United States
Environmental Protection
Agency

Summary of Implementation Approaches and Lessons Learned from the Water Security Initiative Contamination Warning System Pilots

Office of Water (MC 140) EPA 817-R-15-002 October 2015

Disclaimer

The Water Security Division of the Office of Ground Water and Drinking Water has reviewed and approved this document for publication. This document does not impose legally binding requirements on any party. The information in this document is intended solely to recommend or suggest and does not imply any requirements. Neither the U.S. Government nor any of its employees, contractors or their employees make any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use of any information, product or process discussed in this document, or represents that its use by such party would not infringe on privately owned rights. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

Questions concerning this document should be addressed to WQ_SRS@epa.gov or one of the following contacts from EPA's Water Security Division:

Steve Allgeier, Project Management and Public Health Surveillance
Allgeier.Steve@epa.gov, (513) 569-7131

Jeffery Fencil, Consequence Management
Fencil.Jeffrey@epa.gov, (202) 564-0818

Elizabeth Hedrick, Sampling and Analysis
Hedrick.Elizabeth@epa.gov, (513) 569-7296

Nelson Mix, Customer Complaint Surveillance and Enhanced Security Monitoring
Mix.Nelson@epa.gov, (202) 564-7951

Katie Umberg, System Engineering
Umberg.Katie@epa.gov, (513) 569-7925

Matt Umberg, Online Water Quality Monitoring
Umberg.Matt@epa.gov, (513) 569-7357

Acknowledgements

The EPA Water Security Division would like to recognize the following individuals and organizations for their assistance, contributions and review during the development of this document.

Greater Cincinnati Water Works
Yeongho Lee
Jeff Swertfeger

New York City Department of Environmental Protection
Jim Alair
David Lipsky

Philadelphia Water
Geoffrey Brock
Gary Burlingame
Joanne Dahme
Jim Golembeski
Rita Kopansky
John Muldowney
Ralph Rogers
Charles Zitomer
Philadelphia Department of Public Health

San Francisco Public Utilities Commission
Manouchehr Boozarpour
Andrew DeGraca
Sheila Garrett
Brandon Grissom
Rod Miller
June Weintraub

Table of Contents

List of Figures

List of Tables

Abbreviations

AET	Alarm Estimation Tool
CCS	Customer Complaint Surveillance
CIPAC	Critical Infrastructure Protection Advisory Council
CM	Consequence Management
CMP	Consequence Management Plan
CSR	Customer Service Representative
CWS	Contamination Warning System
ED	Emergency Department
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EPA	United States Environmental Protection Agency
ESM	Enhanced Security Monitoring
GIS	Geographic Information System
HIPAA	Health Insurance Portability and Accountability Act
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Incident Command System
IP	Internet Protocol
IT	Information Technology
LIMS	Laboratory Information Management Systems
ORP	Oxidation Reduction Potential
OTC	Over-the-counter
OWQM	Online Water Quality Monitoring
PCC	Poison Control Center
PHS	Public Health Surveillance
QA/QC	Quality Assurance and Quality Control
RCP	Risk Communication Plan
S&A	Sampling and Analysis
SCADA	Supervisory Control and Data Acquisition
SOP	Standard Operating Procedure
SRS	Water Quality Surveillance and Response System
TEVA-SPOT	Threat Ensemble Vulnerability Assessment and Sensor Placement Optimization Tool
TOC	Total Organic Carbon
UV	Ultraviolet
VOC	Volatile Organic Compound
WGCC	Water Government Coordinating Council
WSCC	Water Sector Coordinating Council
WSI	Water Security Initiative

Section 1: Introduction

The purpose of the U.S. Environmental Protection Agency's (EPA) Water Security Initiative (WSI) was to design and demonstrate a sustainable ***Contamination Warning System*** (CWS) capable of providing timely detection of and response to drinking water contamination incidents in the water distribution system. As shown in **Figure 1-1**, a CWS integrates ***information*** from multiple monitoring and surveillance ***components*** to detect unusual water quality conditions and investigate the possibility of distribution system contamination. A CWS also includes a response framework that supports timely and effective actions to reduce the consequences of a contamination incident.

