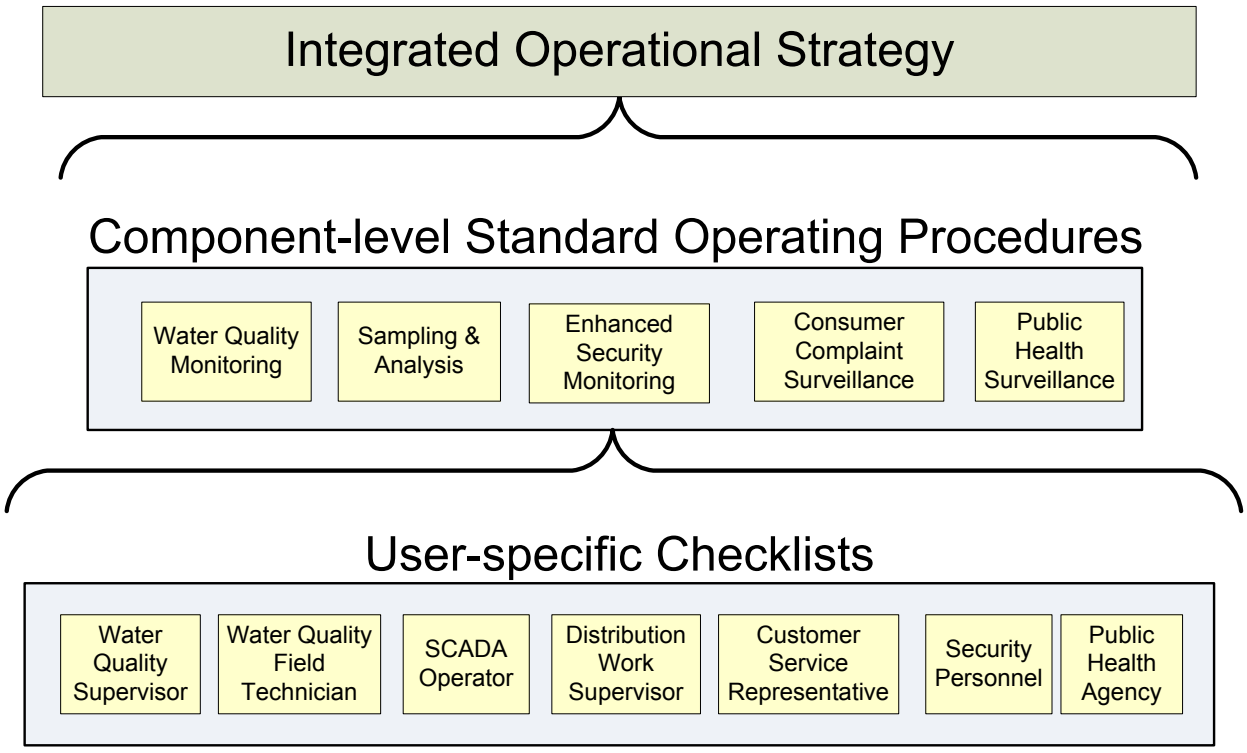

Figure 1-2. Recommended Overarching Structure of Operational Strategy

Additional key concepts and definitions used in this guidance include the following:

- **Routine Operation**. Routine operation refers to the day-to-day monitoring and surveillance activities that are guided by the operational strategy for the contamination warning system. To the extent possible, routine operation of the contamination warning system should be integrated into the routine operations of the drinking water utility.
- **Process Flow**. A process flow is the central element of a standard operating procedure. It describes how routine monitoring and surveillance, event detection, and trigger validation lead to a determination of possible contamination, prior to the implementation of the consequence management plan. Because each component uses different data sources and generates different triggers, the detailed process flow for each component is unique. However, all component process flows should include a common set of process elements.
- **Standard Operating Procedure**. A standard operating procedure should establish specific roles and responsibilities, process flows, and procedural activities for a specified component of the contamination warning system. It should also establish the initial alarm investigation processes that conclude with the determination whether or not a trigger is indicative of a possible contamination threat.
- **Operational Strategy**. The system-wide integration of the standard operating procedures for the routine operation of monitoring and surveillance components of a drinking water contamination warning system. In the event a contamination threat is deemed possible, the operational strategy can facilitate transition to the credibility determination process of a consequence management plan.

- **Job Function**. A description of the duties and responsibilities of a specific job within an organization.
- **User**. In the context of a contamination warning system, a user refers to a specific individual within the drinking water utility or local partner organization who has a defined role and responsibility in the operational strategy.
- **Base-state.** Typical pattern of a parameter, which represents the range of normal conditions observed in a system and captures known causes of variability (such as seasonal or operational changes).
- **Anomaly**. Deviation from an established base-state. For example, a water quality anomaly is a deviation from typical water quality patterns observed over an extended period (i.e., a base-state).
- **Event Detection**. The process by which a deviation from established base-state is identified as an anomaly. The anomaly could be a pattern of unusual water quality readings, a cluster of unusual consumer complaints, or unusual symptoms picked up by a public health surveillance program. For most monitoring and surveillance components, event detection utilizes algorithms to continuously analyze the data stream and filter out perturbations that are part of the established base-state, and signal only those anomalies that are likely to be possible contamination threats. In short, the purpose of the event detection algorithms is to reduce the false positive rate without missing potential contamination incidents.
- **Trigger**. Information from a monitoring and surveillance component indicating an anomalous or unusual condition within the system, which warrants further investigation to determine if it is benign or a possible contamination threat. The nature of a trigger can vary by component and may take the form of an alarm, alert, threshold excursion, or warning. Event detection algorithms are the tool by which triggers can be identified for most monitoring and surveillance components.
- **Possible Contamination Threat**. In the context of the contamination warning system operational strategy, water contamination should be characterized as possible if the cause of a contamination warning system trigger cannot be identified and/or determined to be benign.
- **Initial Trigger Validation**. The process of investigating potential causes of a contamination warning system trigger to either rule out contamination or determine that contamination is possible. This process is related to event detection, but the latter is typically automated and produces the trigger that is investigated during initial trigger validation as guided by a standard operating procedure.
- **Credibility Determination**. Investigation of a possible contamination threat to determine whether or not additional information, including data from other monitoring and surveillance components, corroborates the information from the validated trigger. If the additional information corroborates the trigger, contamination should be considered credible.
- **Water Utility Emergency Response Manager (WUERM)**. A utility may refer to this position by another title, but regardless, this role should generally be filled by a mid-level manager who can integrate information from multiple monitoring and surveillance components, receive notification of possible contamination events, coordinate the credibility determination process, and initiate the consequence management plan. Additionally, the Water Utility Emergency Response Manager may serve as Incident Commander early on in an investigation.

1.2 Document Overview

This document provides guidance for developing, implementing, and maintaining an operational strategy for a drinking water contamination warning system based on EPA's recommended approach. It provides details and background on the content of EPA's recommended operational strategy; a framework or approach for developing, implementing, and testing the operational strategy; and discusses how to align routine operations of a contamination warning system with existing utility operations to achieve a

sustainable system that realizes dual-use applications. Throughout the document, tips and success stories from the initial contamination warning system pilot in Cincinnati are highlighted to draw attention to useful points for consideration.

The following sections are included in this document:

- **Section 2.0: Constructing the Operational Strategy**. This section describes a step-wise process for developing the operational strategy for contamination warning system deployment.
- **Section 3.0: Standard Operating Procedures**. This section provides an overview of the structure and content of standard operating procedures for monitoring and surveillance activities in a contamination warning system.
- **Section 4.0: Implementation and Maintenance**. This section describes activities associated with implementation and maintenance of the operational strategy including training and exercises.
- **Section 5.0: References.** This section lists references cited throughout the document.
- **Appendix: Case Study.** The appendix provides a case study in development of a contamination warning system operational strategy, which was generalized from the operational strategy developed for the initial pilot in Cincinnati. The case study includes example standard operating procedures and corresponding checklists for each of the monitoring and surveillance components.

Section 2.0: Constructing the Operational Strategy

An operational strategy should integrate the standard operating procedures that guide routine operation of each component of a contamination warning system, and in the event a contamination threat is deemed possible, facilitate transition to the consequence management plan. An equally important application of the operational strategy is to support the development of system requirements during the design phase of contamination warning system deployment. A preliminary operational strategy developed during the design phase of the system that describes how it is envisioned to operate once implemented can help to identify key users and their requirements for access to information, procedures to guide system operation, information systems that may be leveraged to support system development, and requirements for notifications to key users and decision-makers. This is also an opportunity to ensure that the overall processes defined by the component standard operating procedures are compatible with the utility's organizational structure and current job functions to the extent possible.

LESSON LEARNED

At the initial Water Security initiative pilot, development of the operational strategy did not begin until late in the design phase. This resulted in some delays as a point was reached in which further progress could not be made without first clearly defining users and their information needs.

Recommendation: Develop a preliminary operational strategy early in the design process!

In order to develop the preliminary operational strategy, the recommended steps include the following three steps as illustrated in **Figure 2-1**:

1. System-wide assessment of resources
2. Component-specific analysis to develop standard operating procedures
3. System-wide integration of component-specific standard operating procedures into a comprehensive operational strategy for the contamination warning system

While the standard operating procedures developed during Step 2 should be the central element of the operational strategy, the system-wide analyses performed at the beginning and end of the development process can ensure that the system functions as an integrated whole.

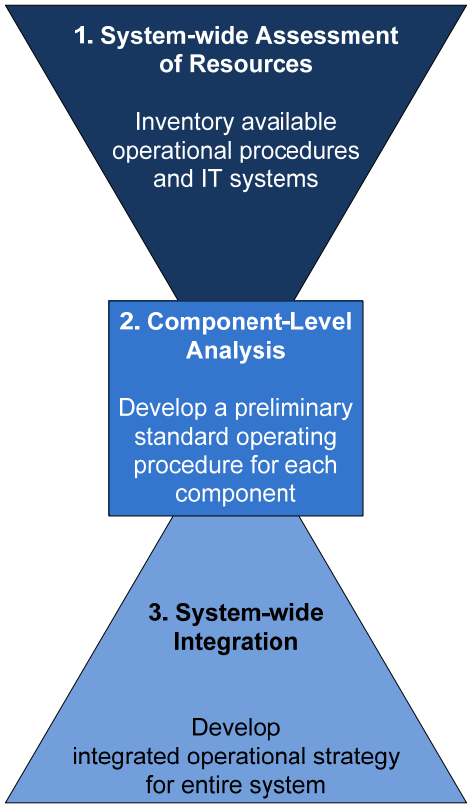

Figure 2-1. Operational Strategy Development Process

The operational strategy should be developed with full and active participation of the project management team, which includes the Water Utility Emergency Response Manager, information technology (IT) staff, and representatives from each division or organization involved in the design or operation of the system. Furthermore, it is important that front-line staff be engaged in the component-level analysis and development of the standard operating procedures to build acceptance of responsibilities for system operation as well as to accurately portray system operations. For some components, this will also include working with local partners outside of the utility who have a critical role in operation. Sections 2.1 through 2.3 provide additional detail on each step of the development process.

2.1 Step 1: System-wide Assessment of Resources

The first step in developing a preliminary operational strategy should be to conduct an initial resource assessment. The resource assessment should include development of an IT system inventory and a review of existing procedures. Although these activities are considered Step 1 of the development process, they may be incomplete or subject to revision based on remaining steps of the development process.

Development of IT System Inventory

Information management is a fundamental aspect of a successful contamination warning system. IT system staff should be engaged early in the contamination warning system deployment process and play an important role in development of the operational strategy. The IT system inventory should include a comprehensive listing of existing IT systems and tools along with applicable user interfaces, a general description of the use of the system/tool in existing operations, and current users. Furthermore, the inventory

REMINDER

Engagement of IT staff as part of the initial system-wide analysis is critical to identification of existing IT systems that may be leveraged, including a review of their capabilities and limitations.

should document the network environment in which each system is deployed, as this may impact the feasibility or ease of data integration across systems. If information is collected from external partners, related IT systems should be identified and included as part of the summary. **Table 2-1** provides an example IT system inventory.

Table 2-1. Example IT System Inventory

System Name	General Description	Users	Network Environment
Call Management System	Provides comprehensive management of customer calls received by the utility. Includes an Interactive Voice Response to triage and direct calls.	Customer Service Representative	Local Area Network
Supervisory Control and Data Acquisition (SCADA)	SCADA system collects, displays, and stores operational data collected from treatment plants, pumping facilities, and other monitoring points throughout the distribution system.	Treatment Plant or Distribution System Operators	Protected Network
Work Order System	Contains information related to work activities in the distribution system, including work orders and work requests.	Distribution Work Supervisor	Local Area Network
Laboratory Information Management System	Contains sample information and detailed analytical results for all water quality analytical data. Information includes data generated in-house as well as data provided by external laboratories.	Laboratory Supervisor, Laboratory Chemist, Laboratory Microbiologist, Managers and Supervisors	Local Area Network
Water Quality Database	Repository for all water quality related data. Includes results associated with investigation of customer water quality complaints, summary analytical results, field investigation results, and special investigations requested from other divisions and departments, such as the Health Department. May be part of a Laboratory Information Management System.	Laboratory Supervisor, Laboratory Chemist, Laboratory Microbiologist, Managers and Supervisors	Local Area Network

Review of Existing Procedures

The second part of the resource assessment should be a review of existing procedures relative to the objectives of the contamination warning system. This includes a review of procedures internal to the utility as well as those of local partners who have a role in operation of the contamination warning system.

Procedures for routine operations at the utility are well established, and some may be applicable to contamination warning system operations. Building on these procedures should help to integrate the contamination warning system with existing procedures and thereby significantly improve the sustainability of the contamination warning system. For example, the initial pilot utility in Cincinnati had established procedures with local law enforcement agencies to support investigation of security breaches at un-staffed facilities, and these procedures were leveraged for enhanced security monitoring. For this component, additional security monitoring capabilities, including video cameras, were installed at facilities already monitored by door or hatch alarms. The video from these facilities is used to remotely assess the security breach and determine if notification to law enforcement was necessary. If so, the existing procedures for notifying law enforcement and investigating the alarm were followed.

HELPFUL HINT

Building on existing procedures for routine operations helps integrate the contamination warning system at the utility and will significantly improve the system's sustainability.

Recommendation: Maximize dual-use applications and leverage existing utility procedures!

To identify existing procedures, determine whether there are established procedures for responding to and investigating alarms generated through SCADA, abnormal analytical results for finished drinking water

samples, security breaches, consumer calls (e.g., taste and odor), and/or public health inquiries. Additional procedures that may be useful include protocols for coordination with: support laboratories, public health agencies, law enforcement, and Hazmat. During this review of existing procedures, enhancements or modifications necessary for contamination warning system operation should be documented to support development of the preliminary operational strategy.

At the conclusion of Step 1, the utility should have sufficient information regarding available resources to facilitate component-level analysis and development of standard operating procedures in Step 2.

2.2 Step 2: Component-Level Analysis – Standard Operating Procedures

The objective of Step 2 is to develop a preliminary standard operating procedure for each of the monitoring and surveillance components. Development of the preliminary standard operating procedures can be facilitated by a multi-disciplinary team with representatives from water quality, IT staff, supervisors from participating divisions, and front-line staff who may have a role in operation of the component. Project management team members such as the Water Utility Emergency Response Manager, senior managers, and IT system administrators may participate in the development of the standard operating procedures for all components, thus providing some continuity to the process and facilitating integration of the individual procedures into an operational strategy during Step 3.

HELPFUL HINT

To develop detailed, component-specific standard operating procedures, form multi-disciplinary teams with representatives from water quality, distribution, engineering, IT, and other divisions as appropriate. Include managers, supervisors, and front-line staff!

The component-level standard operating procedures should contain the elements described in Section 3.0: component description; roles and responsibilities; process flow; and user-specific checklists. In general, development will begin with development of component description followed by establishment of roles and responsibilities. This basic information can then be used to build a process flow, which is the central element of a standard operating procedure.

Section 3.3 provides a general template for a process flow which includes the following elements: routine monitoring and surveillance; event detection; notifications; trigger investigations; and determination regarding possible contamination. Considerations for development of each recommended element of a component-specific standard operating procedure are provided below:

Routine Monitoring and Surveillance

- Identify the users who will be responsible for routine monitoring and surveillance activities of the component, along with the IT systems these users access as part of existing job duties.
- Review routine operations to identify opportunities to effectively integrate contamination warning system monitoring and surveillance activities.
- Determine how users will be alerted to triggers. Options may include visual alarms, audible alarms, email notifications, and text messaging alerts.
- Identify options for data storage and retrieval to support monitoring and surveillance activities.
- Consider how operation of the contamination warning system and staff roles and responsibilities may change during non-business hours.

Event Detection

- Identify potential event detection tools that may be used in the deployment of the component.
- Identify the data sources that will be used by event detection system.

- Identify data output from the event detection system.
- Identify the hardware platform that will host the event detection system and determine how the relevant data streams will be moved to that platform.
- Determine how event detection alarm information will be displayed or otherwise provided to users responsible for routine monitoring.

Notifications

- Determine how users will be notified when an alarm has been received such that they can initiate investigation procedures. Options may include direct notification from users responsible for routine monitoring to more sophisticated and automated notification mechanisms.
- Identify who needs to receive trigger information during each stage of operations: alarm notification, trigger investigation, and determination of possible contamination.

Trigger Investigation

- Identify the users who will be responsible for investigation and validation of triggers for the component, along with the IT systems these users access as part of existing job duties.
- Define the process for conducting the trigger investigation, including all data sources that will be used during the investigation. Determine the data requirements for each specific user, the data system from which each user can access the required data, and the process by which the investigation occurs.
- Evaluate approaches to consolidate data and information used during trigger validation in order to streamline the process and reduce the time required for the investigation.

Determination Regarding Possible Contamination

- Identify who will make the determination regarding possible contamination and the information needed to make this determination.

Once the process flow has been developed, checklists can be derived from the activities outlined in the process flow. In general, checklists should be developed to support specific end-users in fulfilling their role in routine operation of the monitoring and surveillance component.

At the conclusion of Step 2, a preliminary standard operating procedure should exist for each monitoring and surveillance component. Furthermore, these procedures should have been vetted with the front-line staff responsible for day-to-day operation of the system.

2.3 Step 3: System–wide Integration

The final step in developing a preliminary operational strategy is to determine how to effectively integrate all component-level operating procedures into a functional contamination warning system. In order to accomplish this step, the project management team should conduct an analysis of each component-specific standard operating procedure to identify inconsistencies as well as opportunities to streamline and optimize procedures across components. The basic framework for this analysis should include a cross-component evaluation of roles and responsibilities, process flows, timelines, notifications, and checklists. This analysis should result in improved consistency across components as well as more effective leveraging of resources.

Considerations during the system-wide integration step should include the following:

- **Roles and Responsibilities**. For each identified user, verify that their roles and responsibilities are consistent across all components with respect to routine job functions as well as their role in each component.
- **Process Flow**. Verify consistent application of the standard contamination warning system process: routine monitoring and surveillance, event detection, notifications, trigger investigation, and determination of possible contamination. In particular, verify that there is consistency in terms of the level of trigger validation to determine if contamination is possible and timing of notification to the Water Utility Emergency Response Manager. Each standard operating procedure ends with a determination of possible contamination, at which point they include a step to transition to the consequence management plan if contamination is deemed possible.
- **Timelines**. The time to investigate a trigger may vary across components, but should generally reach the point of determining whether or not contamination is possible within a few hours. Through the evaluation of the process flows, similarities may be identified across components. It is important to evaluate and reconcile the timelines for these components so that similar steps and processes occur in a similar timeframe. In addition, opportunities to streamline the process flows may also result in more timely decisions. In a preliminary operational strategy, these timelines are estimates that should be refined through preliminary testing and operation of the system.
- **Notifications**. Based on the process flows, all component-level standard operating procedures should generally conclude with notification of the Water Utility Emergency Response Manager when contamination has been deemed possible. Other notifications occur throughout each step of the process. It is important to consider whether the same individual(s) may receive notifications based on information generated from multiple components. Where this is the case, the mechanism for notification, as well as the information provided, should be consistent. It is also possible that through this analysis, it may be necessary to expand notifications to other individuals or departments within the utility in order to facilitate timely investigation of alarms.
- **Checklists**. During Step 2 of the development process, checklists may have been developed to support implementation of component-level standard operating procedures. During the system-wide integration, these checklists should be analyzed and combined when possible. The resulting checklists should be designed to support specific users in their investigation of triggers for all components in which they have a role. This will help to ensure that user roles and responsibilities are aligned across components and should generally streamline the investigation process.

The system-level analysis can be facilitated by developing summary tables that compile similar information across all components. A tabular summary of roles and responsibilities might include a listing of all identified users, the description of their role/responsibility, and an indication of the component(s) for which they have an operational role. A tabular summary of component-level process flows might include the process for event detection, a description of the trigger, a summary of the investigation process, and the definition of a validated trigger. Similar summary tables can be developed for timelines, notifications, and checklists. The case study in the Appendix includes examples of some of these summary tables.

Once this system-wide analysis is complete, the component-level standard operating procedures should be revised to improve consistency and integration of the system components. These component-level standard operating procedures can then be compiled into an integrated operational strategy, which should include the following:

- Description of the objectives and use of the integrated operational strategy
- Description of the general operational strategy for the contamination warning system
- Comprehensive listing of users and their roles and responsibilities in operation of the contamination warning system

- Summary of the trigger investigation process, and associated timelines, across all components
- Revised, component-level standard operating procedures
- User-specific checklists

After the contamination warning system has been installed and is considered operational, system deployment should enter the baseline and preliminary testing phase. At this point, the operational strategy is revised to guide operation of the system "as-built." The objective during the baseline and preliminary testing phase of deployment is to characterize the system and ensure that procedures, equipment, software, and other components function adequately. During this period, it may be necessary to deviate from the operational strategy that would be implemented in a fully tested, functional system. For example, more time may be spent investigating the cause of triggers in order to understand the source of false alarms. The knowledge and experience gained during the baseline and preliminary testing phase should be used to refine system operations and update the operational strategy in preparation for full deployment.

REMINDER

A primary goal of the operational strategy is to integrate monitoring and surveillance for potential contamination with day-to-day activities to promote sustainability and identify dual-use applications.

During the full deployment phase, the operational strategy should be applied in a manner aligned with the overarching objective stated above: to guide day-to-day operations of the contamination warning system in a manner that can quickly detect and validate triggers indicative of possible contamination. At this phase of deployment, it is critical to integrate the operational strategy into routine operations at the utility and local partner organizations. Otherwise, the system may be difficult, if not impossible, to sustain. Additional guidance on implementation and maintenance of the operational strategy is included in Section 4.

Section 3.0: Standard Operating Procedures

This section describes the recommended content and general structure of standard operating procedures for monitoring and surveillance components of a contamination warning system. The purpose of the standard operating procedures is to describe routine operation of each monitoring and surveillance component and a step-by-step process for the initial investigation and validation of triggers. A standard operating procedure for each of the five monitoring and surveillance components should include the following elements:

- **Component Description**. A summary-level description of the monitoring and surveillance component, initially as conceptualized, but ultimately as-built.
- **Roles and Responsibilities**. A summary listing of all users that have a role in operation of the component along with a description of their responsibilities in operation of the contamination warning system.
- **Process Flow**. A flow diagram illustrating the process for routine operation and investigation of triggers from the component.
- **User-specific Checklists**. Simple forms intended to guide specific users during the initial investigation of a contamination warning system trigger in a manner consistent with the process flows in the standard operating procedures.

The remainder of this section provides additional detail regarding each element of a recommended standard operating procedure. An example operational strategy, including standard operating procedures for each monitoring and surveillance component, is presented as a case study of the Cincinnati pilot in the Appendix.

3.1 Component Description

A standard operating procedure should generally begin with a summary description of the component at its current state of development. The component description is not intended to present detailed design information, rather it is a high-level description to provide the user with the necessary context to understand the remaining elements of the standard operating procedure.

The component description may include the following information:

- The general functionality or objective of the component within the context of the contamination warning system
- A description of major pieces of equipment, such as water quality monitoring stations or security monitoring systems
- A description of the major information systems or software applications supporting the component, such as a Supervisory Control and Data Acquisition (SCADA) system, Geographical Information System (GIS) system, or public health surveillance platform
- A listing of methods that support the component, such as laboratory methods used in baseline sampling and analysis
- The locations of spatially distributed systems, such as enhanced security or water quality monitoring sites

The example component descriptions included in the Appendix (Case Study) are loosely based on the Cincinnati pilot and are intended to illustrate the level of detail that may be useful for this section of the operational strategy.

3.2 Roles and Responsibilities

Many users with different job functions are involved in some aspect of contamination warning system operations. The roles and responsibilities section of the standard operating procedures should provide a comprehensive listing of all users involved in routine operation of the component. **Figure 3-1** illustrates a generic utility organizational hierarchy and indicates which levels of the organization are anticipated to be involved in routine operations of the contamination warning system. While Figure 3-1 focuses on the utility structure, the standard operating procedures should also include representatives from organizations beyond the utility with a role in contamination warning system operations, such as public health, Hazmat, and law enforcement.

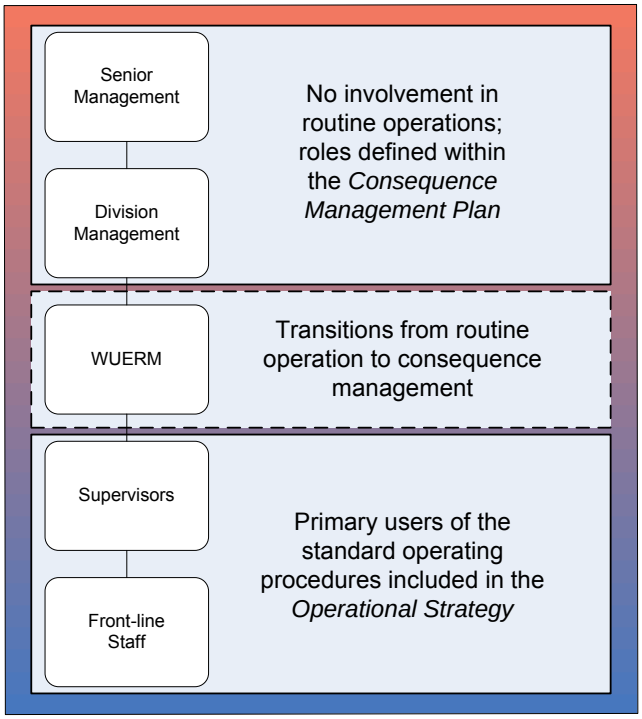

Figure 3-1. Roles within a Generic Utility Organizational Hierarchy

Once users are identified, their specific roles in contamination warning system operations should be defined. As shown, in Figure 3-1, the front-line staff who are responsible for day-to-day monitoring of each component and their supervisors are the primary users of the standard operating procedures. Therefore, it is critical that their responsibilities are detailed therein. Further, it is important to designate one or more individuals with specific, overarching responsibilities for coordinating certain aspects of contamination warning system operation, and in this document these responsibilities are fulfilled by the Water Utility Emergency Response Manager. A utility may refer to this position as something different, but regardless of the title, this role should generally be filled by a mid-level manager who can integrate information from multiple monitoring and surveillance components, assess the threat of contamination, communicate possible contamination events to division and senior management, and initiate the consequence management plan.

HELPFUL HINT

The project management team, as defined in *Planning for Contamination Warning System Deployment*, should be actively involved in the development of the component-level standard operating procedures!

Figure 3-1 depicts the critical role of the Water Utility Emergency Response Manager in guiding the transition from routine operations to consequence management. It is important to note that the responsibilities of the Water Utility Emergency Response Manager may evolve during investigation of a suspected contamination incident; this manager may initially serve as the Incident Commander and later serve in a supportive role as the investigation progresses. A more detailed description of this transitional role is provided in the document *Interim Guidance on Developing a Consequence Management Plan* (USEPA, 2008a).

All roles should detail actions during both routine monitoring and surveillance and trigger investigation and, to the extent possible, be aligned with typical job functions. In some cases, gaps may be identified that can only be filled by assigning new responsibilities to certain users. Assignment of user responsibilities during off-hours, weekends, and holidays should also be considered, as the majority of contamination warning system functions should be covered 24/7/365. Other alternatives include assignment of some users to be on call or providing key users with remote access to various information and notification systems. Regardless, efforts to align the standard operating procedures with existing responsibilities will greatly facilitate integration of the contamination warning system into the utility or partner organizations.

3.3 Process Flow

The process flow should be the central element of a standard operating procedure. It describes how routine monitoring and surveillance, event detection, and trigger validation lead to a determination of possible contamination. Because each component uses different data sources and generates different triggers, the detailed process flow for each component is unique. However, all component process flows should include a common set of process elements:

- **Routine Monitoring**. Typically the process flow will begin with routine monitoring of the component.
- **Initial Trigger**. The process flow should illustrate the manner in which triggers are recognized. Triggers may take the form of an alarm, an alert, an external notification, or an excursion above an established threshold.
- **Notifications**. Throughout the process flow, all necessary notifications should be shown at the point in the process where they would occur. Following initial recognition of the trigger, notifications are typically made to those individuals who would support the investigation of a trigger.
- **Trigger Investigation**. The steps detailing trigger investigation represent a systematic process for ruling out possible benign causes of the trigger. Typically, these steps will comprise the majority of the component process flow, and include information collection and analysis that can be completed in less than two hours.
- **Determination Regarding Possible Contamination**. Process flows should generally conclude with a determination regarding whether or not contamination is possible. If contamination is possible, the Water Utility Emergency Response Manager is notified and the process flow illustrates a transition to credibility determination and consequence management. If not, the process returns to routine operation and documentation of the alarm.

Figure 3-2 illustrates a generic process flow showing the basic steps from routine monitoring and surveillance to event detection and possible determination.

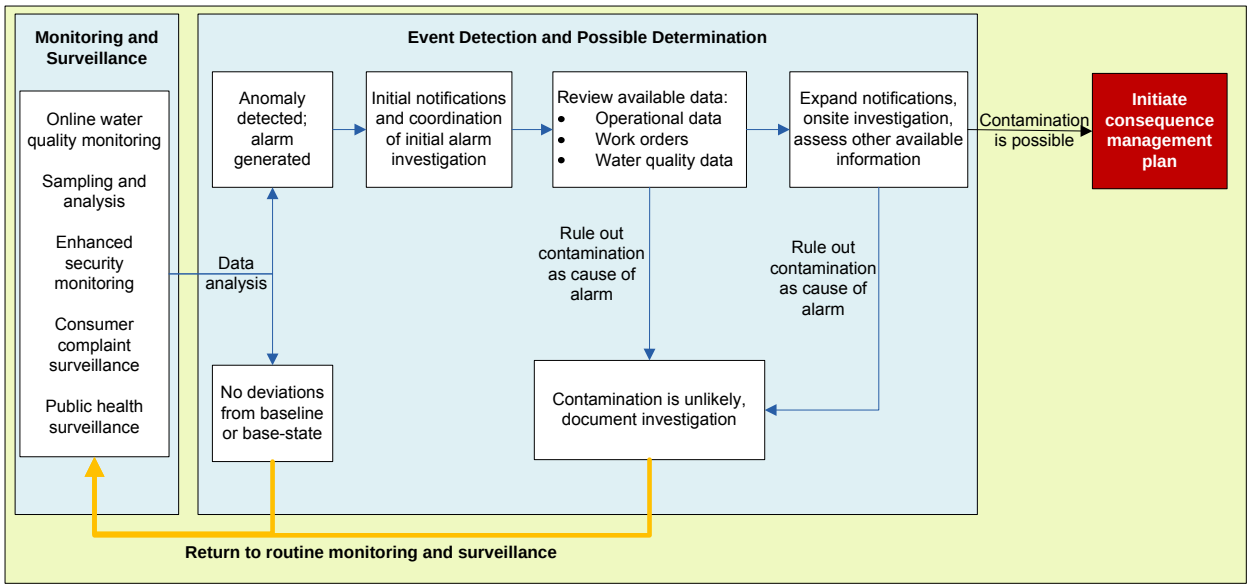

Figure 3-2. Generic Process Flow and Initial Trigger Validation Process

Specific process flows should be developed for each of the monitoring and surveillance components. Process flows will typically include a flow diagram illustrating the process, along with text describing each step of the process. Example process flows for each of the monitoring and surveillance components can be found in the case study discussed in the Appendix. These examples may serve as a starting point for development of process flows to support operation of a specific contamination warning system component, but would be modified and probably expanded to reflect the component as-built and operated in the specific system.

During the development of a process flow it is also useful to estimate the time necessary to investigate and validate a trigger. Time estimates can be used for planning response actions associated with consequence management. For example, a different set of response actions might be considered in the case of a 30 minute validation time compared to those available in the case of a four hour validation time. The case study in the Appendix includes example timeline estimates for each of the components. The time, both average and a range, are estimated for each significant step of the process flow, with consideration given to methods for streamlining the overall timeline. For example, some activities may take place concurrently, while the time required to perform some aspects of the investigation may be reduced through improvements to information systems. The timeline developed for a preliminary operational strategy will likely be based on estimates and should be viewed as goals for system performance that may influence the design of the system. During the baseline and preliminary testing phase, drills and exercise may yield more accurate estimates of the time required to complete the trigger investigation process. Finally, during full deployment, the timeline should be optimized to the extent possible.

3.4 User-specific Checklists

Checklists can complement the standard operating procedures and serve as an aid to specific users during investigation of a contamination warning system trigger. These checklists should be derived from the process flow and serve to prompt the user to check resources, evaluate information, and perform actions as described in the operational strategy. Unlike process flows that are generally component-centric, the checklists are user-centric and organized by job function. Furthermore, a well designed standard operating procedure will generally yield checklists that guide users through a similar set of investigative activities regardless of the source of the trigger. This integration of checklists is achieved through Step 3 of the operational strategy development process – system-wide integration – as discussed in Section 2.3.

Section 4.0: Implementation and Maintenance

This section describes recommended activities associated with implementation and maintenance of the operational strategy throughout the phases of contamination warning system deployment (USEPA, 2007). After the contamination warning system has been designed and implemented, the operational strategy should be revised to incorporate any changes based on the "as-built" system. The contamination warning system should then enter a period of baseline and preliminary testing, which provide users with an opportunity to learn the system and make modifications to optimize performance. After the system has been optimized, operations should enter the full deployment phase during which the system is actively monitored for the purpose of contaminant detection. Over the long-term, the system may undergo periodic cycles of evaluation and refinement. The following subsections discuss the role of the operational strategy in these phases of system deployment: 1) baseline and preliminary testing; 2) full deployment; and 3) evaluation and refinement.

4.1 Baseline and Preliminary Testing

Baseline and preliminary testing begins after design and implementation activities are complete. The objective of this phase of deployment is to operate the contamination warning system for the purpose of collecting data necessary to understand and optimize system performance. It should be noted that the timeline for baseline and preliminary testing phase may vary by component based on the complexity of component operations and the amount of data generated. It may be necessary to conduct drills and exercises in order to generate sufficient data for analysis of system performance during this phase of deployment.

As the system will not be fully operational at this time, it may be desirable to make some adjustments to the operational strategy. For example, while alarms and triggers generated through baseline and preliminary testing may be investigated and documented for the purposes of assessment and optimization of the system, notifications leading to consequence management activities may be limited to drills and exercises. The operational strategy should support baseline and preliminary testing in the following activities: communicating goals and objectives, training, documentation of performance, and refining the operational strategy. Each of these activities is discussed in further detail below.

HELPFUL HINT

Buy-in from all levels, including front-line staff, supervisors, managers, and the project management team prior to initiating baseline and preliminary testing is critical!

Identification of dual-use applications of the contamination warning system components is a powerful way to garner buy-in.

- **Communicating Goals and Objectives.** As discussed, the primary objective of the operational strategy during this phase of deployment is to assess the system and determine whether or not it operates as designed and intended. The operational strategy should guide routine operations and trigger investigations; however, response actions are generally not implemented during this phase. This allows those operating the system on a day-to-day basis to gain a better understanding of the performance, and possible limitations, of the system. These goals and objectives should be clearly communicated to all users involved with system operations.
- **Training.** Training on the operational strategy should occur early in the baseline and preliminary testing phase, once the standard operating procedures have been revised to reflect the "as-built" system. To ensure that training approaches and materials are geared to the appropriate audience, it is recommended that training sessions be divided into training for managers and supervisors and training for front-line staff. Local partners who have a role in operation of the system should also be included in training sessions as appropriate.

- **Manager and Supervisor Training.** The primary objective for this training is to present the integrated operational strategy to managers and supervisors and clearly define the goals and objectives of baseline development. The format for this training may vary, but a classroom setting should be appropriate. It may also be helpful to develop training materials to reference during the training, allowing managers and supervisors to stay engaged in the discussions.
- **Front-Line Staff Training.** The primary objective of this training is to familiarize front-line staff with their role in the operational strategy. Emphasis should be placed on activities that are different from their normal job duties as well as how normal job duties may serve a contamination warning system function. In contrast to the classroom training recommended for managers and supervisors, training for front-line staff should be hands-on and perhaps scenario-based. This will allow front-line staff to focus on the operational activities that are directly applicable to them and begin to assess how to integrate new responsibilities into day-to-day activities.

LESSON LEARNED

Training for front-line staff should be hands-on and focused on how contamination warning system activities fit in with their routine job activities.

- **Documentation of Performance.** As the primary objective of the baseline and preliminary testing phase of deployment is to generate data to characterize system performance, documentation of alarms, triggers, and subsequent actions is critical. Front-line staff should utilize checklists to log and document triggers, the results of investigations, and possible causes of triggers. This information will be analyzed to identify modifications to the operational strategy and/or the contamination warning system to optimize performance prior to full deployment.
- **Optimization of Operational Strategy.** Near the conclusion of the baseline and preliminary testing phase, another system-wide analysis should be conducted by the project management team. The purpose of this analysis is to assess documentation and data generated during the baseline and preliminary testing phase. Based on this analysis, and on lessons learned through baseline and preliminary testing of the system, the operational strategy should be revised to optimize performance. Modifications and enhancements to the contamination warning system components may also be necessary to support system optimization.

4.2 Full Deployment

During the full deployment phase, EPA considers the contamination warning system to be "operational" with active monitoring and surveillance for indications of drinking water contamination. The operational strategy, revised to reflect system optimization and to reflect lessons learned from the baseline and preliminary testing phase, should be distributed to staff with an active role in system operation, including local partners. It may be helpful to include a summary of what has changed from the previous version of the operational strategy. In addition, establishing a "go-live" date for when the system will be fully operational may help to ensure that everyone clearly understands the change in system operation. From the go-live date forward, alarms and triggers should be investigated in accordance with the operational strategy, and the consequence management plan should be enacted when appropriate (e.g., when a trigger is validated and contamination is considered possible). Thus, it is also important to notify local partners who may have a role in response and consequence management of the go-live date.

HELPFUL HINT

Establishing a "go-live" date – the point from which alarms and triggers will be investigated in accordance with the operational strategy – should help to ensure everyone is ready to begin full deployment and routine operation of the system!

Training on the operational strategy will be critical to the success of the system as it enters full deployment. During the transition to full deployment, all users should be trained on the operational

strategy that was revised following baseline and preliminary testing. Furthermore, a maintenance training program should be established to provide refresher training to current staff on a periodic basis and comprehensive training for new staff. Furthermore, drills and exercises can be a highly effective method of training as well as a method for evaluating current procedures as discussed in the next section.

4.3 Evaluation and Refinement

As the contamination warning system is periodically evaluated and refined, it may be appropriate to update the operational strategy to reflect modifications to the system. An annual system-wide review of the operational strategy and system performance is recommended. A process for conducting this review should be established concurrent with full deployment of the system. Factors that may influence revisions to the operational strategy include evaluation of system performance, enhancements or modifications to the system, identification of dual-use applications, or other factors external to the system.

In the absence of actual contamination incidents, drills and exercises provide a means for assessing system performance. In addition, drills and exercises should be considered a part of maintenance training as discussed in the previous section. To address both objectives of drills and exercises, various approaches may be employed. Tabletop exercises or focused drills may be conducted for specific components at greater frequency than drills and exercises designed to assess performance of the entire integrated system. At a minimum, these drills and exercises should be conducted annually to coincide with the system-wide review of the operational strategy. Greater frequency may be desired and important to ensure that functionality of the system is maintained. These activities should also engage local partners involved in operation as appropriate. It may also be advantageous to integrate operational drills and exercises with those planned for consequence management. However, objectives should be clearly defined and agreed to by all participants to minimize confusion and help ensure success of the drill or exercise. Lessons learned through drills and exercises as well as routine operation of the system should be documented and reviewed as part of the annual system-wide analysis.

REMINDER

Throughout the life-cycle of the contamination warning system, remember to …

Conduct periodic system-wide analyses and evaluations to optimize operation and performance of the system:

- Conduct routine drills and exercises and integrate operations with response actions in the consequence management plan
- Document trigger investigations
- Identify dual-use applications and other benefits derived from operation of the system

While drills and exercises are useful for evaluating the system, they are not the only tools available. Routine water quality, operational, or public health excursions can provide a valuable opportunity for system evaluation and training. During full deployment, it is expected that at least a few triggers for each component could result in a conclusion that contamination is possible. The subsequent investigation and implementation of response actions may involve implementation of not only the operational strategy but also the consequence management plan. Post-incident review and documentation could potentially provide some of the most useful information for evaluation, refinement, and identification of dual-use application.