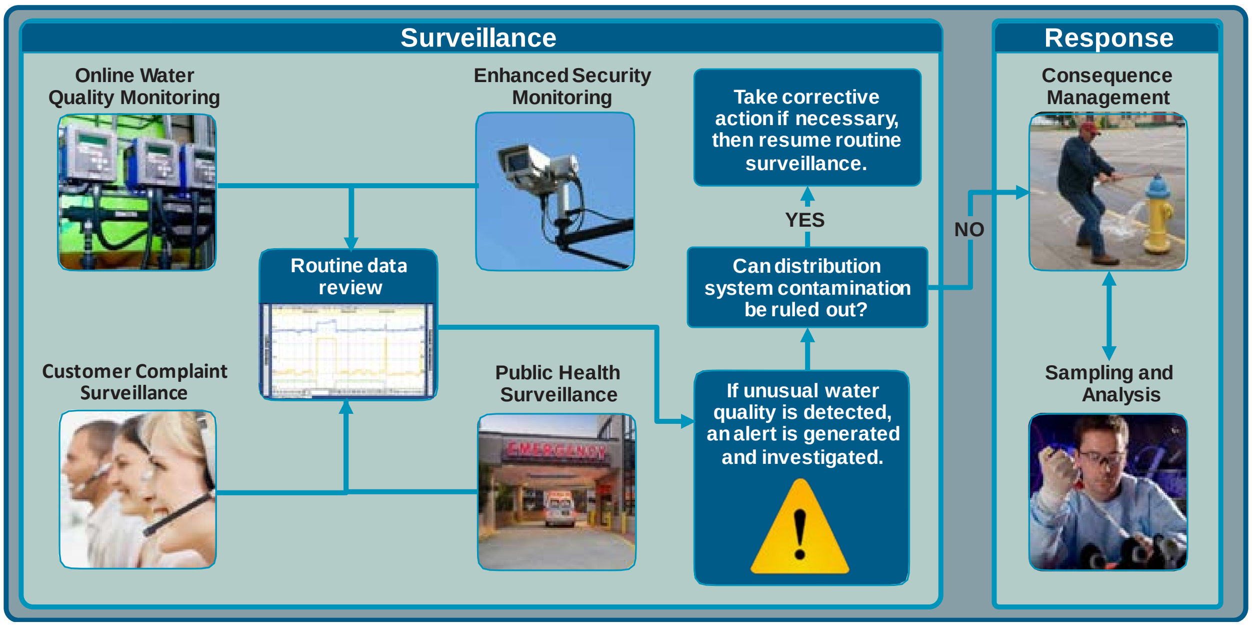

Figure 1-1. CWS Architecture

The CWS architecture shown in Figure 1-1 consists of four surveillance and two response components:

<u>Surveillance</u>

- ***Online Water Quality Monitoring*** (OWQM): Water quality parameters are monitored in real time at strategic locations in the distribution system to identify unusual water quality values or trends.
- ***Enhanced Security Monitoring*** (ESM): Distribution system facilities with a high risk of contamination are monitored using intrusion detection systems.
- ***Customer Complaint Surveillance*** (CCS): Customer contacts are monitored to identify unusual trends in water quality complaints.
- ***Public Health Surveillance*** (PHS): Public health data is analyzed in order to identify disease clusters that might be caused by contaminated drinking water.

<u>Response</u>

- ***Consequence Management*** (CM): Procedures and partner networks are developed for responding to possible drinking water contamination incidents.
- ***Sampling and Analysis*** (S&A): Water samples from a distribution system are collected and analyzed in response to possible drinking water contamination incidents.

To evaluate this CWS model, EPA partnered with the five water utilities listed in **Table 1-1** to implement full-scale CWS ***pilots***. While all five utilities are similar in that they serve large populations, they are diverse with respect to source water and treatment types, organization structure, partnerships with local and state entities, and utility goals for the CWS pilot. EPA provided direct financial and technical support to implement the pilots, with awards ranging from $8.3 million to $12 million. Additionally, the pilots made in-kind contributions to the project at a value of at least twenty percent of the award amount.

Table 1-1. Attributes of Utilities Participating in the CWS Pilot Program

Utility[1]	Population Served	Source Water Type	Residual Disinfectant	Treatment Type
Dallas Water Utilities	2.4 million	6 Surface Water Reservoirs	Chloramines	Conventional Filtration
Greater Cincinnati Water Works	1.1 million	River and Groundwater	Free Chlorine	Conventional Filtration with GAC
New York City Department of Environmental Protection	9.0 million	3 Surface Water Supply Systems	Free Chlorine	Unfiltered Surface Water
Philadelphia Water Department	1.7 million	2 River Sources	Chloramines	Conventional Filtration
San Francisco Public Utilities Commission	2.6 million	5 Surface Water Reservoirs	Chloramines	Unfiltered Surface Water with UV, Conventional Filtration, and Direct Filtration with Ozone

[1] These are the utility attributes during implementation of the CWS pilots

The first pilot was initiated in 2006 with the Greater Cincinnati Water Works through a grant vehicle known as a Cooperative Research and Development Agreement. EPA was actively involved in the design and implementation of this first full-scale CWS. The remaining four pilots were awarded Cooperative Agreement Grants through a competitive process in 2008 and received funding to implement their CWS pilots with technical consultation provided by EPA upon request. The original goal was to complete CWS implementation at each utility in two years; however, it took most pilots three to four years to achieve full operation.

The pilots were required to implement all six components depicted in Figure 1-1, although each pilot had a great deal of latitude in how they designed each component. They used this flexibility to experiment with novel approaches and technologies, some of which were successful while others were not. Ultimately, each pilot settled on a CWS design that they could sustain beyond the formal implementation and evaluation period of the pilot.

Each of the pilots also performed a post-implementation technical evaluation of their CWS with respect to the following performance objectives:

- Detect a broad spectrum of potential contaminants that could cause harm to the public or a disruption in service
- Provide spatial coverage of the entire distribution system
- Detect contamination incidents in sufficient time for implementation of response actions that could reduce public health and economic consequences
- Reliably detect contamination incidents with a minimum number of ***invalid alerts***
- Maintain a high degree of operational reliability with limited downtime of key assets
- Provide a sustainable architecture to monitor the distribution system for general water quality objectives as well as possible contamination incidents

Several evaluation techniques were employed by the pilots. The empirical data generated through the surveillance components was analyzed to characterize metrics such as data accuracy and completeness, percent of time the system was available, and frequency of invalid alerts. Drills and exercises were conducted to assess timeliness of investigative and response actions. Workshops and interviews were used to gather utility perspectives regarding the benefits derived from the CWS. Collectively these techniques were used to evaluate the degree to which the CWSs deployed were effective, implementable, and sustainable. The results of each pilot evaluation were summarized in a report submitted to EPA.

The purpose of this report is to summarize key findings from these pilot evaluations in a manner that is useful and relevant to the drinking water sector. Specifically, this document provides a concise overview of implementation approaches and lessons learned from the CWS pilots that are potentially useful to future CWS implementers. An overview of the remaining sections of the report follows:

- **Section 2.0** describes the role of project management during implementation of the pilots.
- **Section 3.0** describes the application of system engineering principles to the design of the pilots.
- **Sections 4.0 through 9.0** describe the implementation approaches and lessons learned for each of the six CWS components shown in Figure 1-1.
- **Section 10.0** provides an overarching discussion of CWS sustainability and broadly applicable lessons learned from the pilots.
- **Section 11.0** concludes the report with a discussion of the feasibility and benefit of CWS implementation.
- **Section 12.0** provides a list of reports, papers, conference proceedings, and other materials from the pilots that are in the public domain.
- **References** presents a comprehensive list of documents cited in this document.
- **Glossary** presents definitions of terms used in this document, which are indicated by bold italic font at first use in the body of the document.

This report is not intended to provide guidance for CWS implementation. The knowledge gained from these pilots was used to develop guidance and tools that are available from the *Water Quality Surveillance and Response Website* (EPA, 2015).

Consideration should be given to the following factors when reviewing and interpreting the information presented in this report. First, the pilots received large grants from EPA, which likely influenced the scope and design of their CWS. This funding also enabled the utilities to pursue research activities during the pilot, providing an opportunity to implement and evaluate novel technologies that might not otherwise have been considered. Furthermore, the CWS pilot program spurred vendor innovation resulting in new products and tools that were not available when the pilots were implemented. Finally, the CWS pilots were designed for the purpose of detecting and responding to distribution system contamination incidents. While contaminant detection and response is an important application of a CWS, a more sustainable approach to design considers the operational benefits of enhanced distribution system surveillance and response (see the callout box below).

WATER QUALITY SURVEILLANCE AND RESPONSE SYSTEMS

Evaluation of the CWS pilots demonstrated that real-time data generated by a CWS can provide tremendous value to routine distribution system monitoring and management. Furthermore, feedback from stakeholders clearly indicates that sustainability of a CWS depends on the value provided to routine operations (WSCC/WGCC, 2012). For these reasons, the concept of a CWS has evolved into a ***Water Quality Surveillance and Response Systems*** (SRS). An SRS utilizes the same components as a CWS, but is designed to maximize benefits to routine operations. This includes early detection and management of water quality issues such as low residual chlorine levels, nitrification, rusty water, and taste and odor episodes. EPA guidance and products are now presented under the SRS paradigm.