Over time, additional monitoring and surveillance tools may be available or there may be a desire to upgrade or modify certain systems or processes within the utility. It is important to evaluate how these changes may impact or enhance the contamination warning system prior to moving forward with implementation. Some may involve substantial revisions to the operational strategy whereas others might involve a preliminary testing phase to assess the performance of the new tool prior to continuing without modifications to the operational strategy. These instances may be identified in preparation for the annual system-wide review, or pending the timeframe, may result in an ad hoc system-wide review of the operational strategy.

Other factors external to the contamination warning system that may influence revisions to operational strategy include changing priorities within the utility; dual-use applications of tools, technology, or information; and/or organizational and management changes. By conducting an annual system-wide review of the operational strategy, these factors can be identified and addressed while maintaining the functionality and sustainability of the contamination warning system.

Section 5.0: References

U.S. Environmental Protection Agency. 2003. *Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents*. Interim Final.

U.S. Environmental Protection Agency. 2005. *WaterSentinel System Architecture, Draft for Science Advisory Board Review*. EPA 817-D-05-003.

U.S. Environmental Protection Agency. 2007. *Water Security Initiative: Interim Guidance on Planning for Contamination Warning System Deployment*. EPA-817-R-07-002.

U.S. Environmental Protection Agency. 2008a. *Water Security Initiative: Interim Guidance on Developing a Consequence Management Plan*. EPA-817-R-08-001.

U.S. Environmental Protection Agency. 2008b. *Water Security Initiative: Cincinnati Pilot Post-Implementation System Status.* EPA-817-R-08-004.

APPENDIX
Case Study: Operational Strategy for the Cincinnati Contamination Warning System

This appendix presents a case study of the operational strategy developed for the Cincinnati contamination warning system pilot. A detailed description of the post-implementation status of each component of the Cincinnati contamination warning system is provided in the document, *Cincinnati Pilot Post-Implementation System Status* (USEPA, 2008b). In this case study, the operational strategy has been generalized by simplifying process flows and utilizing nonspecific roles and job functions in an attempt to make the example more universal. The intent of the case study is to illustrate the application of the recommendations in this guidance document through presentation of a real-world example, specifically, the experience gained during the initial Water Security initiative pilot in Cincinnati. The *Operational Strategy for the Cincinnati Contamination Warning System* is built around a series of standard operating procedures and supporting checklists that guide the investigation of triggers from each component of the contamination warning system.

This case study may provide a useful reference for the development of an operational strategy customized to a specific locality's contamination warning system. For example, the checklists and process flows provided in this appendix could be tailored to the specific objectives and organizational structure of a utility developing its own contamination warning system. However, it is important to recognize that while the case study has been generalized from the *Operational Strategy for the Cincinnati Contamination Warning System*, many artifacts specific to Cincinnati's contamination warning system remain. Thus, the example should be viewed as illustrative of the concept and not as guidance or recommendations on the detailed content of a specific operational strategy.

A.1 Overview and Objectives

EPA's Water Security initiative contamination warning system model can be used to monitor and integrate a variety of information sources in order to detect conditions that might indicate a contamination incident. The Cincinnati contamination warning system includes five components, each of which monitors a different set of information sources:

- Online Water Quality Monitoring (WQM)
- Sampling and Analysis (S&A)
- Enhanced Security Monitoring (ESM)
- Consumer Complaint Surveillance (CCS)
- Public Health Surveillance (PHS)

The operational strategy for this system describes how the five components are operated in a complementary manner to function as an integrated contamination warning system.

Overview

The *Operational Strategy for the Cincinnati Contamination Warning System* is organized into seven sections. This section, **A.1**, provides an overview of the document and states the objectives of the operational strategy. It also provides an overarching summary of the roles and responsibilities of the various users (identified by "job function") in system operations, indicating each component for which a specific job function has a responsibility in routine operations.

Sections A.2 though **A.6** include standard operating procedures for each of the five monitoring and surveillance components. Each standard operating procedure describes the process for identification and investigation of triggers, and is organized as follows:

- Component Description: provides a high-level summary of the as-built component, with sufficient detail to provide the necessary context to understand the procedures that follow.
- Roles and Responsibilities: identifies each job function with a role in routine operation of the component, and provides a description of their responsibilities.
- Process Flow: presents a step-by-step process for systematically investigating a trigger. The process flow is presented as a flow diagram with supporting text and a tabular summary of time estimates to complete each step.
- Checklists: provides a listing of the checklists that support implementation of the standard operating procedure for the specific component.

Finally, **Section A.7** includes the checklists referenced throughout Sections A.2 through A.6. These checklists are generally developed to support specific job functions across all components in which that job function has a role. Thus, while the standard operating procedures are developed around each component of the system, the checklists are developed around the user.

The scope of the standard operating procedures that comprise the operational strategy are limited to the identification and initial investigation of triggers. Generally, the investigation ends with the conclusion that either the trigger was a false alarm or indicative of a possible contamination incident. If the latter, operations shift from routine operations to consequence management as described in the *Consequence Management Plan for the Cincinnati Contamination Warning System Pilot*. The first major activity under the consequence management paradigm is an investigation into the credibility of the possible contamination incident. This investigation relies upon information obtained from each of the monitoring and surveillance components, and thus there is an important linkage between the standard operating procedures that guide routine activities and the consequence management plan that guides the credibility determination process. For the Cincinnati pilot, these two documents (the *Operational Strategy* and the

Consequence Management Plan) have been thoroughly reviewed and integrated to facilitate a smooth transition from routine operations to consequence management in the event of a possible contamination incident.

Objectives

The Cincinnati contamination warning system was designed to integrate with existing systems and procedures such that system operations can be performed by existing staff and front-line supervisors. Contamination warning system monitoring and surveillance operations will provide benefits beyond contamination warning, by enabling the utility to rapidly detect and respond to routine water quality problems.

The objectives of this operational strategy are to document the users, roles and responsibilities, and procedures used in routine operation of the Cincinnati contamination warning system. The intended audience for the operational strategy includes the staff and supervisors from the utility and local partner organizations with responsibility for routine operation of the system. Additionally, upper-management from participating organizations can use this document to plan for integration of contamination warning system operations into normal activities, and explore opportunities for dual-use application of the system.

Overview of Roles and Responsibilities

Effective operation of the Cincinnati contamination warning system involves a variety of personnel from the utility and local partner organizations, each having well-defined responsibilities. Each of the standard operating procedures presented in this document lists the personnel (identified by job function) that have roles and responsibilities with respect to routine operation of that component. **Table A-1** is a comprehensive listing of job functions and shows that many have roles in multiple monitoring and surveillance components. The table describes the general role of each job function in contamination warning system operations and identifies each component in which that job function has a role.

Table A-1 was derived from a system-level analysis of the standard operating procedures for all components and was used to ensure that responsibilities were defined consistently across components. It is important to note that the roles described in this table will likely evolve as a suspected contamination event transitions from routine operation to consequence management. A more detailed description of the responsibilities of each of these roles in the credibility determination process of consequence management is provided in the document *Interim Guidance on Developing a Consequence Management Plan* (USEPA, 2008a).

Table A-1. Summary of Primary Roles in Routine Contamination Warning System Operations

Job Function	General Role in CWS Operations	WQM*	S&A	ESM	CCS	PHS
Water Utility Emergency Response Manager	Receive notification of possible contamination incidents and transition to consequence management	✓	✓	✓	✓	✓
Water Quality Supervisor	Supervise the water quality component of any trigger investigation and coordinate synthesis of information from other utility personnel	✓	✓		✓	✓
Water Quality Technician	Investigate the site of WQM or CCS triggers; inspect WQ monitor stations; collect samples; and perform field tests	✓	✓		✓	
Water Quality Customer Service Representative	Monitor for CCS triggers and serve as subject matter expert during investigation of a water quality complaint				✓	
Customer Service Representative	Respond to customer calls and identify those with unique water quality concerns				✓	
Laboratory Supervisor	Manage laboratory sampling & analysis activities at the utility and coordinate use of laboratory results during a trigger investigation		✓			✓
Laboratory Chemist	Perform analysis and QC review of results from chemical analyses		✓			
Laboratory Microbiologist	Perform analysis and QC review of results from biological analyses		✓			
SCADA Operator	Monitor for WQM and ESM triggers; and review distribution system operations to support the investigation of triggers	✓	✓	✓	✓	✓
Distribution Work Supervisor	Monitor for CCS triggers during non-business hours, and review ongoing and recent distribution system work to support the investigation of triggers	✓	✓	✓	✓	✓
Distribution Field Crews	Perform field investigations in response to CCS and ESM triggers			✓	✓	
Utility Security Personnel	Lead the investigation of all ESM triggers			✓		
Local Law Enforcement	Lead the criminal aspect of the investigation of security breach			✓		
Local Public Health Agencies	Provide local public health data; epidemiologists and disease investigators					✓
Poison Control Center	Monitor for and investigate PHS triggers resulting from calls to the center					✓
Fire Department	Manage the IT system that provides 911 and EMS data					✓
State Health Department	Analyze samples for select biological agents and radiochemicals		✓			
Contract Laboratory	Analyze samples for designated chemical analytes		✓			

*System names: Water Quality Monitoring (WQM), Sampling and Analysis (S&A), Enhanced Security Monitoring (ESM), Consumer Complaint Surveillance (CCS), and Public Health Surveillance (PHS)

Overview of Trigger Investigation Process Flows

A similar system-level analysis was conducted for the process flows to ensure that the decision points, notifications, and end points are consistently defined across components. **Table A-2** provides a summary across all components that includes: the data source, event detection, trigger, investigation, and trigger validation for each component.

Table A-2. Summary of Process Flows and Trigger Validation Process for Contamination Warning System Components

CWS Component	Event Detection	Trigger	Investigation	Validated Trigger
Online Water Quality Monitoring	Event detection system determines if an anomaly is present in the water quality data	Water quality alarm is displayed on a graphical user interface to the SCADA system located in a control room staffed 24/7	● Analyze monitoring station status ● Review operational data and ongoing work in the distribution system ● Review water quality data from spatially related locations ● Investigate monitoring station that witnessed the anomaly	Trigger is validated if alarm is not explained by a monitoring equipment problem, operational changes, distribution system work, or water quality data review
Sampling and Analysis	Sample analysis results exceed control levels or contain non-target analytes	Internal or external analytical laboratory contacts the designated water quality point of contact at the utility	● Review data to determine if results exceed baseline control values ● Review operational data, ongoing work in the distribution system, and other water quality data ● Perform confirmatory analysis (if appropriate)	Trigger is validated if baseline exceedence cannot be explained by benign causes
Enhanced Security Monitoring	Security monitoring systems detect intrusion at a utility facility	Intrusion alarm is displayed on a graphical user interface to the SCADA system located in a control room staffed 24/7	● Review video feed (if available) ● Conduct field investigation ● Assess witness legitimacy (if trigger is from witness account)	Trigger is validated if field investigation indicates that an intrusion occurred that provided access to the water supply, or reveals that hazardous conditions exist or are suspected
Consumer Complaint Surveillance	Event detection system determines if an anomaly exists in the number and location of consumer complaint calls	Consumer complaint alarm text message sent to designated water quality point of contact at the utility	● Review water quality data ● Review operational data and ongoing work in the distribution system ● Spatially analyze consumer complaint data to identify clustering	Trigger is validated if the consumer complaint alarm is not explained by review of water quality data, operational changes, or distribution system work
Public Health Surveillance	Public health agency detects an anomaly in EMS/911 data, emergency room chief complaints, poison control center cases, or analysis of infectious disease cases	Public health alert is sent to designated water quality point of contact at the utility via email or a phone call	● Review data from other monitoring and surveillance components ● Review operational data and ongoing work in the distribution system ● Review of other pertinent test results, e.g., coliform	Trigger is validated if the public health agency determines the trigger could be related to drinking water, and the utility determines contamination is possible, based on results of investigation

A.2: Online Water Quality Monitoring Standard Operating Procedures

Component Description

As a component of EPA's contamination warning system model, online water quality monitoring may provide an indication of contamination through detection of a water quality anomaly as indicated by deviations from an established water quality base-state. The online water quality monitoring network deployed in this contamination warning system is comprised of the monitoring stations deployed at specific locations throughout the drinking water distribution system, a supervisory control and data acquisition (SCADA) system to transmit and manage data in a centralized location, and an event detection system to analyze data for anomalies and possible contamination incidents. The following is a brief description of the water quality monitoring component.

Twelve water quality monitoring stations were installed throughout the distribution system as shown in **Table A-3**. A tiered sensor network design was used, employing two types of monitoring stations. The Type A water quality monitoring stations monitor for: total organic carbon (TOC), chlorine residual, oxidation-reduction potential (ORP), conductivity, pH, turbidity, and temperature. The Type B water quality monitoring stations are similar to the Type A stations, but have a UVA spectrophotometer instead of a TOC analyzer.

Table A-3. Summary of the Example Online Water Quality Monitoring Network

Location	Monitoring Station Type
Fairview Pump Station	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Greenville Fire Dept.	Type B (UVA, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Glenn Township Police Dept.	Type B (UVA, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Plum Street Pump Station	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Madison Reservoir	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)
City University, North Campus	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Hillcrest Reservoir	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Main Street US Post Office	Type B (UVA, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Conner Pump Station	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Northbrook Fire Dept.	Type B (UVA, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Highland Street Police Dept.	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)
Golf Drive Storage Tank	Type A (TOC, Chlorine, ORP, conductivity, pH, turbidity, temperature)

Data from the water quality monitoring stations are transferred to the SCADA system at the utility control center via a digital cellular network. A graphical user interface (GUI) provides real-time data from the entire water quality monitoring network as well as alarms, operational data, and information from the event detection system described below. In addition to the primary SCADA workstation installed in the control center, several remote workstations were installed throughout the utility to provide key personnel with direct access to data from the water quality monitoring network.

Once the data from the water quality monitoring stations are collected within the SCADA system, it is analyzed for anomalies that could be indicative of contamination by an event detection system. The event detection system is installed on a high-performance workstation in a dedicated protected zone that is connected to the SCADA system through a firewall.

Roles and Responsibilities

Table A-4 shows the roles that utility personnel and managers have in water quality monitoring. For the Cincinnati pilot, the Water Quality Supervisor has the lead role in the investigation of water quality alarms while the SCADA Operator has primary responsibility for routine monitoring for triggers.

Table A-4. Roles and Responsibilities for Routine Operation of Online Water Quality Monitoring

Job Function	Role in Online Water Quality Monitoring Component Operations
Water Quality Supervisor	• Assume the lead in the investigation of a water quality trigger. • Coordinate support from appropriate utility personnel during investigation of a water quality trigger. • Review water quality data and related information during the investigation of a water quality trigger. • Make the determination regarding whether or not the water quality trigger is a "possible" contamination threat. • Decide whether to initiate remote sample collection at the site of the water quality monitoring station that detected the anomaly. • Decide whether or not to send field technicians to the field to inspect the water quality monitoring station. • Notify the Water Utility Emergency Response Manager if the determination is made that the contamination threat is "possible."
SCADA Operator	• Monitor all SCADA alarms 24/7/365, including water quality triggers. • Notify Water Quality Supervisor in the event of a water quality trigger. • Review distribution system operations to support the investigation of a water quality trigger.
Distribution Work Supervisor	• Review distribution system work orders to support the investigation of a water quality trigger. • Lead the investigation of a water quality trigger if the Water Quality Supervisor (or alternate) is unavailable. • Notify the Water Utility Emergency Response Manager if the abbreviated investigation cannot rule-out contamination.
Water Quality Field Technician	• Inspect online water quality monitoring stations. • Perform field verification of online water quality sensor readings. • Collect samples from the distribution system in support of a water quality trigger investigation.
Water Utility Emergency Response Manager (WUERM)	• Review water quality data and related information during the investigation of a water quality trigger when the Water Quality Supervisor (or alternate) is unavailable. • Implement the consequence management plan as necessary.

Process Flow

The process flow in **Figure A-1** illustrates the steps taken during the investigation of an online water quality monitoring trigger. The process begins with recognition of a water quality alarm as displayed on the SCADA GUI and ends with notification of the Water Utility Emergency Response Manager (if contamination is deemed "possible"), or with logging the incident (if contamination is deemed "not possible"). The anticipated timeline for validation of a trigger from water quality monitoring is presented in **Table A-5**.

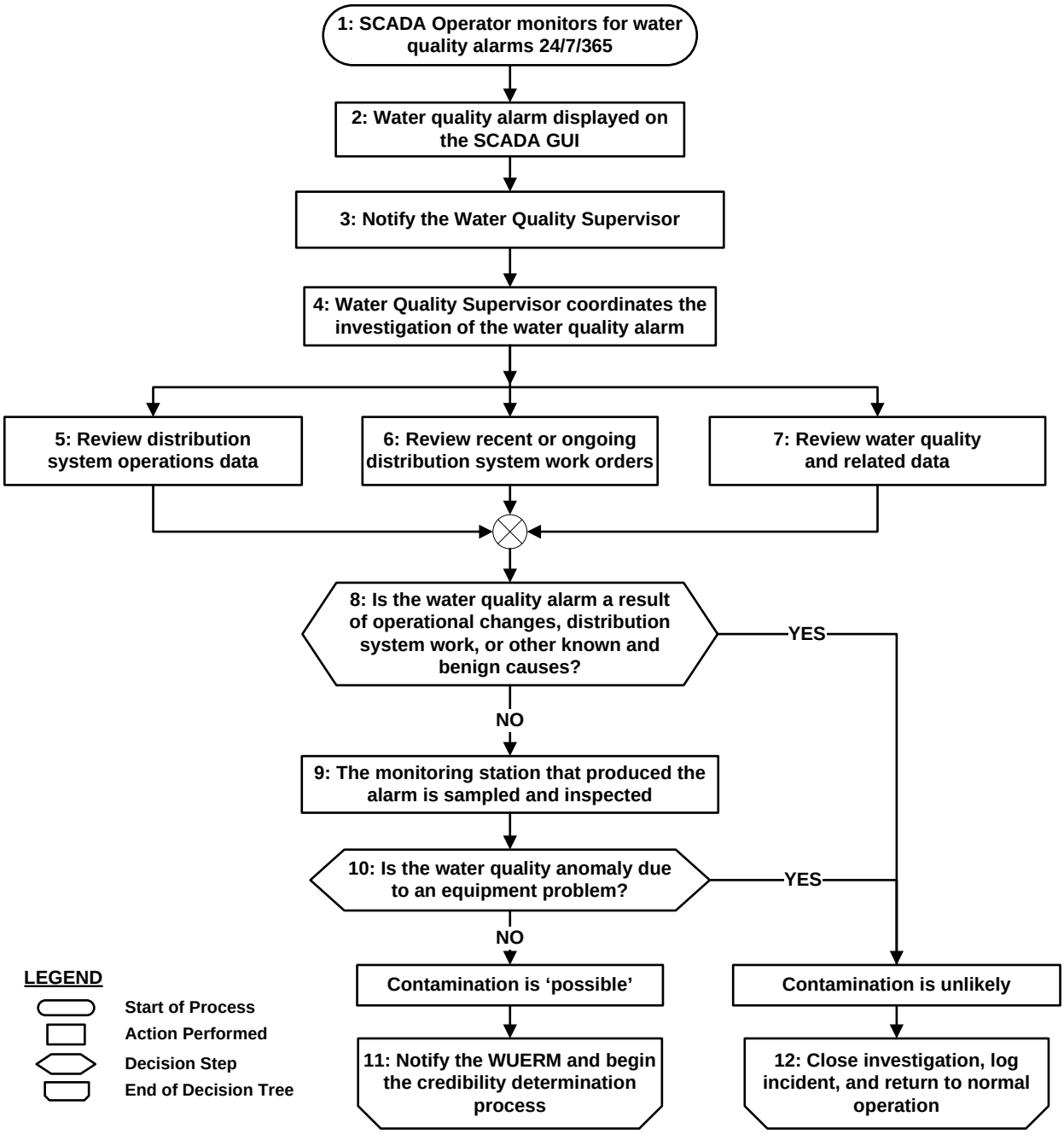

Figure A-1. Process Flow for Online Water Quality Monitoring: Routine Monitoring and Initial Trigger Validation

1. SCADA Operator monitors for water quality alarms 24/7/365.

- The event detection system operates in real-time, continuously updating the alarm status shown on the SCADA GUI for each water quality monitoring location.
- Routine monitoring for water quality alarms is integrated into the procedures typically used for monitoring of other high priority SCADA alarms.