Section 2: Project Management

Project management encompasses the activities and framework required for overall CWS planning, organization, coordination, and management. It was an important aspect of all five pilots and required significant time and effort.

2.1 Summary of Implementation Approaches

All five pilots established a project management team prior to initiation of CWS design and implementation. The pilots also formed a team for each CWS component. Each component team consisted of a component lead, as well as other key personnel responsible for design, implementation, and operation of that component. Components that rely on external partners, such as PHS and CM, included representatives from the relevant partner organizations. All pilots also used consultants to provide technical expertise and additional support during CWS implementation.

The project management team for each pilot was responsible for overseeing all CWS project activities. In addition to senior utility managers, the project management team comprised each of the CWS component leads as well as representatives from utility divisions including operations, engineering, water quality, security, and information technology (IT). The responsibilities of the project management team included:

- Establishing design goals and performance objectives for the CWS
- Communicating these goals and objectives to utility managers, utility personnel, and external partners involved in the project
- Defining constraints for the system and its components based on budget, schedule, and policies
- Developing a master plan for the CWS implementation
- Establishing priorities for the CWS and allocating resources across components
- Approving component workplans and ensuring system integration
- Tracking the overall budget and schedule
- Evaluating the effectiveness of the system

2.2 Summary of Lessons Learned

Support from senior management is critical. All pilots noted that the success of the CWS depended significantly on buy-in from utility senior management. By demonstrating commitment to the project, senior managers showed that the project was a priority for the utility. Their support also promoted the interdivisional collaboration necessary to successfully implement the CWS.

Knowledgeable component leads are important. The pilots emphasized the importance of the component leads in making the project a success and ensuring effective and sustainable component designs. The most successful component leads had project management skills as well as subject-matter expertise in the area they managed.

Engage all stakeholders from the beginning. The pilots noted the importance of engaging all departments and individuals responsible for design, implementation, and maintenance of the information management system, as well as end users of the system. For example, one pilot did not engage IT personnel

LESSON LEARNED HIGHLIGHT

When launching a new project that places an additional workload on personnel, it is important to demonstrate how the project benefits day-to-day operations and utility goals. At one utility, this was achieved by demonstrating data analysis and display tools to utility personnel to help them see how the information collected by the CWS could enhance their core job functions.

initially and spent significant resources designing the information management system, only to find out that their design conflicted with IT requirements.

Consistent project communication is necessary to ensure that project goals are met. Regular meetings, both within component teams and with the project management team, kept all team members informed of project status and ensured that project activities were completed as expected. These meetings also helped track the timeline and budget. At the beginning of the project, several utilities held meetings as frequently as every week. After the project direction was clearly set, meetings continued but at a reduced frequency.

LESSON LEARNED HIGHLIGHT

The method of procuring equipment can have a significant impact on costs and schedule. One utility sent bid packages to preapproved vendors under a statewide contract for security equipment. This led to a shorter bidding process by avoiding the lengthy public advertisement and bidding stages.

Two other pilots experienced difficulties during the procurement process, and the project scope was reduced to meet the cost estimates and scheduled completion dates. One of these pilots noted that traditional governmental purchasing programs can cause delays if sole-source or non-U.S. vendors are being solicited. Using preapproved vendors through a statewide contractor resulted in a time and cost saving procurement, yielding more equipment on a fixed budget.

Section 3: System Engineering

In all five pilots, system engineering principles were applied to ensure that the CWS functioned as an integrated system rather than a collection of independent surveillance and response components. While system engineering principles permeate the design and implementation process, the four ***design elements*** listed in **Table 3-1** were particularly dependent upon effective system engineering.

Table 3-1. System Engineering Design Elements

Design Element	Description
Data Communications	Component data is transmitted to a central location.
Information Management	Data and information are stored and made available to utility personnel.
Alert Investigation Procedures	Procedures to guide the systematic and efficient investigation of alerts are developed and implemented.
Training and Exercises	Personnel are trained on their roles and responsibilities, and procedures are tested, evaluated, and refined through drills and exercises.

3.1 Data Communications

The data communications design element covers the solution(s) implemented to transmit the data generated by a CWS component to an ***information management*** system (discussed in Section 3.2). This section covers the general types of data communications solutions implemented by the pilots to transmit data from remote to centralized locations for OWQM, ESM, and PHS. CCS, S&A, and CM are not discussed here because, in most cases, the data generated by those components was entered directly into utility information management system(s) and did not require transfer from external sources.

3.1.1 Summary of Implementation Approaches

The pilots used different transmission methods depending on how the data was to be used. For example, if data was to be analyzed in real time, it needed to be transmitted in real time. The methods used fell into the following three general categories.

- *Automatic transfer*: Data was transmitted to the data management system (generally initiated by a query from the system) at a user-defined polling interval (e.g., every 10 minutes). All the pilots used automatic transfer for OWQM, and some also used it for PHS ***datastreams***, although at a lower frequency (e.g., once per day).
- *Event-based transfer*: Data without a defined generation frequency was transmitted to the data management system as it was created. This was most commonly used for transmitting component ***alerts*** and alerts or faults generated by online equipment (e.g., OWQM sensor hardware and ESM door contact switches).
- *On-demand transfer*: Data was transferred only if requested by utility personnel. All pilots used on-demand transfer for ESM video data (in addition to event-based transfer), as the volume of data produced made it infeasible to regularly transmit this data.

IMPLEMENTATION HIGHLIGHT

For data that was automatically transferred, all pilots configured their communications system to automatically collect missing data in the case of a communication failure. In the case of long failures, the systems were configured to query the data in subsets (e.g., 12-hour sets) to avoid overwhelming the network with large requests.

In addition to identifying transmission methods for each datastream, the pilots had to select specific communications solutions, such as the technology and architecture used to transmit data. The following considerations impacted the selection of communications solutions:

- *Availability of viable communications solutions at monitoring locations*: For OWQM and ESM, data had to be transmitted from equipment installed at locations in the distribution system, and potential communications solutions varied by location. Many of these locations had existing communications infrastructure that could be leveraged, such as internet connections or existing hard-wiring at utility facilities. At non-utility facilities, communications system service providers, such as cellular service, were often used. However, in some cases, cellular communication could not be used due to insufficient signal.
- *Volume of data produced and transmitted*: Contact switches used in ESM and most sensors used for OWQM produced modest volumes of data that could easily be handled by any communications solution. However, ESM video equipment and OWQM spectral instruments, which generated 256 data points at each timestep, produced much larger quantities of data. Often, existing communications systems were incapable of handling these large amounts of data, and high bandwidth solutions were required to transmit the data at an acceptable speed.
- *Need for bidirectional communications*: Some pilots had a need for bidirectional communications for some components, in which information or queries can be sent back to equipment in addition to collecting data. For example, some OWQM and ESM equipment allow users to remotely access the instrument interfaces for remote diagnostics or configuration.
- *Cybersecurity requirements*: The pilots prioritized cybersecurity to varying degrees, and these requirements impacted the selection of communications solutions. For example, some were concerned about the vulnerability of internet-based solutions to cyber-attacks and thus pursued non-internet-based solutions.

Table 3-2 summarizes the communications methods used by the pilots. All pilots used more than one method of data communications. Four of the five pilots used more than one method within a single component (OWQM and ESM) based on the location from which data needed to be transmitted.

Table 3-2. Communications Methods Implemented by the Pilots

Communications Method	OWQM	ESM	PHS
Digital cellular network[1]	4	2	0
Internet lines (DSL, fiber-optic, T1, TLS)	2	4	3
Utility-controlled lines (intranet)	3	1	0
Private radio	1	2	0
Plain old telephone service	1[2]	0	2

[1] One pilot was able to use the city's secure wireless network, which was distinct from the public cellular network
[2] This was used as a backup method at select utility facilities

Communications methods varied across components. In particular, methods selected for PHS were different from those used in the other components. This was because PHS generated a lower volume of data compared to OWQM and ESM, and data was transferred from an outside entity. Note that in addition to ensuring that the communications method met their requirements, the pilots also had to ensure that they secured enough bandwidth with their selected solution to meet their communications needs.

3.1.2 Summary of Lessons Learned

Reliability varies by communications solution. The pilots found that cellular solutions were most susceptible to communication outages and dropped data during the pilot period. Thus, two pilots switched some locations from wireless to wired solutions during the pilot period, although 3G, 4G, and 4G LTE technologies are believed to have improved cellular data transmission since pilot implementation.