2. Water quality alarm displayed on the SCADA GUI.

- When a water quality anomaly is detected by the event detection system, the SCADA GUI displays alarm status, date/time, location, and the parameters suspected of triggering the alarm.

- The alarm is acknowledged to turn off the audible alert.

3. Notify the Water Quality Supervisor of the water quality alarm.

- If the water quality alarm occurs during non-business hours, a pre-assigned alternate is notified.

4. The Water Quality Supervisor coordinates the investigation of the water quality alarm.

- Request the assistance of the appropriate utility personnel (i.e., SCADA Operator, Distribution Work Supervisor, etc.) in the investigation of a water quality alarm.
- Review distribution system operations data, as described under Step 5.
- Review recent and ongoing distribution system work, as described under Step 6.
- Review water quality data and related information, as described under Step 7.

5. Use *Checklist A-3: Distribution System Operations Review* to check for distribution system operating conditions that could have influenced water quality at the monitoring location, including the following:

- Pump operation.
- Tank levels and fill/drain status.
- Valve open/close status.
- Relevant system alarms (e.g., control limit, loss of power, loss of communications, intrusion, etc.)
- Unusual demands (e.g., due to fire flow).
- Pressure anomalies in the vicinity of the monitoring station that detected the water quality anomaly.
- Additional flow and pressure data in the vicinity of the monitoring station that detected the water quality anomaly, if available.

6. Use *Checklist A-4: Distribution System Work Order Review* to check ongoing or recent distribution system work that could have influenced water quality at the monitoring location, including the following:

- Main breaks, repairs, and replacement.
- Flushing operations.
- Water outages.
- Power outages.
- Work that may have interfered with proper operation of the online monitoring instrumentation.
- Other distribution system work that could have impacted water quality in the vicinity of the monitoring station(s).

7. Use *Checklist A-1: Contamination Warning System Trigger Investigation* to check water quality data and other information potentially related to the trigger, including the following:

- Water quality trend lines from the monitoring location(s) that detected the water quality event.
- Water quality trend lines from other water quality monitoring stations in the distribution system. Approximate travel time between monitoring stations should be considered when selecting the time period for display of water quality data from other distribution system monitoring stations.

- Water quality trend lines for the finished water leaving the treatment plant that supplies the region in which the monitoring station is located. Approximate travel time from the plant to the monitoring station that witnessed the water quality anomaly should be considered when selecting the time period for display of data from the treatment plant.
- Recent treatment plant operating conditions, process water quality, or source water quality.
- Change in the source water supplying the monitoring location that witnessed the anomaly.
- Historic water quality trends, such as seasonal patterns, which are not automatically factored into the event detection system configuration.
- A log of previously observed water quality anomalies.
- Maintenance and calibration records for the monitoring station(s) that detected the anomaly.
- Attributes, configuration, and settings of the event detection system.

8. Is the water quality alarm a result of operational changes, distribution system work, or other known and benign causes?

- If "YES," contamination is considered unlikely, the investigation is closed and the trigger is logged. Go to Step 12.
- If "NO," the water quality EDS alarm is considered valid. Go to Step 9.

9. The water quality monitoring station that produced the alarm is inspected.

- Initiate remote sample collection at the monitoring station that detected the anomaly.
- Based on available information, the appropriate utility supervisor decides whether or not utility personnel can be sent to the site to conduct the investigation. If conditions are considered too hazardous for utility personnel, contamination is deemed "possible." Go to Step 11 and seek additional support (e.g., a Hazmat responder) to investigate the site.
- If no obvious hazards are apparent, water quality field technicians are dispatched to the site to retrieve the sample and investigate the water quality monitoring station. Precautions outlined in a Site Characterization Plan should be followed during the field inspection.
- Record results of the inspection in *Checklist A-2: Distribution System Site Investigation*.
- Report the results of the site investigation to the Water Quality Supervisor from the field as they become available.

10. Is the water quality anomaly due to an equipment problem? Equipment problems may include sensors, communication systems, IT systems, or ancillary components such as plumbing or electric.

- If "YES," contamination is considered unlikely. Go to Step 12.
- If "NO," contamination is considered "possible." Go to Step 11.

11. Notify the Water Utility Emergency Response Manager and initiate the credibility determination process.

- Once all reasonable explanations for the water quality anomaly have been assessed and ruled out, the water quality trigger is considered valid, and contamination is considered "possible."
- The Water Quality Supervisor notifies the Water Utility Emergency Response Manager.
- The Water Utility Emergency Response Manager implements the credibility determination process, thereby transitioning to consequence management activities as described in the

consequence management plan. This includes review of data from other contamination warning system components.

12. Close investigation, log the incident, and return to normal operation.

- At the conclusion of the investigation, if contamination can be ruled out, return to normal operation. However, some level of investigation may continue if the anomaly is indicative of an operational or water quality problem.
- Return to routine monitoring and operating activities.
- The Water Quality Supervisor documents the review and assessment of the water quality trigger by compiling the checklists used in the investigation.

Table A-5. Example Timeline for Validation of a Water Quality Trigger in the Context of an Operational Contamination Warning System

Process Activity ID Number	Process Activity Description	Expected Response Time (minutes)	Range of Response Times (minutes)
2	Water quality alarm displayed on the SCADA GUI	2	1-5
3	Notify the Water Quality Supervisor of the water quality alarm	3	2-10
4	Initiate the water quality trigger investigation and requests support from the appropriate utility personnel	5	2-10
5-7	**5**: Review distribution system operations data **6**: Review recent or ongoing distribution system work **7**: Review water quality and related data	20	10-30
8	Evaluate initial data and determine the validity of the water quality trigger	20	10-30
9-10	Inspect the water quality monitoring station that witnessed the anomaly and determine if the cause was an equipment problem	60	30-120
11	Notify the WUERM and begin the credibility determination process	15	5-20
	TOTAL ELAPSED TIME	**125**	**60-225**

Checklists

Four checklists, described in **Table A-6,** are used in the review of water quality monitoring triggers based on this example. The checklists are included in Section A.7.

Table A-6. Example Checklists Used during Investigation of a Water Quality Monitoring Trigger

Reference	Checklist	User	Description
Checklist A-1	Contamination Warning System Trigger Investigation	Water Quality Supervisor	Checklist involves the review of water quality data, plant operating conditions, event detection system settings, and other information potentially related to the trigger.
Checklist A-2	Distribution System Site Investigation	Water Quality Field Technician	Checklist covers inspection of water quality monitoring stations in support of the investigation of a water quality trigger.
Checklist A-3	Distribution System Operations Review	SCADA Operator	Checklist involves the review of distribution system operations that may have influenced water quality near the location of the trigger.
Checklist A-4	Distribution System Work Order Review	Distribution Work Supervisor	Checklist involves the review of distribution system work orders that may have influenced water quality near the location of the trigger.

A.3: Sampling and Analysis Standard Operating Procedures

Component Description

In EPA's contamination warning system model, routine operation of the sampling and analysis component involves routine monitoring at the treatment plants, distribution system locations where water quality monitoring stations or enhanced security systems are installed, and other strategic distribution system locations. The primary objective of routine monitoring as part of the contamination warning system model is to maintain proficiency in the collection and analysis of samples for analytes that may be of concern during a drinking water contamination incident, and to maintain a database of method performance and contaminant occurrence (contaminants detected, levels detected, and frequency of detection) throughout the distribution system. This phase of operation is called maintenance monitoring. Data generated from baseline monitoring are updated through maintenance monitoring and may be referenced during triggered sampling and analysis for determination of "possible" contamination events.

To facilitate routine monitoring as part of the contamination warning system a network of local laboratories, listed in **Table A-7**, was established. Many of the laboratories may also play a role in consequence management activities, depending on availability and circumstances surrounding the suspected incident.

Table A-7. Local Laboratory Network and Sampling Frequency for Maintenance Monitoring

Laboratory	Analysis	Analytes
Utility	Gas Chromatography / Mass Spectrometry with Purge and Trap Extraction	VOCs
	Gas Chromatography with Mass Spectrometry Detection using liquid-solid extraction (LSE)	SVOCs
	Cyanide – Colorimetric Analysis	Free cyanide
Contract Laboratory	Inductively Coupled Plasma – Mass Spectrometry	Metals
	High Performance Liquid Chromatography with fluorescence determination	Carbamates
State Health Department Laboratory	Real-time PCR and Immunoassay (TRF) platforms	BT Agents
	Alpha Beta Scintillation Scaler or Gas Flow Low-Background Proportional Detector	Radiochemicals
	High Purity Germanium Gamma Spectrometry System	

In addition, the field methods identified in **Table A-8** are also performed as part of routine monitoring on a monthly basis at water quality monitoring stations, priority pump stations, reservoirs, and tanks in the distribution system, with the objective of updating baseline data and maintaining emergency response capabilities.

Table A-8. Field Methods for Safety and Contaminant Screening

Contaminants	Field Test Kit
Free cyanide	Portable Colorimeter
Free chlorine	Portable Colorimeter
pH, conductivity, and ORP	Portable electrochemical detector
Turbidity	Portable Turbidimeter
Chemical Warfare Agents (VX, sarin, etc.)	Test kit
Radioactivity (alpha, beta, gamma)	Hand-held device
VOCs and combustible gases	Hand-held device
Toxicity	Test kit

Roles and Responsibilities

As summarized in **Table A-9**, the sampling and analysis component involves internal and external laboratory personnel, as well as personnel from water quality, distribution, and operations to assist in investigation of triggers caused by analytical results outside of established baselines for routine samples.

Table A-9. Roles and Responsibilities for Routine Operation of Sampling and Analysis

Job Function	Role in Sampling and Analysis Component Operations
Water Quality Supervisor	• Coordinate support from appropriate utility personnel during investigation of the sampling and analysis trigger. • Review water quality data and related information during the investigation of a sampling and analysis trigger. • Decide whether to initiate additional analysis of sample(s). • Make the determination regarding whether or not the sampling and analysis trigger is indicative of possible contamination. • Notify the Water Utility Emergency Response Manager if the determination is made that the sampling and analysis trigger is indicative of possible contamination.
Laboratory Supervisor	• Coordinate sample flow and laboratory analysis of routine samples. • Perform data review and update baseline control charts. • Assist with data interpretation and resolution of Quality Control issues for analytical methods. • Provide technical support regarding sample analysis.
Laboratory Chemist	• Perform routine and confirmatory analyses for chemical contaminants that are analyzed in-house by the utility. • Assist the Laboratory Supervisor with updating the Water Quality Database and control charts. • Provide technical support regarding sample analysis and data interpretation.
Laboratory Microbiologist	• Process samples for microbiological analysis using Laboratory Response Network protocol. • Assist the Laboratory Supervisor with updating the Water Quality Database and control charts. • Provide technical support regarding sample analysis and data interpretation.
Water Quality Field Technician	• Collect samples from routine monitoring locations in the distribution system. • Perform routine field screening.
Distribution Work Supervisor	• Review distribution system work orders to support the investigation of a sampling and analysis trigger.
SCADA Operator	• Review operational data to support the investigation of a sampling and analysis trigger.
Water Utility Emergency Response Manager (WUERM)	• Review analytical and related information during the investigation of a sampling and analysis trigger when the Water Quality Supervisor is unavailable. • Implement the consequence management plan, as necessary.
State Health Department Laboratory	• Perform screening and confirmatory analyses for select pathogens and toxins in routine samples. • Perform screening and confirmatory analyses for radiochemicals.
Contract Laboratory	• Perform screening and confirmatory analyses for target analytes as specified in the contract with the utility.

Process Flow

Samples collected through routine monitoring activities may not be analyzed as soon as they are received by laboratories. However, in the event that a baseline sample exceeds a trigger level, the process flow in **Figure A-2** illustrates the steps that should be taken to investigate the trigger and determine whether or not contamination is possible based on analytical results. The timeline for validation of a trigger from routine sampling and analysis presented in **Table A-10** reflects this potentially lengthy delay in recognition of a trigger from this component.

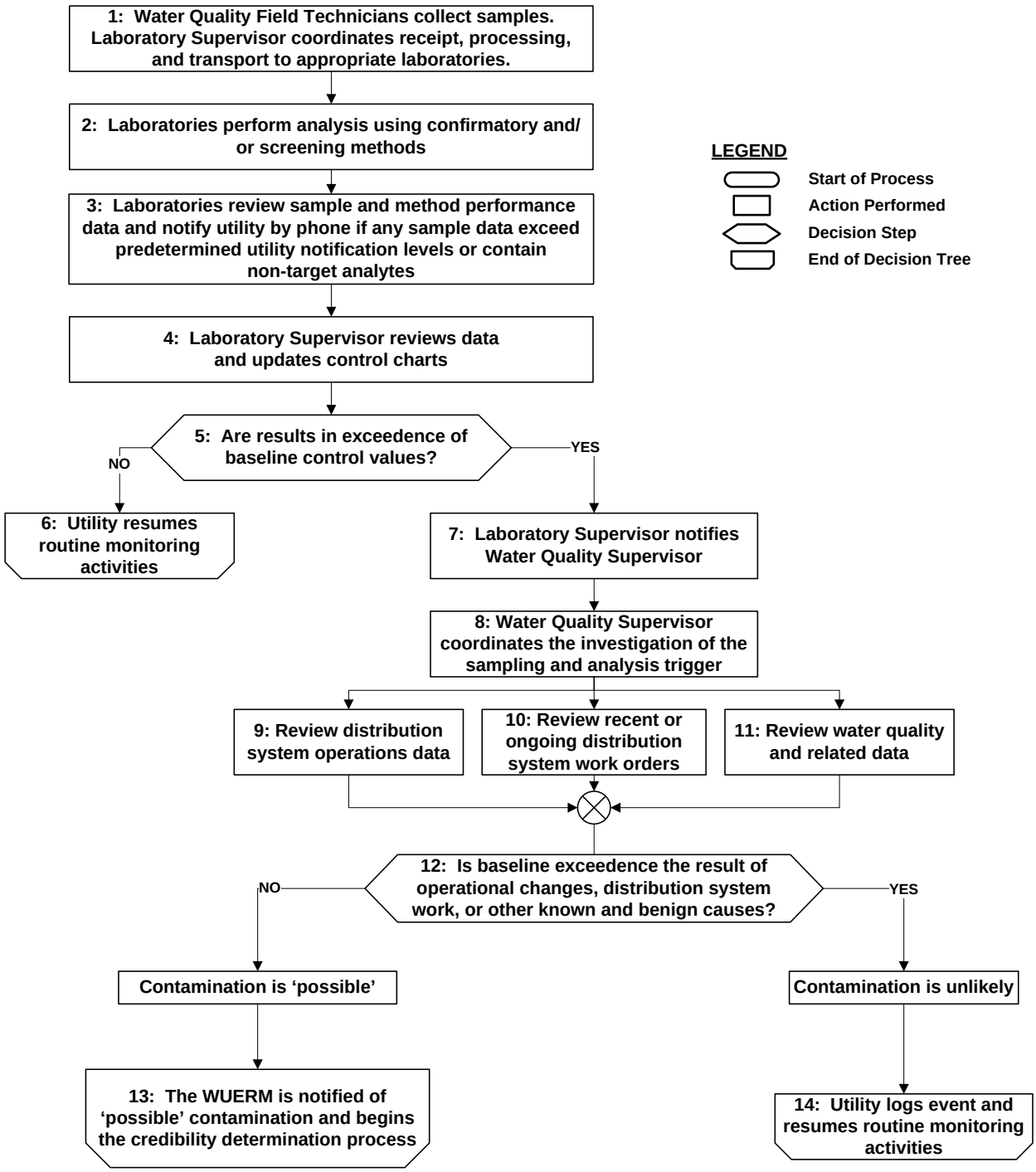

Figure A-2. Process Flow for Sampling and Analysis: Routine Monitoring and Initial Trigger Validation

1. **Water Quality Field Technicians collect samples. Laboratory Supervisor coordinates transfer of sample to appropriate laboratories for analysis.**

   - Collect samples from designated contamination warning system sampling locations using standard in-house procedures. As this is a routine sampling event, it is assumed that there is no hazard present unless otherwise indicated.
   - Receive samples from the field technicians and send samples to the appropriate laboratory for analysis, per instruction of the Laboratory Supervisor.

- Complete and maintain chain of custody forms in accordance with standard operating procedures.
- For samples to be analyzed by contract laboratory, a local courier picks up samples from the utility within 24 hours of collection.
- Contact courier to transport samples to State Health Department Laboratory for pathogen and radiochemical analyses.

2. Designated laboratories perform analyses using confirmatory and/or screening methods.

- Analyze samples for VOCs by Gas Chromatography / Mass Spectrometry with Purge and Trap Extraction, semivolatile organic compounds (SVOCs) by Gas Chromatography with Mass Spectrometry Detection using liquid-solid extraction (LSE), and cyanide by a colorimetry test.
- Analyze samples for carbamates using High Performance Liquid Chromatography with fluorescence determination and analyze samples for metals using Inductively Coupled Plasma – Mass Spectrometry.
- Analyze samples for BT Agents using Real-time PCR and Immunoassay (TRF) platforms and analyze radiochemicals by Gross Alpha and Gross Beta Scintillation and Gamma Spectroscopy.

3. Laboratories review sample and method performance data.

- Contact the utility Laboratory Supervisor by phone as soon as possible if any targeted contaminant result exceeds the pre-determined utility notification level or any non-targeted contaminants are detected. Any flags associated with the results should also be reported to aid in the interpretation of the data.
  - For chemicals and radiochemicals, each laboratory will be provided with utility notification levels for targeted analytes. For BT agent analysis, the utility notification levels are in accordance with the State Health Department and Laboratory Response Network protocols.
- Proceed with standard data reporting. This includes delivery of an electronic file compliant with the utility's Water Quality Database and a hardcopy deliverable summarizing results.

4. Laboratory Supervisor reviews data and updates control charts.

- Receive data from external laboratories by phone or electronically and work with the appropriate laboratory personnel to review data and update control charts.

5. Are results in exceedence of baseline control values?

- If "NO," baseline control values are not exceeded. Proceed to Step 6.
- If "YES," baseline control values are exceeded. Proceed to Step 7.

6. Resume routine monitoring activities.

- Baseline control values are not exceeded and utility resumes routine monitoring activities.

7. Laboratory Supervisor notifies the Water Quality Supervisor and provides the following information:

- Sample location.
- Sample date and time.
- Summary of analytical results and associated QA/QC data for both field and laboratory-based methods.
- Summary interpretation of results.

8. Water Quality Supervisor coordinates the investigation of the sampling and analysis trigger.

- Request the assistance of the appropriate utility personnel (i.e., SCADA Operator, Distribution Work Supervisor, etc.) in the investigation of analytical result that exceeds baseline control values. In the event that the Water Quality Supervisor is unavailable, a pre-assigned alternate may assume the lead in the investigation.
- Review distribution system operations data, as described under Step 9.
- Review distribution system work orders, as described under Step 10.
- Review water quality data and related information, as described under Step 11.

9. Use *Checklist A-3: Distribution System Operations Review* to check for distribution system operating conditions that could have influenced water quality at the sampling location, including the following:

- Pump operation.
- Tank levels and fill/drain status.
- Valve open/close status.
- Relevant system alarms (e.g., control limit, loss of power or communications, intrusion, etc.).
- Unusual demands (e.g., due to fire flow).
- Pressure anomalies in the vicinity of the sampling location.

10. Use *Checklist A-4: Distribution System Work Order Review* to check ongoing or recent distribution system work that could have influenced water quality at the sampling location, including the following:

- Main breaks, repairs, and replacement.
- Flushing operations.
- Water outages.
- Power outages.
- Other distribution system work that could have impacted water quality in the vicinity of the monitoring station(s).

11. Use *Checklist A-1: Contamination Warning System Trigger Investigation* to check water quality data and related information, including the following:

- Water quality trend lines from online water quality monitoring location(s) hydraulically linked to the location where the sample was collected, and based on date and time of sample collection. If the sampling and analysis trigger is based on pathogen analyses, the investigation should include data from chlorine sensors as well as heterotrophic plate counts and/or coliform data.
- Water quality trend lines for the finished water leaving the treatment plant that supplies the region where the sample was collected. Approximate travel time from the plant to the sampling location where the baseline exceedence occurred should be considered when selecting the time period for display of data from the treatment plant.
- Recent treatment plant operating conditions, process water quality, or source water quality.
- A change in source water at the location and time of sample collection.
- Historic water quality trends, such as seasonal patterns, which may not be reflected in baseline control charts.
- A log of previously observed water quality anomalies.

12. Is the baseline exceedence a result of operational changes, distribution system work, or other known and benign causes?

- If "NO," contamination is "possible". Go to Step 13.
- If "YES," contamination is considered unlikely, the investigation is closed and the trigger is logged. Go to Step 14.

13. The Water Utility Emergency Response Manager is notified that contamination is "possible" and begins the credibility determination process.

- If a baseline exceedence is identified and the contaminant was quantified using a confirmatory method then there is a high degree of confidence in the analytical result. The fact that the analytical result was from a confirmatory method is significant and should be given considerable weight when proceeding with credibility determination.
- If a baseline exceedence is identified based on the results of a screening method (i.e., is from any method that cannot provide both qualitative and quantitative information with accompanying valid QC), additional analyses should be performed to confirm and quantify the analytical result. When available, this information should be weighed against other information gathered through the credibility determination process.

14. Utility logs event and resumes routine monitoring activities.

- Conduct additional sampling and analyses, if necessary, to better understand the cause of the analytical result although contamination is considered unlikely based on available information.
- Document the investigation and any follow-up activities in the event that this information can aid in the interpretation of future deviations from the baseline.

Table A-10. Example Timeline for Validation of a Sampling and Analysis Trigger in the Context of an Operational Contamination Warning System

Process Activity ID Number	Process Activity Description	Expected Response Time (minutes)	Range of Response Times (minutes)
1-2	Collect and analyze samples[1]	7 days	1 – 14 days
3	Notify Laboratory Supervisor based on review of sample and method performance data	10	5 – 20
4	Laboratory Supervisor reviews data and updates control charts	10	5 – 20
7	Laboratory Supervisor notifies Water Quality Supervisor that results are in exceedence of baseline control values	5	1 – 10
8	Water Quality Supervisor initiates initial trigger validation and coordinates review of operational, work order, and other water quality data	5	2 – 10
9-11	**9**: Review distribution system operations data **10**: Review distribution system work orders **11**: Review water quality and related data	20	10 – 30
13	Notify the WUERM and initiate credibility determination process, along with additional analyses as necessary[2]	5	0 – 24 hours
	TOTAL ELAPSED TIME[3]	55	23 minutes – 25.5 hours

1. Note that for routine monitoring there is no urgency during the sample collection, shipping, and analysis, thus the lengthy duration for Steps 1 and 2. Also, the time for analysis of routinely collected samples is dependent on the analysis schedules of the various laboratories in the network.
2. This step includes confirmatory analysis, which if necessary, could take 24 hours or longer.
3. This is the total elapsed time from Steps 3 through 13.

Checklists

Three checklists, described in **Table A-11,** are used in the review of sampling and analysis triggers based on this example. The checklists are included in Section A.7.

Table A-11. Example Checklists Used during Investigation of a Sampling and Analysis Trigger

Reference	Checklist	User	Description
Checklist A-1	Contamination Warning System Trigger Investigation	Water Quality Supervisor	Checklist involves the analysis of water quality data and plant operating conditions in the interpretation of analysis results.
Checklist A-3	Distribution System Operations Review	SCADA Operator	Checklist involves the review of distribution system operations that may have influenced water quality at the sampling location.
Checklist A-4	Distribution System Work Order Review	Distribution Work Supervisor	Checklist involves the review of distribution system work orders that may have influenced water quality at the sampling location.

A.4: Enhanced Security Monitoring Standard Operating Procedures

Component Description

As a component of EPA's contamination warning system model, enhanced security monitoring may provide an indication of contamination through detection of security breaches that could provide an intruder with access to the drinking water supply. The enhanced security monitoring component is comprised of security monitoring enhancements at priority pump stations, reservoirs, and tanks in the distribution system. Security monitoring enhancements vary by facility, and are summarized in **Table A-12**.

Table A-12. Summary of Enhanced Security Monitoring Equipment per Location

Facility Name	Security Monitoring Device
Poplar Grove Storage Tank	Ladder Motion Sensor
Golf Drive Storage Tank	Ladder Motion Sensor and Hatch Switch
North Service Reservoir	Hatch Switches (3)
Hillcrest Reservoir	Level Switches (2) and Hatch Switches (5)
Fairview Pump Station	Indoor Fixed Mount Video Cameras (6)
	Door Contact Switches (3) and Hatch Switches (4)
	Indoor Motion Sensors (2)
	Security and Video Panel Tamper Contact
	Lighting Panel Tamper and Loss of Power Contact
Mitchell Pump Station	Indoor Pan Tilt Zoom Video Cameras (4)
	Outdoor Fixed Mounted Camera
	Door Contact Switches (8)
	Glass Break Sensors (4)
	Security and Video Panel Tamper Contact
	Lighting Panel Tamper and Loss of Power Contact

At elevated storage tanks, ladder motion sensors would signal an alarm if an intruder attempts to climb the ladder in an effort to reach the tank hatches. The ladder motion sensor alarms provide an added level of security as door contact switch alarms would also indicate whether someone had gained access to the enclosures. Hatch switch alarms installed on top of storage tanks would signal an alarm if an intruder were to tamper with a tank hatch opening. The combination of ladder motion sensor alarms and hatch alarms provides redundancy and a more reliable indication of a tampering event.

Fixed mount and pan-tilt-zoom video cameras are installed inside and/or at entrances to pump stations and are activated by door contact switches or internal motion sensor signals if an intruder were to attempt to gain access. The video system stores continuous video data on local video recorders, and transmits short duration event-based video clips in response to a detected security incident (e.g., door contact switch or motion sensor alarm) for review by utility personnel.

The alarm and video data are sent to a SCADA system via a digital cellular network. A GUI provides real-time alarm information (intrusion detection and video clips). In addition to the primary SCADA workstation installed in the utility's control center, remote workstations are installed in the utility security

office and guard station to provide utility security personnel with direct access to alarm information and video data.

Table A-12 shows that different types of security information are available from different facilities in the distribution system. Most notably, some facilities have video monitoring equipment, while others have only contact switches and motion sensors. There is an important distinction in the investigation of triggers from facilities with and without video monitoring equipment, as discussed below.

Roles and Responsibilities

Table A-13 shows that utility personnel in water quality, security, and distribution system operations have a role in enhanced security monitoring. Utility security personnel have a lead role in the investigation of enhanced security triggers, while the SCADA Operator has primary responsibility for routine monitoring of alarms, including security alarms.

Table A-13. Roles and Responsibilities for Routine Operation of Enhanced Security Monitoring

Job Function	Role in Enhanced Security Monitoring Component Operations
Utility Security Personnel	• Lead the investigation of all enhanced security triggers, including: intrusions, tampering incidents, witness accounts, and threats. • Assess the legitimacy of witness accounts of possible intrusion. • Notify local law enforcement if intrusion at a facility is suspected or a written or verbal threat is received. • Lead the on-site investigation of a security incident, with assistance from distribution field crews and local law enforcement, as necessary. • If an intrusion is confirmed, determine whether or not the intruder could have accessed the water supply. • Make the determination regarding whether or not a security incident is a "possible" contamination threat.
SCADA Operator	• Monitor all SCADA alarms 24/7/365, including security alarms. • Make the initial determination regarding whether or not the intrusion alarm has detected an apparent intruder. • Notify utility security personnel if an intrusion is suspected.
Distribution Work Supervisor	• Coordinate the site activities of field crews who may support utility security personnel in the on-site investigation of a security incident. • Review distribution system work activity to determine whether or not a security alarm could have been inadvertently caused by utility personnel.
Distribution Field Crews	• Perform site activities to support utility security personnel in the on-site investigation of a security breach.
Local Law Enforcement	• Conduct an investigation at the site of a security incident if warranted. • Interview potential witnesses to a security incident. • If an unlawful intrusion has been confirmed, establish a crime scene perimeter and initiate a criminal investigation.
Water Utility Emergency Response Manager (WUERM)	• Notify Water Quality Supervisor if contamination is possible. • Implement the consequence management plan as necessary.

Process Flow

The process flow in **Figure A-3** illustrates the steps taken during the investigation of an enhanced security monitoring trigger. The process begins with recognition of a security alarm as displayed on the SCADA GUI and ends with notification of the Water Utility Emergency Response Manager (if contamination is deemed "possible"), or with logging the incident (if contamination is deemed "not possible"). The anticipated timeline for validation of a trigger from enhanced security monitoring is presented in **Table A-14**.

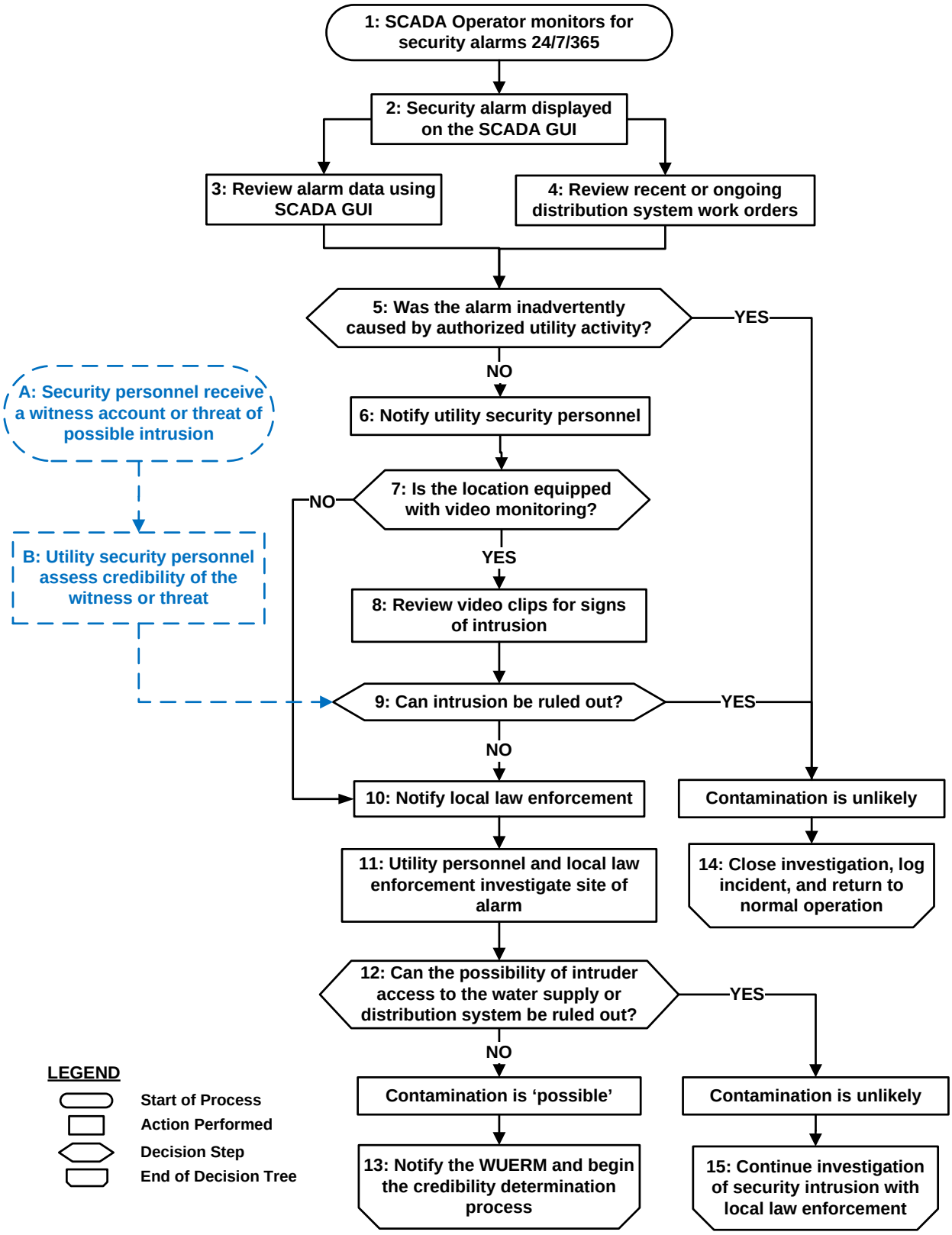

Figure A-3. Process Flow for Enhanced Security Monitoring: Routine Monitoring and Initial Trigger Validation

The process flow in Figure A-3 illustrates the primary process for investigating security alarms in Steps 1 through 15. A parallel process for investigating witness accounts and threat notifications is shown as

Steps A and B, which merges with the primary flow at Step 9 of the process flow. This parallel path is described directly below.

A. Security personnel receive a witness account or threat of possible intrusion/contamination.

- Utility security personnel may be alerted to a possible intrusion in the distribution system through witness accounts from utility employees or the public, and potentially through a direct threat of intrusion/contamination (e.g., threatening phone call). Unlike alarms, these alerts may occur at any location within the system.

B. Utility security personnel assess credibility of the witness account or threat.

- Assess the credibility of a witness through interviews, possibly in collaboration with local law enforcement.
- In the case of a direct threat to tamper with the water supply or utility property, local law enforcement should be contacted to assist in the assessment.
- Go to Step 9 of the primary process flow to determine whether or not intrusion can be ruled out.

1. SCADA Operator monitors for security alarms 24/7/365.

- Monitor the security alarms 24/7/365 using the SCADA GUI.
- Routine monitoring for security alarms is integrated into the procedures typically used for monitoring of other high priority SCADA alarms.

2. Security alarm displayed on the SCADA GUI.

- The SCADA GUI displays alarm status, date/time, location, and possibly video clips associated with a security alarm.
- The alarm is acknowledged to turn off the audible alarm.
- Security alarms are also displayed to other users with responsibility for monitoring security alarms, as listed in Table A-12, through remote workstations.

3. Review alarm data using the SCADA GUI for the following:

- Review available alarm information displayed on the SCADA GUI.
- Review the video clips from locations equipped with video cameras to assess whether or not the alarm may be a result of legitimate utility activity. If the review of video data shows signs of tampering that could have contaminated the water supply, utility security personnel should be notified immediately. Go to Step 6.
- Review information from contact alarms and motion sensors (for locations without video cameras) which may provide an indication of the location within the facility where activity is occurring. This spatial information may help to assess the nature of the activity and the number of individuals present.
- Contact the utility personnel thought to be at the site of the alarm for confirmation if legitimate utility activities are being conducted.

4. Use *Checklist A-4: Distribution System Work Order Review* to check ongoing or recent distribution system work that could have caused the security alarm.

- Notify the Distribution Work Supervisor about the security alarm and request support during the initial investigation.

- Review work orders to determine if utility personnel could have inadvertently caused the security alarm.
- Contact the utility personnel thought to be at the site of the alarm for confirmation if legitimate utility activities are being conducted.

5. Was the alarm inadvertently caused by authorized utility activity?

- If "YES," contamination is considered unlikely, the investigation is closed and the incident is logged. Go to Step 14.
- If "NO," continue the investigation. Go to Step 6.

6. Notify utility security personnel.

- Notify utility security personnel of a suspected, unauthorized intrusion.
- Utility security personnel review available alarm information displayed on the SCADA GUI.

7. Is the location equipped with video monitoring?

- If "YES," go to Step 8.
- If "NO," go to Step 10.

8. Review video clips for signs of unauthorized intrusion, including:

- Visual confirmation of unauthorized personnel.
- Signs of forced entry, such as damaged doors or broken windows.
- Signs of tampering, such as damaged utility equipment.
- Presence of non-utility equipment, such as tanks, drums, and pumps.
- If the review of video data shows signs of tampering that could have contaminated the water supply, contamination should immediately be considered "possible."

9. Can intrusion be ruled out?

- If "YES," contamination is considered unlikely. Go to Step 14.
- If "NO," continue the investigation. Go to Step 10.

10. Notify local law enforcement.

- At this point in the investigation, unauthorized intrusion is suspected.
- Contact local law enforcement from the jurisdiction where the facility is located to lead the criminal investigation.

11. Using *Checklist A-5: Security Incident Investigation,* utility security personnel, distribution field crews, and local law enforcement investigate the site of the alarm for the following:

- Visual confirmation of unauthorized personnel.
- Signs of forced entry, such as damaged doors or broken windows.
- Signs of tampering, such as damaged utility equipment.
- Presence of non-utility equipment, such as tanks, drums, pumps, containers, or unfamiliar apparatus.

- Signs of a security breach at any point that provides access to the drinking water supply.
- Precautions outlined in the Site Characterization Plan should be followed during the site investigation.

12. Can the possibility of intruder access to the drinking water supply or distribution system be ruled out?

- If "YES," contamination is considered unlikely. Go to Step 15.
- If "NO," contamination is considered "possible." Go to Step 13.

13. Notify the Water Utility Emergency Response Manager and initiate the credibility determination process.

- Once an intrusion has been confirmed and intruder access to the water supply cannot be ruled out, contamination is considered "possible."
- Utility security personnel notify the Water Utility Emergency Response Manager.
- The Water Utility Emergency Response Manager implements the credibility determination process, including investigation of other contamination warning system components, as described in the consequence management plan.

14. Close investigation, log alarm, and return to normal operation.

- At the conclusion of the investigation, if contamination can be ruled out, return to normal operation.
- Utility security personnel document the investigation of the security incident.

15. Continue investigation of security intrusion.

- If intrusion is confirmed but contamination is ruled out, the security aspect of the investigation should continue. The investigation should be a joint effort between utility security personnel and local law enforcement.
- Utility security personnel document the investigation of the security breach.

Table A-14. Example Timeline for Validation of a Security Trigger in the Context of an Operational Contamination Warning System

Process Activity ID Number	Process Activity Description	Expected Response Time (minutes)	Range of Response Times (minutes)
2	Security alarm displayed on SCADA GUI	2	1-5
3-4	**3**: Review ongoing distribution system activity **4**: Review alarm data using the SCADA GUI	10	5- 15
6	Notify utility security personnel	2	1-5
8	Review video clips if site is equipped with video cameras	6	4-10
10	Notify local law enforcement	2	1-5
11-12	Investigate site of security alarm and assess possible access to the drinking water supply	60	30–120
13	Notify the WUERM and begin the credibility determination process	15	5 -20
	TOTAL ELAPSED TIME	**97**	**47-180**

The time to trigger validation may be substantially reduced for sites with video monitoring equipment if the video record shows clear evidence regarding unauthorized intrusion (i.e., the trigger may be resolved at Step 4 in fewer than 10 minutes). Also, if the alert comes through a witness account or intrusion/contamination threat warning, the time to complete the trigger validation process may be reduced by 10 to 30 minutes.

Checklists

Two checklists, described in **Table A-15,** are used in the review of enhanced security triggers based on this example. The checklists are included in Section A.7.

Table A-15. Example Checklists Used during Investigation of an Enhanced Security Trigger

Reference	Checklist	User	Description
Checklist A-4	Distribution System Work Order Review	Distribution Work Supervisor	Checklist involves the review of distribution system work orders that may have caused a security alarm.
Checklist A-5	Security Incident Investigation	Utility Security Personnel	Checklist covers activities during investigation of a security breach.

A.5: Consumer Complaint Surveillance Standard Operating Procedures

Component Description

As a component of EPA's contamination warning system model, consumer complaint surveillance may provide an indication of contamination through detection of unusual trends or characteristics in consumer calls regarding water quality issues. The component design is based on the principles of funnel, filter, and focus. Calls from multiple sources are funneled into the utility's call center. Next, calls are filtered by customer service representatives in the call center to eliminate issues that do not involve unusual water quality. Finally, focus is achieved through the collection of additional information about unusual water quality concerns that may lead to detection of a water quality anomaly resulting in a consumer complaint surveillance trigger.

The central element of the consumer complaint surveillance component is an event detection system that uses algorithms to detect anomalies through analysis of the compiled data at various points through the system. **Table A-16** summarizes the data streams, information system and algorithms used by the event detection system to analyze those data streams.

Table A-16. Summary of the Algorithms used in the Consumer Complaint Surveillance Event Detection System

Data Stream	Information System	Event Detection System
Interactive Voice Response	Call Management System	Callers use a voice menu to select the reason for their call, including an option to indicate a water quality concern. A scan statistic is used to detect excursions above an established base-state that is specific to both day of the week and time of day.
Customer Service Representative Call Log	Call Management System	Customer Service Representatives log each call within predefined categories, one of which captures unusual water quality concerns. A scan statistic is used to detect excursions above an established base-state that is specific to both day of the week and time of day. This is similar to the algorithm used for the interactive voice response system, but the Call Log provides a more accurate characterization of the nature of the call and eliminates routine concerns, such as rusty or cloudy water.
Water Quality Work Orders	Work Order System	A water quality call may result in creation of a work order to investigate the issue raised by the consumer. GIS is used to analyze for unusual clusters of water quality work orders relative to an established base-state.
Detailed Description of Water Quality Issues	Water Quality Database	Unusual water quality issues are referred to a designated customer representative who interviews the caller to obtain detailed information regarding the nature of the concern. An anomaly detection algorithm analyzes the collective data for anomalies in the characteristics, as well as the temporal distribution, of reported water quality issues.