Contract terms from communications vendors can change unexpectedly. The pilots experienced challenges with the service contracts from cellular companies. Two of the pilots chose to switch to wired solutions after experiencing a significant increase in monthly fees after the initial contract period ended. Another had to switch to a wired solution when their original provider terminated their wireless service. In general, utility-owned networks were the preferred solution, although were generally only available at utility-owned facilities.

Data identifiers must be synchronized. The largest cause of communications failure was inconsistency in data identifiers between monitoring locations and information management systems. Whenever a source name, location, or data format changes, it must be reflected in every phase of the communications process. If this is not done, the data fields that are inconsistently identified in different elements of the communications system will not be transferred.

Lack of industry standards can present challenges. The lack of industry standards for connectivity between technologies created challenges for implementing communications solutions using equipment from different vendors. Close collaboration with the vendors and service providers was necessary to achieve connectivity.

3.2 Information Management

A utility's information management system includes the hardware and software required to manage CWS data and make it available in a usable format. This includes data management system(s) for receiving and storing the data generated through the CWS components, as well as the tools and interfaces that allow users to access and interact with this data.

3.2.1 Summary of Implementation Approaches

The following considerations impacted the information management solutions selected by the pilots.

- *Existing information management capabilities*: When selecting an information management solution, all pilots considered whether existing systems, such as data historians, call and work management systems, video management systems, and geographic information systems (GIS) could meet system requirements. While leveraging existing resources reduced project costs and training requirements, the pilots considered the potential impact on the existing systems, such as increased cybersecurity vulnerabilities or reduced resources for existing processes, before making a final decision.
- *Attributes of source data systems*: CWS component data came from a variety of sources including sensors, other data management systems within the utility, and sources outside the utility. This consideration was particularly relevant to PHS, as alerts were generally transmitted to the utility from a public health department's data management system.
- *User requirements*: A preliminary step in the selection and design process was to engage a representative group of end users to identify their expected uses and requirements for the information management system. To inform this process, the pilots reviewed alert investigation procedures to identify actions that would need to be executed using the system.

The following points provide a high-level summary of the information management systems implemented by the pilots.

- Four of the five pilots developed a CWS ***dashboard***, where information and alerts from multiple components were available through a single user interface.
- Two of the pilots made the user interfaces available over the internet. For the remaining utilities, the systems were accessible only on workstations connected to a utility network.
- None of the pilots developed a single database to store and manage all CWS data. Each used a different data management solution for each component (multiple data management systems were used for some components). Several of the pilots upgraded at least one component-specific data management system as part of this project. Some had upgrades planned before the project started, and some chose to upgrade a system to better support the CWS.
- None of the pilots used their existing supervisory control and data acquisition (SCADA) system as their CWS information management system. The four pilots that developed a dashboard chose solutions specifically designed to accommodate complex user interfaces. The remaining pilot implemented a parallel SCADA system due to concern that their primary SCADA integration of the CWS requirements could introduce vulnerabilities.
- Three of the pilots exclusively used local data storage in which all hardware and software associated with CWS information management was stored and managed internally. Two utilities used a solution in which some of the data was stored and managed off-site by a contractor or vendor.

IMPLEMENTATION HIGHLIGHT

Video data had unique data management challenges because of the volume of data generated. For all pilots, a storage device was installed at each monitoring location to record video from on-site cameras, and data was only transmitted when triggered by an intrusion alert or manually initiated by users. Decentralizing the storage of video data reduced the amount of high bandwidth video data traffic on the CWS network.

The four pilots that developed a dashboard transmitted data and alerts from different CWS components to a central, temporary database via web services and scripted ETLs (extract, transform and load). **Table 3-3** shows the CWS components that were integrated into CWS dashboards.

Table 3-3. CWS Components Integrated into Dashboards

Component	Number of Utilities that Integrated this Component into their Dashboard	Information Available through the Dashboard	Typical Delay between Data Generation and Availability on the Dashboard
OWQM	4	Data and alerts	Minutes
CCS	4	Data and alerts	Minutes or hours
ESM	0	N/A	N/A
PHS	3	Alerts	Hours or days
S&A	4	Grab sample results	Hours or days
CM	4	Information entered by investigators	Minutes

All of the pilots' dashboards integrated OWQM and CCS data and alerts. This information was seen as valuable and pertinent both as part of the CWS and to support routine system operations. Also, this information was easily obtained (as it was typically generated and managed by the utility) and interpreted by utility personnel. Also, all dashboards were used for documentation of alert investigations and CM activities. No pilots included ESM data on their dashboard due to concerns that ESM video data would overwhelm the system and the technical difficulties with customizing proprietary data management systems used for ESM. However, all pilots did build an interface for ESM data and alerts that was generally available to users with dashboard access.