A dedicated server on the utility's local area network (LAN) hosts the consumer complaint surveillance event detection system, comprised of the algorithms described in Table A-16. This server also hosts the application that integrates information that resides in the three supporting IT systems: Call Management System, Work Order System, and Water Quality Database, in addition to the city's GIS platform that provides a means of spatial analysis and display of information. Because the server is located on the LAN, the consumer complaint surveillance event detection system can be accessed from any workstation connected to the network by users with the appropriate credentials.

Roles and Responsibilities

Table A-17 shows that utility personnel in water quality, distribution system operation, and customer service have a role in consumer complaint surveillance. While not explicitly shown, other city departments and call centers may receive calls related to water quality issues. These partners have been provided with a backdoor number to the utility to ensure that all such calls are funneled into the utility's consumer complaint surveillance process.

Table A-17. Roles and Responsibilities for Routine Operation of Consumer Complaint Surveillance

Job Function	Role in Consumer Complaint Surveillance Component Operations
Water Quality Supervisor	• Assume the lead in the investigation of a consumer complaint surveillance alarm. • Coordinate support from appropriate utility personnel during investigation of a consumer complaint surveillance alarm. • Review the collective data from the investigation and make the determination regarding whether or not the consumer complaint surveillance trigger is a "possible" contamination threat. • Notify the Water Utility Emergency Response Manager if the determination is made that contamination is "possible."
Water Quality Customer Service Representative	• Serve as a subject matter expert in the area of water quality and common customer water quality concerns. • Monitor for consumer complaint surveillance alarms during normal business hours. • Interview customers who contact the utility with questions or concerns regarding water quality issues. • Decide whether or not to create a work order to respond to a water quality concern raised by a customer.
Water Quality Field Technician	• Lead the field investigation of a consumer complaint in response to a water quality work order.
Customer Service Representative	• Receive all calls to the utility, including those dealing with water quality issues, during normal business hours. • Advise customers about water quality concerns related to typical distribution system issues (e.g., rusty water, chlorine odor, etc.) without additional support, unless requested by the customer. • Identify calls that deal with unusual or complex water quality issues, and forward those calls on to the Water Quality Customer Service Representative.
SCADA Operator	• Review distribution system operations to support the investigation of a consumer complaint surveillance trigger.
Distribution Work Supervisor	• Monitor for consumer complaint surveillance alarms during non-business hours when customer calls are re-routed to the Distribution Operations center. • Receive all emergency calls to the utility during non-business hours, including those related to water quality concerns. • Advise customers about water quality concerns related to typical distribution system issues (e.g., rusty water, chlorine odor, etc.). • Decide whether or not to create a work order to respond to a water quality concern raised by a customer during non-business hours. • Assign distribution field crews to support the field investigation of a consumer complaint. • Review distribution system work orders to support the investigation of a consumer complaint surveillance alarm.
Distribution Field Crews	• Support the water quality field technician during the field investigation of a consumer complaint.
Water Utility Emergency Response Manager (WUERM)	• Review water quality data and related information during the investigation of a consumer complaint surveillance trigger when the Water Quality Supervisor (or alternate) is unavailable. • Implement the consequence management plan as necessary.

Process Flow

The process flow for consumer complaint surveillance is shown in two diagrams for clarity. **Figure A-4** presents the process flow for routine operation, illustrating how consumer calls are funneled, filtered, and focused to efficiently identify water quality issues. **Figure A-5** presents the process flow, beginning with routine monitoring for consumer complaint surveillance triggers, the process for investigating a trigger, and the determination regarding "possible" contamination. The anticipated timeline for validation of a trigger from consumer complaint surveillance is presented in **Table A-18**.

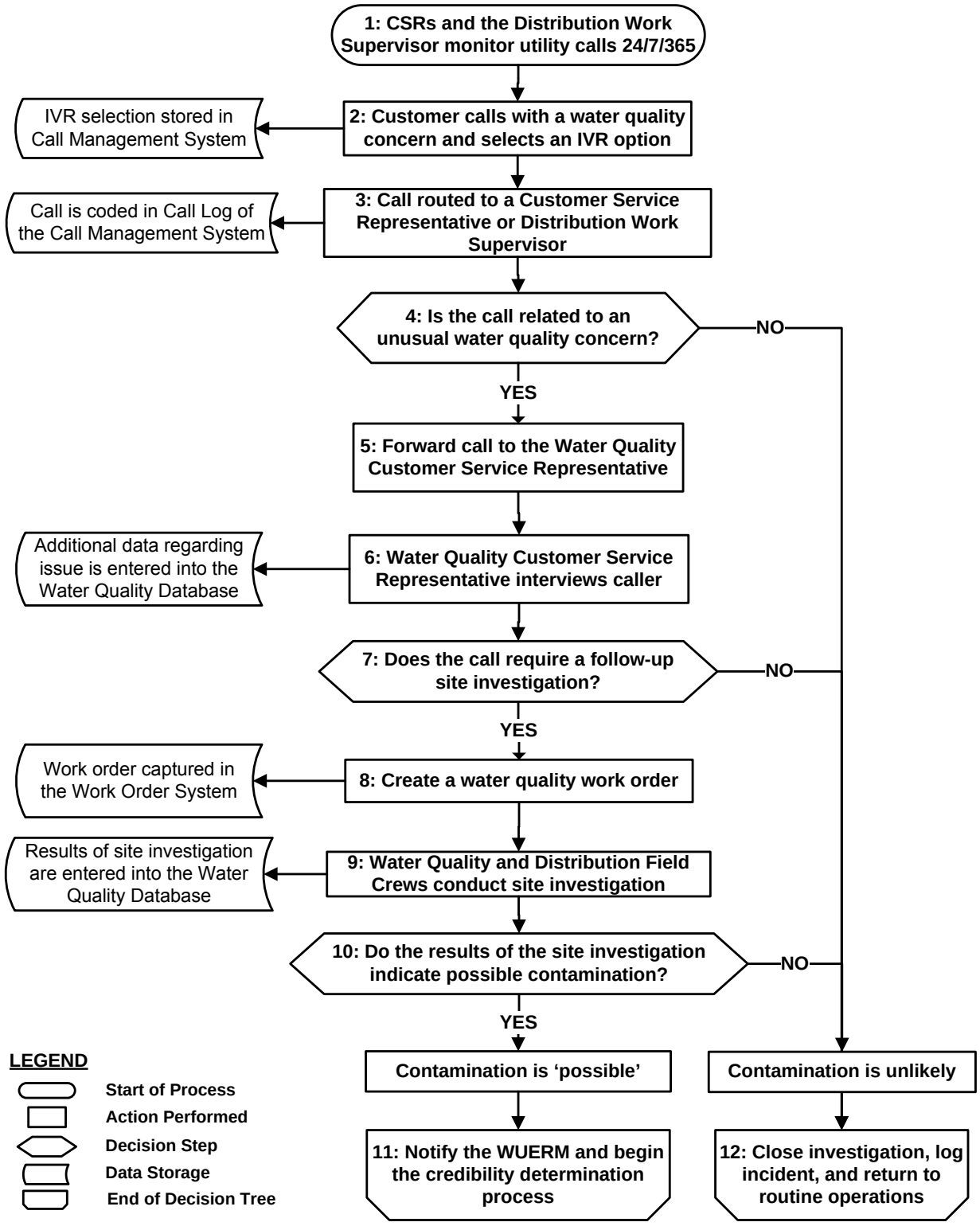

Figure A-4. Process Flow for Consumer Complaint Surveillance: Routine Monitoring

1. Monitor consumer complaint calls to the utility 24/7/365.

- Customer service representatives (CSRs) handle all calls to the utility during normal business hours.

- The Distribution Work Supervisor handles emergency calls to the utility during non-business hours, including calls from customers with concerns about water quality.
- Callers with non-emergency calls are directed to the interactive voice response (IVR) system and encouraged to call back during normal business hours.

2. Customer calls with a water quality concern.

- Consumers are directed to call one number for any issue related to drinking water, including water quality concerns. If consumer calls another local call center or department within the utility's service area, the call recipient has been trained to route the call to the utility via a backdoor number.
- Calls to the utility call center are processed through an interactive voice response system, which presents callers with a voice menu with an option for "water quality questions or concerns."
- The caller's selection from the voice menu is stored in the Call Management System.

3. Call routed to a Customer Service Representative or Distribution Work Supervisor.

- Calls for which the "water quality questions or concerns" option is selected from the voice menu are moved to the front of the queue during normal business hours or routed directly to the Distribution Work Supervisor during non-business hours.
- Verify the location the customer is calling about and determines the type of water quality concern.
- Typical water quality issues handled by the Customer Service Representative or Distribution Work Supervisor include: rusty water, chlorine odor, and cloudy water due to dissolved air.
- Code all calls in Call Log once the nature of the water quality concern has been identified.

4. Is the call related to an unusual water quality concern?

- If "YES," consumer complaint tracking continues. Go to Step 5.
- If "NO," consumer complaint tracking stops and the call is handled according to routine utility procedures. Go to Step 12.

5. Forward call to the Water Quality Customer Service Representative.

- If the customer water quality concern is received during non-business hours, the Distribution Work Supervisor handles the call as described in Step 6.

6. Water Quality Customer Service Representative uses *Checklist A-6: Water Quality Customer Complaint Investigation* to interview the caller.

- Collect additional information about the nature of the water quality issue from the caller. If the caller has difficulty describing the issue, the categories listed in the checklist can be presented for self-selection by the caller.
- Standardize and enter the information collected during the interview into the Water Quality Database.

7. Does the call require a follow-up site investigation?

- If "YES," consumer complaint tracking continues. Go to Step 8.
- If "NO," consumer complaint tracking stops and the call is handled according to routine utility procedures. Go to Step 12.

8. Create a water quality work order.

- Create a work order in the Work Order System once it is determined that a site investigation is necessary.

9. Conduct site investigation.

- Identify a field crew to support the site investigation.
- Determine whether or not utility personnel can be sent to the site to conduct the investigation. If conditions are considered too hazardous for utility personnel, contamination is deemed "possible." Go to Step 11 and seek additional support (e.g., a Hazmat responder) to investigate the site.
- Dispatch field crew to the site of the reported water quality issue. Precautions outlined in a Site Characterization Plan should be followed during the field investigation.
- Record results of the inspection in the *Checklist A-2: Distribution System Site Investigation.*
- Report the results to the Water Quality Customer Service Representative or Distribution Work Supervisor from the field as they become available.

10. Do the results of the field investigation indicate contamination?

- If "YES," contamination is considered "possible." Go to Step 11.
- If "NO," consumer complaint tracking stops and the call is handled according to routine utility procedures. Go to Step 12.

11. Notify the Water Utility Emergency Response Manager and initiate the credibility determination process.

- If the field investigation yields signs of contamination or site hazards, contamination is considered "possible" without going through the steps of the initial trigger validation process flow in Figure A-5.
- The Water Quality Customer Service Representative or Distribution Work Supervisor notifies the Water Utility Emergency Response Manager.
- The Water Utility Emergency Response Manager implements the credibility determination process, including investigation of other contamination warning system components, as described in the consequence management plan.

12. Close investigation, log alarm, and return to normal operation.

- Once sufficient information is collected to determine that a call is not related to an unusual water quality issue, it is filtered out of the consumer complaint surveillance process.
- While the call may not relate to unusual water quality, it may still require follow-up by the utility. Normal utility procedures are followed to resolve any calls filtered out of the consumer complaint surveillance process.

Figure A-5, below, presents the process flow for initial trigger validation, showing the process for routine monitoring of consumer complaint surveillance triggers, steps in the trigger investigation, and the determination regarding "possible" contamination.

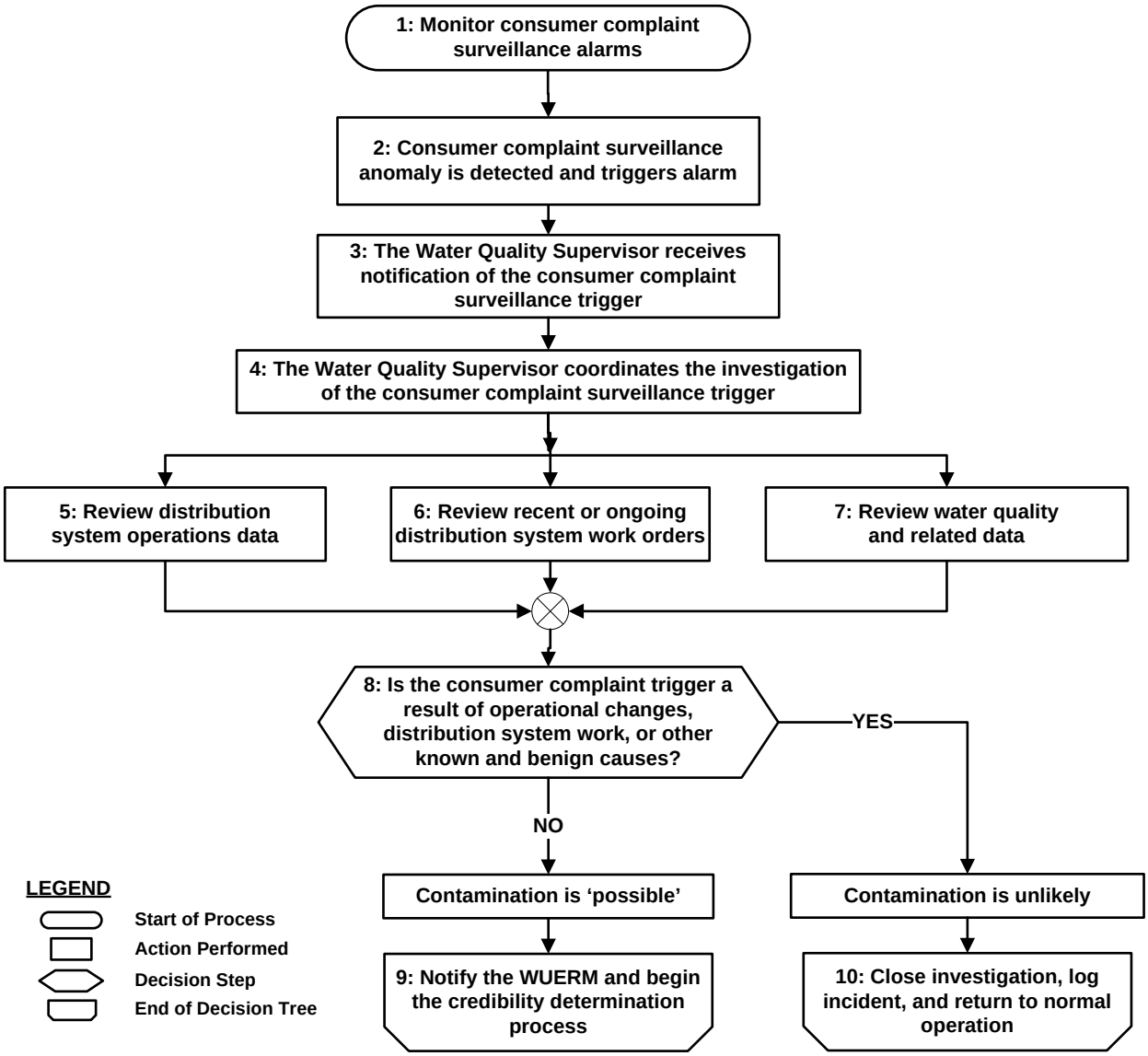

Figure A-5. Process Flow for Consumer Complaint Surveillance: Initial Trigger Validation

1. **Monitor for consumer complaint surveillance alarms.**

   - The Water Quality Customer Service Representative monitors for alarms during normal business hours.
   - The Distribution Work Supervisor monitors for alarms during non-business hours.

2. **Consumer complaint surveillance anomaly is detected and triggers alarm.**

   - The consumer complaint event detection system operates in real-time, continuously updating the alarm status for each consumer complaint surveillance data stream listed in Table A-16. When a consumer complaint anomaly is detected, the alarm status will change to alert the Water Quality Customer Service Representative or Distribution Work Manager.
   - The consumer complaint surveillance alarm includes the following information: dates and times of complaints, locations of water quality complaints, and possibly annotated information about the call.

3. **Water Quality Supervisor receives notification of the consumer complaint surveillance trigger.**

   - If the consumer complaint surveillance alarm occurs during non-business hours, a pre-assigned alternate is notified.

4. **The Water Quality Supervisor coordinates the investigation of the consumer complaint surveillance trigger.**

   - Request the assistance of the appropriate utility personnel (i.e., SCADA Operator, Distribution Work Supervisor, etc.) in the investigation of a consumer complaint surveillance alarm.
   - Review distribution system operations data, as described under Step 5.
   - Review recent and ongoing distribution system work, as described under Step 6.
   - Review water quality data and related information, as described under Step 7.

5. **Use *Checklist A-3: Distribution System Operations Review* to check for distribution system operating conditions that could have influenced water quality aesthetics at the location of the consumer complaint anomaly, including the following:**

   - Pump operation.
   - Tank levels and fill/drain status.
   - Valve open/close status.
   - Relevant alarms (e.g., control limit, loss of power, loss of communications, intrusion, etc.)
   - Large, unusual demands (e.g., due to fire flow).
   - Pressure anomalies.

6. **Use *Checklist A-4: Distribution System Work Order Review* to check ongoing or recent distribution system work that could have influenced water quality aesthetics at the location of the consumer complaint anomaly, including the following:**

   - Main breaks, repairs, and replacement.
   - Flushing operations.
   - Other distribution system work that could have impacted water quality aesthetics in the vicinity of the sampling location(s) such as tank cleaning or painting, tank or pipe relining, etc.

7. **Use *Checklist A-1: Contamination Warning System Trigger Investigation* to check water quality data and other information potentially related to the trigger, including the following:**

   - Spatial representation of the data that produced the alarm to determine if there is a pattern or cluster in the water quality calls.
   - Characteristics of the reported water quality issues to determine if there are similarities in the reported aesthetic qualities.
   - Recent water quality data from water quality monitoring stations upstream or downstream from the consumer complaint anomaly.
   - Finished water quality data from the treatment plant that supplies the region in which the consumer complaint occurred. Approximate travel time from the plant to the location of the complaint should be considered when selecting the time period for analysis.
   - Recent treatment plant operating conditions, process water quality, or source water quality.

8. **Is the consumer complaint surveillance trigger a result of operational changes, distribution system work, or other known and benign causes?**

   - If "YES," contamination is considered unlikely. Go to Step 10.
   - If "NO," contamination is considered "possible." Go to Step 9.

9. **Notify the Water Utility Emergency Response Manager and initiate the credibility determination process.**

   - Once all reasonable explanations for the consumer complaint surveillance trigger have been assessed and ruled out contamination is considered "possible."
   - The Water Quality Supervisor notifies the Water Utility Emergency Response Manager.
   - The Water Utility Emergency Response Manager implements the credibility determination process, including investigation of other contamination warning system components, as described in the consequence management plan.

10. **Close investigation, log alarm, and return to normal operation.**

    - At the conclusion of the investigation, if contamination can be ruled out, the system returns to normal operation. However, some level of investigation may continue if the anomaly is indicative of an operational or water quality problem.
    - The Water Quality Supervisor documents the review and assessment of the consumer complaint surveillance trigger by compiling the checklists used in the investigation.

Table A-18. Example Timeline for Validation of a Consumer Complaint Surveillance Trigger in the Context of an Operational Contamination Warning System

Process Activity ID Number	Process Activity Description	Expected Response Time (minutes)	Range of Response Times (minutes)
2	Consumer complaint surveillance anomaly triggers an alarm through analysis any of the data streams listed in Table A-16	2	1-5
3	Notify Water Quality Supervisor	3	2-10
4	Initiate the trigger investigation and request support from appropriate utility personnel	5	2-10
5-7	**5**: Review distribution system operations data **6**: Review distribution system work orders **7**: Review water quality and related data	20	10-30
8	Evaluate initial data and conduct determination regarding "possible" contamination	20	10-30
9	Notify the WUERM and begin the credibility determination process	15	5-20
	TOTAL ELAPSED TIME	**65**	**30-105**

Checklists

Five checklists, described in **Table A-19,** are used in the review of consumer complaint surveillance triggers based on this example. The checklists are included in Section A.7.

Table A-19. Example Checklists Used during Investigation of a Consumer Complaint Surveillance Trigger

Reference	Checklist	User	Description
Checklist A-1	Contamination Warning System Trigger Investigation	Water Quality Supervisor	Checklist involves the review of water quality data, plant operating conditions, spatial distribution of consumer calls, and the nature of the reported water quality concern to determine if the problem is systematic.
Checklist A-2	Distribution System Site Investigation	Water Quality Field Technician	Checklist is used to document observations during field investigation of a consumer complaint.
Checklist A-3	Distribution System Operations Review	SCADA Operator	Checklist involves the review of distribution system operating conditions that could have influenced water quality aesthetics at the location of the consumer complaint.
Checklist A-4	Distribution System Work Order Review	Distribution Work Supervisor	Checklist involves the review of distribution system work orders that could have influenced water quality aesthetics at the location of the consumer complaint.
Checklist A-6	Water Quality Consumer Complaint Investigation	Water Quality Customer Service Representative	Checklist facilitates the collection of information from callers reporting unusual water quality concerns.

A.6: Public Health Surveillance Standard Operating Procedures

Component Description

Public health surveillance systems gather and analyze health-related data to identify anomalies, or triggers that might indicate unusual incidence of disease. The role of public health surveillance in EPA's contamination warning system model is to gather and analyze data for investigation that will augment traditional epidemiological surveillance (which often relies on an astute clinician to notice and report anomalies, or triggers) in order to determine whether a public health event could be attributable to drinking water. The public health data streams discussed in **Table A-20** may be used to detect chemical or biological contaminants, as indicated.

Table A-20. Data Streams, Public Health Partners, and Detection Capabilities

Data Stream / Source	Public Health Partner	Target Contaminant Types Detected
911 call data and EMS logs	Fire Department	Fast-Acting Chemicals
Poison Control Center calls	Regional Poison Control Center	Fast-Acting Chemicals
Over-the-Counter drug sales	Local Public Health Department	Pathogens
Infectious disease reports	Local Public Health Department	Pathogens
Emergency room chief complaints	Local Public Health Department	Pathogens

Each public health data stream provides community level health information. The detail of this information and the ability to share it is limited by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA aims to preserve the privacy of medical records by mandating protections on the communication of medical data, and typically protects certain information that can be used to identify an individual. Measures to remain compliant with HIPAA should be taken when using public health surveillance data.

911 call data and EMS logs are gathered from the local fire department in as near real-time as possible and analyzed using statistical algorithms, to identify anomalies that may be indicative of fast-acting chemical contamination. An agreement with the local poison control center established analysis protocols to detect fast-acting chemical contamination, as well as provide toxicological expertise in handling any sort of public health event. Over-the-counter drug sales are monitored through the National Retail Data Monitor to detect increases of sales that could be associated with public exposure to pathogens; likewise, infectious disease records and emergency room chief complaints are collected and monitored to detect changes in baseline for the identified syndromic categories using the Real-time Outbreak Disease Surveillance (RODS) tool. Automated data gathering, analysis, and alert generation are emphasized in order to maximize the potential for timely contamination detection and investigation.

Roles and Responsibilities

The role of public health experts in routine operation of the contamination warning system is to provide information that might not otherwise be available to utilities. This allows for a coordinated investigation and response to determine whether or not an association between public health events and water quality anomalies is possible. As listed in **Table A-21**, water quality personnel, SCADA operators, and distribution personnel within the utility play a critical role working in concert with local public health partners as part of the operational strategy.

Table A-21. Roles and Responsibilities for Routine Operation of Public Health Surveillance

Job Function	Role in Routine Operation of Public Health Surveillance
Fire Department	• Provide HIPAA-compliant EMS and/or 911 data. • Ensure data meet mutually agreed upon quality control requirements.
Poison Control Center	• Provide HIPAA-compliant Poison Control data. • Provide supplemental toxicological expertise. • Ensure data meet mutually agreed upon quality control requirements.
Local public health agencies within utility service area	• Investigate public health surveillance triggers. • Make the determination whether or not public health surveillance trigger could be related to drinking water. • Notify the utility Water Quality Supervisor if the determination is made that the public health surveillance trigger could be related to drinking water. • Discuss data with the Water Quality Supervisor to help determine whether public health surveillance trigger is a "possible" drinking water contamination threat.
Water Quality Supervisor	• Receive notification of public health surveillance triggers. • Review pertinent water quality data and the status of other components to assess spatial and/or temporal correlations to public health surveillance trigger. • Discuss data with public health surveillance partners and make the determination regarding whether or not the public health surveillance trigger is a "possible" drinking water contamination threat. • Notify the Water Utility Emergency Response Manager if the determination is made that the public health surveillance trigger is a "possible" drinking water contamination threat.
Laboratory Supervisor	• Review analytical results to investigate a potential link between water and the public health surveillance trigger.
SCADA Operator	• Review distribution system operations data to investigate a potential link between water and the public health surveillance trigger.
Distribution Work Supervisor	• Review maintenance activities to investigate a potential link between water and the public health surveillance trigger.
Water Utility Emergency Response Manager (WUERM)	• Review water quality data and related information during the investigation of a public health surveillance trigger when the Water Quality Supervisor (or alternate) is unavailable. • Implement the consequence management plan as necessary.

Process Flows

The process flow for public health surveillance in **Figure A-6** shows investigation procedures for both the public health officials and utility officials, and illustrates how they relate to one another. In EPA's contamination warning system model, public health data are monitored and analyzed to identify triggers, and local public health determines whether or not a trigger is considered valid and could be indicative of a possible drinking water contamination event. The public health agency will then notify the utility Water Quality Supervisor, who in turn investigates utility data to determine whether or not the public health trigger may be related to drinking water quality. The investigation continues until it is determined either that the trigger is related to drinking water contamination or that drinking water contamination can be reliably ruled out. The anticipated timeline for validation of a trigger from public health surveillance is presented in **Table A-22**.

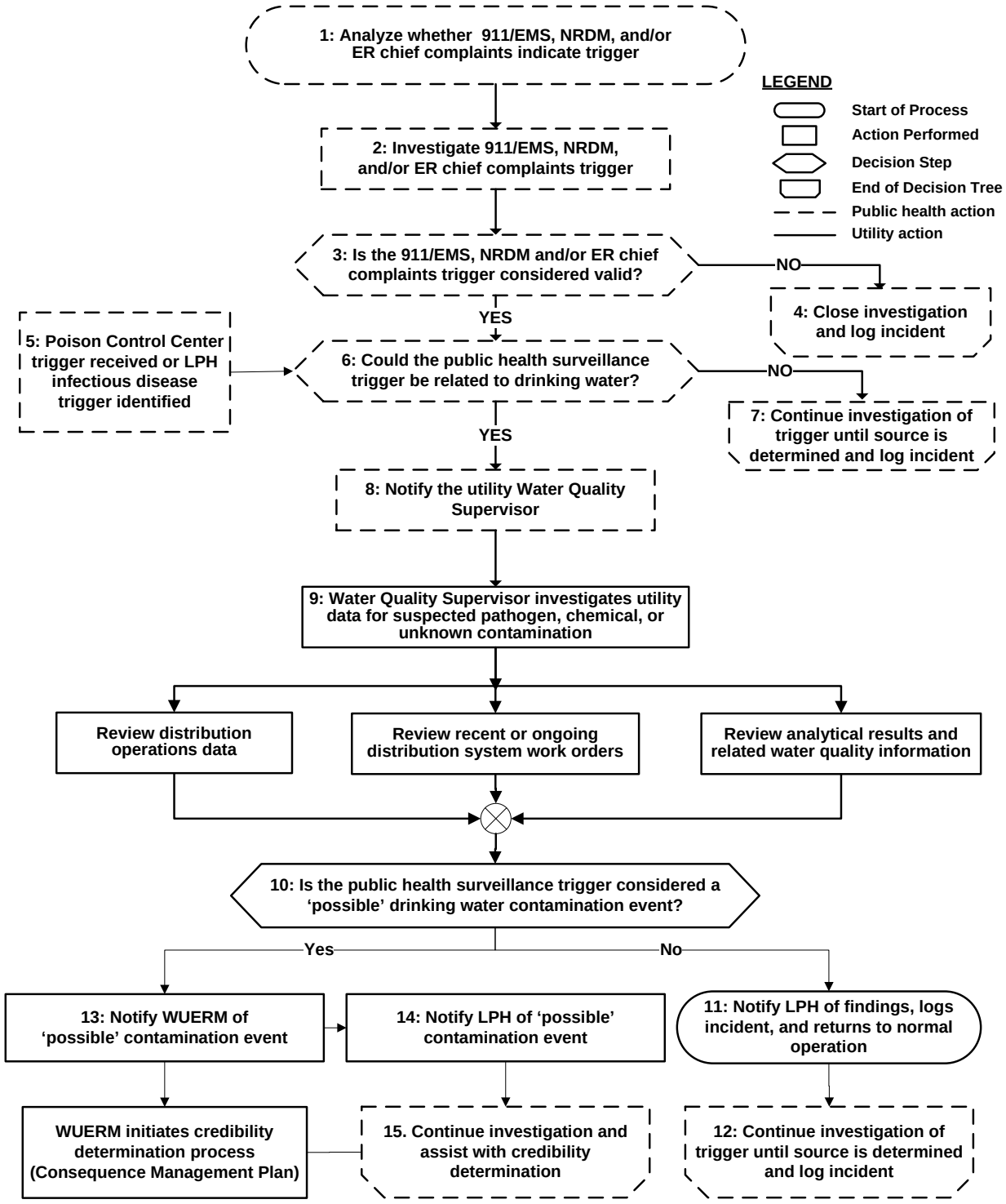

Figure A-6. Process Flow for Public Health Surveillance: Routine Monitoring and Initial Trigger Validation

1. **Analyze data from the 911/EMS, National Retail Drug Monitor, and/or emergency room chief complaint for potential triggers.**

   - Designated Epidemiology/Disease Investigation personnel from the Local Public Health agency (or agencies) receive a trigger for the data stream through public health surveillance tools.

2. Use *Checklist A-7: Public Health Surveillance Trigger Investigation* to support review of 911/EMS, National Retail Drug Monitor, and/or emergency room chief complaint data.

- Investigate the characteristics of the trigger:
  - 911/EMS trigger: do the calls occur in one area, or "cluster?" What chief complaint or syndrome differs from the expected health of the community?
  - National Retail Drug Monitor trigger: what over-the-counter medicine category is being sold at a rate higher than the established base-state?
  - Emergency room chief complaint trigger: what chief complaint syndrome category differs from the established base-state?
- Verify that underlying data are properly coded (e.g., does not contain an unusual amount of missing data).
- Review the other public health surveillance data streams for corresponding trends.
- Develop a preliminary hypothesis regarding the cause of the trigger, such as whether the causative agent is a pathogen or chemical and the potential source(s) of exposure, or if the trigger is a false alarm.

3. Is the 911/EMS, National Retail Drug Monitor, and/or emergency room chief complaint trigger considered valid?

- If no, proceed to Step 4. The trigger is not considered valid when it is not supported by other available public health data.
- If yes, proceed to Step 6. The trigger is considered valid if other available public health data streams or supplemental information indicate a public health episode. For example, an increase in over-the-counter anti-nausea medications corresponds to an increase in emergency room chief complaints for nausea and vomiting. There may be a time delay between when alarms may be generated by these data streams; this should be considered in the investigation.

4. Close investigation and log alarm.

- Document the investigation and the reason(s) for determining the trigger to be a false alarm using *Checklist A-7: Public Health Surveillance Trigger Investigation*.

5. Receipt of trigger from Poison Control Center or Local Public Health infectious disease surveillance.

- Poison Control Center notifies Local Public Health via phone of a change from the established base-state; notification includes the Poison Control Center's preliminary hypothesis regarding the cause of the trigger, such as whether the causative agent is a pathogen or chemical, and the potential source(s) of exposure.
- Local Public Health Epidemiologist/Disease Investigation personnel identify a change in established base-state during the course of their routine infectious disease surveillance activities; this trigger may include notification from an astute physician of a situation with an unusual cluster of illnesses.

6. Could the public health surveillance trigger be related to drinking water?

- If no, proceed to Step 7. Trigger may be attributable to another known incident, or the symptoms presented are not indicative of water-based illnesses.
- If yes, proceed to Step 8. Trigger could possibly be water related if symptoms or other patterns presented relate to illnesses and conditions caused by pathogen or chemical water contamination.

7. Continue investigation until source of trigger is identified and log alarm.

- Monitor relevant public health surveillance data streams until the source of the trigger is identified or the trigger is determined to be a false alarm.
- Log trigger upon conclusion of investigation using *Checklist A-7: Public Health Surveillance Trigger Investigation*.

8. Notify utility Water Quality Supervisor.

- Notify utility Water Quality Supervisor via telephone of the trigger and provide the following information:
  - Type of trigger (i.e., 911/EMS, National Retail Drug Monitor, emergency room chief complaint, Poison Control Center, physician, other).
  - Data element(s) causing trigger (i.e., provider impression, chief complaint, type of over-the-counter).
  - Additional indicators of a public health issue from other public health surveillance streams, or the absence of such indicators.
  - Time frame of cluster.
  - Zip code(s).
  - Hypothesis regarding the cause of health effects (i.e., pathogen, chemical, unknown) and the potential source(s) of exposure.
  - Plans for further investigation, including estimated timeline.

9. Water Quality Supervisor investigates utility data for suspect pathogen, chemical, or unknown contamination.

- Review records from the previous 21 days (in cases of suspected pathogen), previous 24 hours (in cases of suspected chemical), or both (for unknown contaminant) for other contamination warning system triggers: water quality, routine sampling & analysis, consumer complaint surveillance, and security alarms that could be spatially or temporally related to the public health episode. Use *Checklist A-1: Contamination Warning System Trigger Investigation*.
- Contact Distribution Work Supervisor to review distribution system operations data, including online water quality monitoring data for previous 21 days (in cases of suspected pathogen, 24 hours (in cases of suspected chemical), or both (for unknown contaminant). Use *Checklist A-3: Distribution System Operations Review*.
- Contact Distribution Work Supervisor to review distribution system work activities for previous 21 days (in cases of suspected pathogen, 24 hours (in cases of suspected chemical), or both (for unknown contaminant). Use *Checklist A-4: Distribution System Work Order Review*.
- Contact Laboratory Supervisor to review pertinent analytical results for sampling records not included in contamination warning system triggers, such as coliform and/or HPC, for the previous 21 days (in cases of suspected pathogen, 24 hours (in cases of suspected chemical), or both (for unknown contaminant), for all sample locations.

10. Is the trigger considered a "possible" drinking water contamination threat?

- If no, proceed to Step 11. The collective results of the utility investigation indicate normal operations.
- If yes, proceed to Step 13. The collective results of the utility investigation indicate that the public health event may be related to drinking water.

11. Notify Local Public Health of findings and return to normal operations:

- Email Local Public Health Epidemiologist/Disease Investigator a copy of *Checklist A-1: Contamination Warning System Trigger Investigation* which documents that no corresponding contamination warning system triggers or abnormal water quality test results occurred during the time period investigated.
- Return to normal operations.

12. Local Public Health continues investigation until source of trigger is identified and logs alarm.

- Monitor relevant public health surveillance data streams until the source of the trigger is identified or the trigger is determined to be a false alarm. If at any time drinking water is suspected as the source of the trigger, return to Step 8.
- Log trigger upon conclusion of investigation using *Checklist A-7: Public Health Surveillance Trigger Investigation*.
- Email a copy of *Checklist A-7: Public Health Surveillance Trigger Investigation* to the utility Water Quality Supervisor for the utility's records.

13. Notify the Water Utility Emergency Response Manager.

- Notify the Water Utility Emergency Response Manager of the "possible" drinking water contamination threat and provide the details of the public health surveillance trigger and corresponding information.
- Water Utility Emergency Response Manager initiates credibility determination process as outlined in the consequence management plan.

14. The Water Utility Emergency Response Manager notifies Local Public Health of a "possible" drinking water contamination event.

- During business hours, call the Local Public Health Epidemiologist/Disease Investigator who reported the public health surveillance trigger; provide specific information about the corresponding contamination warning system trigger and/or abnormal water quality test results identified.
- After business hours or on the weekend, call appropriate "after hours" contact and request a call back from Local Public Health agency that initially notified the utility of the public health surveillance trigger; provide specific information about the corresponding trigger and/or abnormal water quality test results identified to Local Public Health representative who returns the call.
- Inform Local Public Health of the utility's plans for further investigation, including estimated timeline.

15. Local Public Health continues investigation and assists with credibility determination.

- Continue to monitor relevant public health surveillance data streams until the source of the trigger is identified or the trigger is determined to be a false alarm.
- Assist with credibility determination in coordination with the Water Utility Emergency Response Manager.
- Document incident using *Checklist A-7: Public Health Surveillance Trigger Investigation*.
- Email a copy of *Checklist A-7: Public Health Surveillance Trigger Investigation* to the Water Utility Emergency Response Manager for the utility's records.

Table A-22. Example Timeline for Validation of a Public Health Surveillance Trigger in the Context of an Operational Contamination Warning System

Process Activity ID Number	Process Activity Description	Expected Response Time (minutes)	Range of Response Times (minutes)
1 & 5	Receive notification of public health surveillance trigger	15	1-60
2, 3 & 6	Investigate and validate public health surveillance trigger	60	15-120
8	Notify utility Water Quality Supervisor of public health surveillance trigger	10	5-60
9 & 10	Water Quality Supervisor investigates utility data and determines if there is a possible link to water	45	30-60
13 & 14	Notify the WUERM and Local Public Health agency of "possible" drinking water contamination threat	10	1-30
15	Initiate credibility determination as defined in a consequence management plan	10	1-30
	TOTAL ELAPSED TIME	**145**	**53-360**

Checklists

Four checklists, described in **Table A-23,** are used in the review of public health surveillance triggers based on this example. The checklists are included in Section A.7.

Table A-23. Example Checklists Used during Trigger Investigation for the Public Health Surveillance Component

Reference	Checklist	User	Description
Checklist A-1	Contamination Warning System Trigger Investigation	Water Quality Supervisor	Checklist involves review of records of other CWS triggers from previous 24 hours for suspected chemical contamination or previous 21 days for suspected biological contamination.
Checklist A-3	Distribution System Operations Review	SCADA Operator	Checklist involves the review of distribution system operating conditions from previous 24 hours for suspected chemical contamination or previous 21 days for suspected biological contamination.
Checklist A-4	Distribution System Work Order Review	Distribution Work Supervisor	Checklist involves the review of distribution system work orders from previous 24 hours for suspected chemical contamination or previous 21 days for suspected biological contamination.
Checklist A-7	Public Health Surveillance Trigger Investigation Checklist	Local public health agencies	Checklist involves the review of 911/EMS, National Retail Drug Monitor, and/or emergency room chief complaint data.

A.7: Examples of Contamination Warning System, Trigger Investigation Checklists

This section contains examples of checklists that can be used during contamination warning system trigger investigations, and are designed to facilitate implementation of the standard operating procedures presented in Section A.2 through A.6. Each checklist is designed for a particular user, and identifies specific activities that should be performed during investigation of a contamination warning system trigger. **Table A-24** provides a summary listing of the checklists, including a brief description, listing of the primary user, and indication regarding which monitoring and surveillance SOPs the checklists are designed to support.

Table A-24: Example Checklists Used during Investigation of Contamination Warning System Triggers

Reference	Checklist	Primary User	Description	Relevant CWS Components
Checklist A-1	Contamination Warning System Trigger Investigation	Water Quality Supervisor	Checklist involves the review of water quality data and plant operating conditions.	Water Quality Monitoring; Sampling and Analysis; Consumer Complaint Surveillance; Public Health Surveillance
Checklist A-2	Distribution System Site Investigation	Water Quality Field Technician	Checklist covers site investigation of a consumer complaint or a water quality monitoring station.	Water Quality Monitoring; Consumer Complaint Surveillance
Checklist A-3	Distribution System Operations Review	SCADA Operator	Checklist involves the review of distribution system operational data, such as tank levels and pump operations.	Water Quality Monitoring; Consumer Complaint Surveillance; Sampling and Analysis; Public Health Surveillance
Checklist A-4	Distribution System Work Order Review	Distribution Work Supervisor	Checklist involves the review of distribution system work.	Water Quality Monitoring; Sampling and Analysis; Enhanced Security Monitoring; Consumer Complaint Surveillance
Checklist A-5	Security Incident Investigation	Utility Security Personnel	Checklist covers activities during investigation of a security breach, including the site investigation.	Enhanced Security Monitoring
Checklist A-6	Water Quality Consumer Complaint Investigation	Water Quality Customer Service Representative	Checklist facilitates the collection of information from callers reporting unusual water quality concerns.	Consumer Complaint Surveillance
Checklist A-7	Public Health Surveillance Trigger Investigation	Local public health agencies	Checklist involves the review of the time, location, and data elements that characterize a public health trigger.	Public Health Surveillance

Checklist A-1: Contamination Warning System Trigger Investigation

Water Quality Supervisor or Alternate

Roles and Responsibilities

- Assume the lead in the investigation of a water quality trigger when notified by SCADA Operator.
- Assume the lead in the investigation of a consumer complaint surveillance trigger when a notification is received.
- Coordinate support from SCADA Operator and the Distribution Work Supervisor during investigation of a trigger.
- Review water quality data and related information during the investigation of a trigger.
- Review public health surveillance data during investigation of a trigger.
- Make the determination regarding whether or not a sampling and analysis trigger is valid, and decide whether to initiate additional analysis of sample(s).
- Make the determination regarding whether or not a water quality or consumer complaint surveillance trigger is a "possible" contamination threat.
- Notify the Water Utility Emergency Response Manager if the determination is made that contamination is "possible."