PHS and S&A information was included in many dashboards, although it was often not available in as timely a manner as it was for other components. The frequency with which PHS information was transmitted to the dashboard varied across pilots and was often only provided when an alert was generated. S&A data from grab sampling was uploaded no more frequently than once per day.

All of the pilots' dashboards were custom-built using a GIS interface, and information was superimposed on an area map. In general, the location of component alerts and data relevant to alert investigations was shown on the map. The user could navigate to additional screens that included more detailed plots and tables showing component data, alerts, and investigation details.

3.2.2 Summary of Lessons Learned

Demonstrate solutions during the selection process. Pilots that implemented a new, vendor-provided solution for the CWS information management system found the demonstration of potential solutions valuable. Several pilots asked vendors to demonstrate their product at the utility, particularly highlighting the functionality and features of interest to the utility.

Allow sufficient time to transition to full system deployment. All pilots recommended allowing sufficient time and resources for testing and system commissioning. This included allocating 10% to 20% of the information management system budget, and up to a year of the project schedule, to acceptance testing, bug fixes, enhancements requested by users during initial use, and optimization.

Only implement necessary product upgrades. Several pilots experienced problems after implementing updates to system software or hardware, as changes to one system impacted the processes and interfaces with all other elements of the information management system. Thus, one pilot suggested only implementing necessary system updates and not doing an update simply because it is available.

> **LESSON LEARNED HIGHLIGHT**
>
> GIS displays were found to be an effective way to organize and present CWS information, providing a clear and visually-appealing user interface and allowing personnel to rapidly identify relationships between different datastreams and alerts.

Eliminate unnecessary processes. To optimize performance, pilots configured their information management systems to perform only desired operations. At one utility, servers were overloaded because the system was updating statistics, plots, and tables each time a new data point was received. The utility worked with the vendor so that screens and plots were only updated when the user accessed them.

Establish a change management system. All pilots needed to modify information management systems after they were initially launched. Reasons for the modifications included identification of bugs and new requirements that were only evident after the system was put into use. In order to implement these modifications efficiently, and with minimum disruption to operations, one pilot recommended that a change management system be implemented.

3.3 Alert Investigation Procedures

Alert investigation procedures provide a systematic process for reviewing relevant information about the possible cause of CWS component alerts. This section describes the general approach that the pilots took in developing these procedures for the four surveillance components: OWQM, ESM, CCS, and PHS. Additional details about component-specific procedures can be found in Sections 4 through 7.

3.3.1 Summary of Implementation Approaches

All five pilots developed alert investigation procedures for each surveillance component, which included a process flow and assigned responsibilities for each step in the investigation process. For four of the pilots, these were captured in component-specific documentation. The remaining pilot incorporated alert investigation procedures from all components into a single CWS consequence management plan (CMP).

The pilots leveraged existing utility procedures when developing alert investigation procedures. This helped to identify key personnel, expected roles and responsibilities, and important steps in the process flow. It also minimized the time required to train personnel on the procedures, as individuals' roles and responsibilities for CWS alert investigations generally aligned with activities they were already performing.

All pilots developed checklists to guide investigators through the steps of the alert investigation. Multiple checklists were developed for each component, each including activities that would be carried out by a specific investigator. Four of the pilots (those that developed a dashboard as described in Section 3.2) integrated these checklists into the dashboard. This allowed users to access and populate the checklists within the dashboard user interface, and the entered information was viewable to anyone with access to the dashboard. The remaining utility used paper checklists that were stored in designated binders.

3.3.2 Summary of Lessons Learned

Develop alert investigation procedures early. All pilots developed at least a preliminary draft of alert investigation procedures before attempting to finalize the design of the CWS components. This was particularly important for the design of the information management system user interface and ensured that all information necessary for alert investigations and routine data review was readily available.

Engage front-line personnel in development of alert investigation procedures. The pilots found it beneficial to include all personnel who would ultimately be responsible for conducting alert investigations in the development of procedures. This helped align activities with existing job functions, ensured the practicality of proposed procedures, and fostered buy-in from those who would ultimately be responsible for implementing the procedures.