Information Systems used During a Trigger Investigation

- Water quality database.
- SCADA GUI.
- Water quality event detection system (EDS).
- Consumer complaint surveillance event detection system (EDS).
- Public health surveillance event detection system

Investigator Name	Investigator Role

Type of CWS Trigger

❑ Water Quality Monitoring	❑ Sampling and Analysis
❑ Consumer Complaint Surveillance	❑ Public Health Surveillance

Date of CWS Trigger	Time of CWS Trigger	Location of CWS Trigger	Sub-type of CWS Trigger (component specific)

Water Quality Trigger Investigation Checklist

Activity	Completed	Time
Begin Trigger Investigation: Record time.	❑	
Water Quality Trend Analysis: Analyze water quality trend lines from the monitoring location that detected the water quality anomaly.	❑	
Initiate Investigation: Following confirmation of the location and nature of the water quality anomaly, contact the SCADA Operator and Distribution Supervisor to initiate the EDS alarm investigation.	❑	
Historic Water Quality Data: Review historic water quality trends, such as seasonal or weekly patterns that are not accounted for by the EDS tool.	❑	
Historic Water Quality Anomalies: Review records of previously observed water quality anomalies. Consider patterns and causes of the previous anomalies.	❑	
Instrument Maintenance: Review the maintenance and calibration records for the water quality monitoring station that detected the anomaly.	❑	
EDS Tool Configuration: Check the attributes, configuration, and settings of the EDS tool that triggered the alarm.	❑	
Other Distribution System Locations: Analyze water quality trend lines from other water quality monitoring stations in the distribution system. Consider the travel time between monitoring stations when selecting time periods.	❑	

Finished Water Quality: Analyze water quality trend lines from water quality monitoring stations at the treatment plants. Consider the travel time between monitoring stations when selecting time periods.	❑	
Source Water Quality: Review online water quality monitoring data for source water or treatment plant process water.	❑	
Plant Operations: Check the recent treatment plant operating conditions.	❑	
Sampling and Analysis Trigger Investigation Checklist		
Activity	**Completed**	
Location: Confirm the location where the sample that produced the excursion was collected.	❑	
Data and Time: Confirm the date and time of the sample.	❑	
Compare sampling and analysis data to water quality results: Review sampling data and compare to water quality data for the sample time, including chlorine data and heterotrophic plate counts and/or coliform data if trigger based on pathogen analysis.	❑	
Treatment plant operating conditions: Review conditions for treatment plant, with assistance from the Treatment Plant Manager to interpret data.	❑	
Consumer Complaint Surveillance Trigger Investigation Checklist		
Activity		
Location: Plot customer complaint call and work orders on a GIS map to analyze for spatial clusters.	❑	
Initiate Investigation: Following confirmation of the location and nature of the customer complaints, contact the SCADA Operator and Distribution Supervisor to initiate the consumer complaint EDS alarm investigation.	❑	
Cluster Analysis: Analyze the nature of customer complaints to determine if there is a commonality in the reported aesthetics.	❑	
Water Quality Trend Analysis: Check trend lines in water quality parameters from water quality monitoring stations in the vicinity of complaints, if possible.	❑	
Finished Water Quality: Review recent finished water quality data for parameters that may be indicative of aesthetic water quality problems in the finished water.	❑	
Source Water Quality: Review recent source water quality data for parameters that may be indicative of aesthetic water quality problems in the finished water.	❑	
Plant Operations: Check for changes in treatment plant operating conditions that may have an impact on water quality aesthetics.	❑	
Public Health Surveillance Trigger Investigation Checklist		
Activity		
Suspected Pathogen Contamination: Check records from previous 21 days for other CWS triggers: water quality monitoring, enhanced security monitoring, sampling and analysis, or consumer complaint surveillance occurring within the zip codes(s) provided by the public health agency. Check pertinent test results that are not included in the other CWS triggers, such as coliform and/or HPC, for high values.	❑	

Suspected Chemical Contamination: Check records from previous 24 hours for other CWS triggers: water quality monitoring, enhanced security monitoring, sampling and analysis, or consumer complaint surveillance occurring within the zip codes(s) provided by local public health.	❑	
Suspected Contamination of Unknown Cause: Perform activities for both suspected pathogen contamination and suspected chemical contamination.	❑	
"Possible" Determination		
Activity	**Completed**	**Time**
Distribution System Operations: Evaluate information provided by SCADA Operator.	❑	
Distribution System Work: Evaluate information provided by Distribution Supervisor.	❑	
Consumer Call Classification: Evaluate information provided by Water Quality Customer Service Representative.	❑	
Local Public Health Information: Evaluate information provided by local public health.	❑	
Historical anomalies: Review log of previously observed water quality anomalies in an attempt to identify potential causes of the current trigger.	❑	
Is Contamination Possible?: When all reasonable explanations of the alarm have been assessed and ruled out, consider water contamination as "possible." Otherwise, reset the trigger and return to normal operations.	❑ YES ❑ NO	
WUERM Notification: If trigger cannot be explained by known, benign causes, notify the WUERM.	❑	
Investigation Closed: Record time.	❑	
Cause of CWS Trigger *Briefly summarize the results of the investigation and document the suspected cause of trigger, **regardless** of whether or not contamination was deemed "possible."*		

Checklist A-2: Distribution System Site Investigation

Water Quality Field Technicians			
Roles and Responsibilities			
• Inspect online water quality monitoring stations. • Lead the field investigation of a consumer complaint. • Perform field water quality analyses at the site of the water quality monitoring station or consumer complaint. • Collect samples from site of water quality monitoring station consumer complaint associated with a trigger.			
Investigator Name		**Investigator Role**	
Type of CWS Trigger			
❑ Water Quality Monitoring		❑ Consumer Complaint Surveillance	
Date of CWS Trigger	**Time of CWS Trigger**	**Location of CWS Trigger**	**Sub-type of CWS Trigger** (component specific)

Water Quality Monitoring Station Inspection Checklist		
Activity	**Completed**	**Time**
Location: Confirm the inspection location with the Water Quality Supervisor.	❑	
Notification: Notify the facility manager for inspections at non-utility locations.	❑	
Verify Power: Verify that all sensors on the monitoring station are powered.	❑	
Verify Pressure: Verify that pressure to the monitoring station is within specifications.	❑	
Verify Flow: Verify flow to all sensors on the monitoring station.	❑	
Check Reagents: Where possible, verify the supply and flow of reagents, and confirm that none are past expiration.	❑	
Check Carrier Gas Flow: Verify that the flow rate of a carrier gas is within acceptable range for the TOC instruments.	❑	
Review Calibration Records: Check the last known calibration date and determine if it was performed.	❑	
Field Verification of Sensor Reading: Compare monitoring station sensor readings to field test result for a grab sample from the water quality monitoring station sampling port **and/or** from a nearby fire hydrant.	❑	
Calibration Check: Perform a one-point calibration on the sensor that detected the water quality anomaly.	❑	
Sample Collection: If sample was remotely collected, remove sample vessel for transport to the water quality laboratory.	❑	
Sample Collection Vessel: Install a clean sample vessel with sodium thiosulfate below the sample tap at the monitoring station.	❑	
Reset Station: Reset the remote sampling device as well as all local alarms.	❑	

Do the field inspection results confirm online water quality readings?	❑ YES ❑ NO	
Reporting: Report results of the monitoring station investigation to the Water Quality Supervisor from the field.	❑	

Consumer Complaint Site Investigation Checklist		
Activity	**Completed**	**Time**
Location: Confirm the location of the investigation with the Water Quality Customer Service Representative.	❑	
Notification: Notify the customer when en route to the site.	❑	
Interview: Discuss the water quality issue with the customer. Verify all taps on the premise where the water quality issue was observed.	❑	
Site Inspection: Investigate the premise for signs of recent work on the plumbing system, as well as possible sources of contamination based on the characteristics of the water quality issue.	❑	
Sample Collection - Premise: Collect samples from taps on the premise where the water quality issue was observed. Perform field tests for basic water quality parameters.	❑	
Sample Collection - Hydrants: Collect samples from hydrants upstream and downstream from the premise. Perform field tests for basic water quality parameters.	❑	
Reporting: Report results of the monitoring station investigation to the Water Quality Supervisor or Distribution Work Supervisor from the field.	❑	

Summary Findings of Site Inspection

Checklist A-3: Distribution System Operations Review

SCADA Operator			
Roles and Responsibilities			
• Monitor all control room alarms, including water quality and physical security alarms, 24/7. • Notify Water Quality Supervisor in the event of a water quality trigger. • Notify Utility Security personnel in the event of a physical security trigger. • Review distribution system operations data to support the investigation of a CWS trigger.			
Information Systems used During a Trigger Investigation			
• SCADA GUI.			
Investigator Name		**Investigator Role**	
Type of CWS Trigger			
❑ Water Quality Monitoring	❑ Enhanced Security Monitoring	❑ Sampling and Analysis	
❑ Consumer Complaint Surveillance	❑ Public Health Surveillance		
Date of CWS Trigger	**Time of CWS Trigger**	**Location of CWS Trigger**	**Sub-type of CWS Trigger** (component specific)
Activity		**Completed**	**Time**
Notification: Notify Water Quality Supervisor in the event of a water quality trigger or Utility Security personnel in the event of an enhanced security trigger.		❑	
SCADA Alarms: Review SCADA alarms that may be related to the CWS trigger, such as water quality alarms, intrusion alarms, loss of power, and loss of communications.		❑	
System Operations: Review the impact of tank, reservoir, and pump operation on water quality in the vicinity of the CWS trigger.		❑	
System Flows: Consider unusual flow conditions, such as fire flows, that may have impacted water quality in the vicinity of the CWS trigger.		❑	
System Pressures: Consider unusual pressure conditions, such as surges or low pressure events, that may have impacted water quality in the vicinity of the CWS trigger.		❑	
Reporting: Report results of the CWS trigger investigation to Water Quality Supervisor or Utility Security personnel as appropriate.		❑	
Summary Findings of Investigation			

Checklist A-4: Distribution System Work Order Review

Distribution Work Supervisor			
Roles and Responsibilities			
• Review distribution system work orders to support the investigation of a CWS trigger. • Monitor for consumer complaint surveillance triggers during non-business hours.			
Information Systems used During a Trigger Investigation			
• Work Order System.			
Investigator Name		**Investigator Role**	
Type of CWS Trigger			
❑ Water Quality Monitoring	❑ Enhanced Security Monitoring	❑ Sampling and Analysis	
❑ Consumer Complaint Surveillance	❑ Public Health Surveillance		
Date of CWS Trigger	**Time of CWS Trigger**	**Location of CWS Trigger**	**Sub-type of CWS Trigger** (component specific)

Activity	Completed	Time
Active Work: Identify any current work in the distribution system involving utility personnel or contractors that could be related to the CWS trigger.	❑	
Main Breaks: Identify any main breaks in the vicinity of the CWS trigger, and investigate the potential relationship between the break and the CWS trigger.	❑	
Flushing Operations: Identify any flushing operations in the vicinity of the CWS trigger, and investigate the potential relationship to the CWS trigger.	❑	
Water Outages: Identify any water outages or recent valve operations in the vicinity of the CWS trigger, and investigate the potential relationship to the CWS trigger.	❑	
System Maintenance: Review system maintenance activities, such as tank cleaning, and investigate the potential relationship to the CWS trigger.	❑	
Power Outages: Identify any power outages affecting system operations, and investigate the potential relationship to the CWS trigger.	❑	
Reporting: Report results of the CWS trigger investigation to Water Quality Supervisor or Utility Security personnel as appropriate.	❑	

Summary Findings of Investigation

Checklist A-5: Security Incident Investigation

Utility Security Personnel

Roles and Responsibilities

- Lead the investigation of all enhanced security triggers, including: intrusions, tampering incidents, witness accounts, and threats.
- Assess the legitimacy of witness accounts of possible intrusion through interviews.
- Notify local law enforcement if intrusion at a facility is suspected or a written or verbal threat is received.
- Lead the on-site investigation of a security incident, with assistance from Distribution System Field Crews and local law enforcement as necessary.
- If an intrusion is confirmed, determine whether or not the intruder could have accessed the water supply.

Information Systems used During a Trigger Investigation

- SCADA GUI (to view video clips).

Investigator Name	Investigator Role

Date of Security Trigger	Time of Security Trigger	Location of Enhanced Security Trigger

Type of Enhanced Security Trigger

❑ Verbal/Written threat	❑ Security alarm with cameras	❑ Security alarm w/o cameras	❑ Witness Account

Verbal/Written Threat Review Checklist

Activity	Completed	Time
Document Threats Received by Phone: Record date, time, name, incoming phone number, caller characteristics, background noises, type of possible malice, reason, etc.	❑	
Document Written Threats: Record date, time, name, mode of receipt (US mail, fax, email, FedEx, etc.), return address/fax number, type of possible malice, reason, etc.	❑	
Notification: Notify local law enforcement.	❑	

Camera Video Clip Review Checklist

Activity	Completed	Time
Video Review Clip For:		
• Visual confirmation of intruder at site.	❑	
• Signs of forced entry, such as cut fences, cut locks, damaged doors, etc.	❑	
• Signs of tampering, such as damaged utility equipment.	❑	
• Presence of non-utility equipment, such as tanks, drums, etc.	❑	
Notification: Unless video review confirms legitimate utility activity was the cause of the alarm, notify local law enforcement.	❑	

Witness Account

Activity	Completed	Time
Receive witness account: If witness reports account directly to the utility, Utility Security Personnel should collect incident information from the witness. If witness reports directly to law enforcement, Utility Security Personnel should support the investigation.	❑	

Is witness employed by the utility? If "yes", then account is considered a reliable threat warning.	❑ YES ❑ NO	
Document witness information: Include date/time of interview, name, full contact information, and why the witness was in the vicinity of suspicious activity.	❑	
Document location: Verify location and type of facility where suspicious activity was witnessed.	❑	
Document type of suspicious activity: Determine whether activity was trespassing, vandalism, theft, tampering, surveillance, breaking and entering, or other suspicious activity.	❑	
Document a description of the suspects: Include how many suspects were present, sex, race, hair coloring, clothing, voice, or other unusual characteristics.	❑	
Document a description of any vehicles at the site: Include make, model, color, license plate, or other unusual characteristics.	❑	
Document a description of any unusual equipment at the site: Equipment could include explosives, firearms, tools, containers, hardware, pumps, PPE, lab equipment, or other equipment.	❑	
Document a description of any unusual conditions at the site: Conditions could include explosions or fires, dead/stressed vegetation, fogs or vapors, dead animals, unusual odors, or unusual noises.	❑	
Consider reliability of the source: If witness is not employed by the utility, have they filed false reports in the past? If "yes", then source is considered suspect.	❑ YES ❑ NO	
Site Investigation (including investigation of alarms from sites w/o cameras)		
Activity	**Completed**	**Time**
Confirm location of possible security breach: Determine facility type, such as source water, tank, treatment plant, distribution, water main, etc.	❑	
Check for unusual equipment: Such as discarded PPE (e.g., gloves, masks) tools, hardware, lab equipment, empty containers, etc.	❑	
Check for unusual vehicles on the site: Such as non-utility trucks, cars, SUVs, construction vehicle, etc.	❑	
Check for signs of tampering: Such as cut locks, open access hatches, damaged gates/windows/doors, missing or damaged equipment, facility in disarray, etc.	❑	
Check for signs of hazards: Such as unexplained or unusual odors, dead or distressed vegetation, unexplained clouds or vapors, dead animals, unexplained liquids, etc.	❑	
Check for any sign of security breach: Check all points of access for the facility.	❑	
"Possible" Determination		
Activity	**Completed**	**Time**
Is Contamination Possible?: If the possibility of an intruder gaining access to the water supply cannot be ruled out, then contamination is "possible."	❑ YES ❑ NO	
WUERM Notification: If contamination is considered "possible", notify the WUERM. If not, continue investigation of intrusion with local law enforcement.	❑	

Investigation Closed. Return to normal operations.	❑	

Cause of the Enhanced Security Trigger

*Briefly summarize the results of the investigation and document the suspected cause of trigger, **regardless** of whether or not contamination was deemed "possible."*

Checklist A-6: Water Quality Consumer Complaint Investigation

Water Quality Customer Service Representative

Roles and Responsibilities

- Monitor for consumer complaint surveillance triggers during normal business hours.
- Interview customers who contact the utility with questions or concerns regarding water quality issues.
- Decide whether or not to create a work order to respond to a water quality concern raised by a customer.

Information Systems used During a Trigger Investigation

- Water Quality Database.
- Work Order System.

Investigator Name	Investigator Role

Date of Call	Time of Call	Location of Customer Calls

Consumer Complaint Investigation Checklist

Activity	Completed	Time
Address: Confirm the address where the customer observed the water quality issue.	❑	
Date & Time: Confirm the date and time when the customer first noticed the issue and how long it persisted.	❑	
Location: Confirm the specific location within the premise where the customer observed the water quality issue (e.g. bathroom, kitchen, etc.).	❑	
Water Quality Issue: Ask the caller to describe the nature of the water quality issue in as much detail as possible. Record characteristics below.	❑	
Possible Causes: Ask the caller about possible causes of the issue, such as recent work on the plumbing system at the premise.	❑	
Recent Calls: Review work orders and call logs to determine if other water quality calls of a similar nature or in the same vicinity occurred recently.	❑	
Field Investigation: Does the nature of the water quality issue described by the customer necessitate a field inspection?	❑ YES ❑ NO	
Water Quality Work Order: If "yes" to previous question, create water quality work order to initiate field investigation.	❑	
Notifications: Notify the Water Utility Emergency Response Manager if the results of the field investigation indicate "possible" contamination.	❑	

Description of Water Quality Issue

❑ Odor	❑ Taste	❑ Appearance	❑ Tactile	❑ Illness
❑ Musty	❑ Bitter	❑ Cloudy	❑ Oily	❑ Nausea
❑ Chlorine	❑ Sweet	❑ Rusty/red	❑ Soapy	❑ Diarrhea
❑ Sulfur/septic	❑ Metallic	❑ Particulate	❑ Abrasive	❑ Rash

Additional Description:

Summary Findings of Investigation

Checklist A-7: Public Health Surveillance Trigger Investigation

Local Public Health Agencies			
Roles and Responsibilities			
• Review time, location, and data trends of triggers from public health data streams.			
Information Systems Unique to Public Health Surveillance Trigger Investigation			
• Public health surveillance event detection system • Real-time Outbreak Disease Surveillance System (RODS) • National Retail Data Monitor (NRDM) • Poison Control Center			
Investigator Name		**Investigator Role**	
Date of Public Health Trigger	**Time of Public Health Trigger**	**Location of Public Health Surveillance Trigger**	
Type of Public Health Surveillance Trigger			
❑ EMS	❑ RODS	❑ Poison Control Center	
❑ 911	❑ NRDM	❑ Infectious Disease	

Activity	Completed	Time or Result
Verify location: Is the location of the trigger within the jurisdiction?	❑ YES ❑ NO	
Verify location: Does 911/EMS call data occur in a "cluster"?	❑ YES ❑ NO	
Verify data completeness: Ensure the underlying data are properly coded and complete.	❑	
Determine initial cause of trigger: 911/EMS: What chief complaint or syndrome has increased? RODS (ER Chief Complaints): What chief complaint has increased? NRDM: What over-the-counter medicine is being sold at a higher rate? Poison Control Center: What sort of symptoms and call types have increased? Infectious Disease Reports: What disease incidence has increased?	❑	
Check other Public Health data streams: Do they show similar trends that support initial trigger?	❑ YES ❑ NO	
Determine if Public Health Surveillance trigger could be related to drinking water: Do symptoms or other patterns presented relate to illnesses and conditions caused by pathogen or chemical water contamination? Determine whether symptoms are more likely due to pathogen or chemical contamination.	❑ YES ❑ NO	
Notify Water Quality Supervisor: Public health agency notifies the utility Water Quality Supervisor that public health trigger is suspected to be related to water, and provides available information, such as location or possible causative agents.	❑	
Assist in investigation: Continue to monitor relevant public health data until source of trigger is identified and log alarm.	❑	

Email checklist: Email copy of the "Public Health Surveillance Trigger Investigation Checklist" to Water Quality Supervisor for the utility's records.	❑	

Summary Findings of Investigation