Actively maintain alert investigation procedures. Procedures should be reviewed and updated when changes in equipment, operations, or personnel occur. In addition, it is important to incorporate lessons learned from exercises and regular alert investigations to ensure the procedures remain relevant and effective. It was suggested that specific person(s) be made responsible for regularly reviewing these procedures and making updates as necessary, such as ensuring that all contact information is current.

Establish a clear hierarchy of responsibility for investigating alerts. For most of the pilots, multiple personnel received alerts. Thus, it was critical to establish a clear protocol for who was responsible for initiating the alert investigation, as well as what should be done if they failed to promptly respond (e.g., alert notifications would be repeatedly sent out until acknowledged). This often included special procedures for alerts that occurred after hours.

Establish different tiers for alerts. Several pilots had tiers of alerts depending on the response required. Lower-level alerts were generated when immediate response was not necessary, such as for instrument faults or OWQM alerts based on water quality parameters less likely to indicate a water quality problem. High-level alerts required personnel to investigate immediately because they were deemed more likely to identify potentially serious water quality issues. One pilot implemented logic that certain combinations of lower-level alerts (e.g., OWQM and CCS alerts from the same area) would automatically trigger a high-level alert.

3.4 Training and Exercises

For all the pilots, training, drills, and exercises were important to the successful implementation of all CWS components. Training was performed to teach personnel about their roles and responsibilities in performing specific procedures and to familiarize them with the tools available to support them in these activities. Drills and exercises were used to evaluate the ability of personnel to execute procedures in the context of a scenario and to identify deficiencies in the procedures themselves.

3.4.1 Summary of Implementation Approaches

All of the pilots adopted a progressive approach to drills and exercises as illustrated in **Figure 3-1**. The pilots implemented both discussion-based and operations-based exercises, generally starting with workshops and seminars, progressing through increasingly complex exercises, and culminating in full-scale exercises involving multiple components. Training, drills, and exercises were implemented at both the component level, to train personnel on and evaluate component procedures, and at the system level to evaluate end-to-end CWS operation. For larger, more complex drills and exercises, the pilots followed the Homeland Security Exercise and Evaluation Program (HSEEP), which provides a standardized approach for developing drills and exercises (FEMA, 2013).

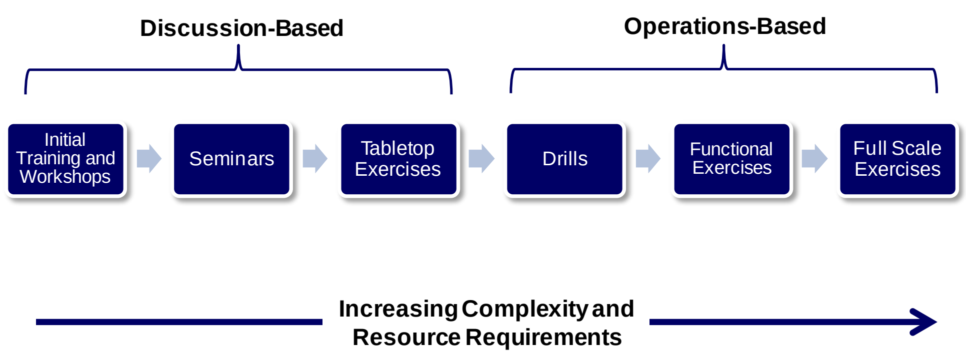

Figure 3-1. Progression of Drills and Exercises followed by the Pilots

Initial training and exercises were focused on teaching or testing a specific activity such as execution of a sampling protocol, use of a field test, or use of an alert investigation checklist. These were component-specific and were generally shorter and simpler than multi-component activities. As personnel became more familiar with their responsibilities and the procedures were refined, these exercises became more complex and involved more activities and participants, including external stakeholders. The full-scale exercises included multiple components (both surveillance and response), as well as the involvement of multiple utility divisions and external partners, to provide an end-to-end demonstration of the CWS. Participating personnel were notified in advance for the majority of drills and exercises. However, in a few cases, unannounced drills and exercises were conducted in order to more accurately assess the actions and timeline that could be expected during a real alert or emergency.

The insight gained from exercises was used to refine procedures. In some cases, refinements included the development of supplemental materials to support the correct and efficient execution of procedures, such as new user interface screens, field guides, and improved checklists. These activities also helped the pilots to identify future training needs.

IMPLEMENTATION HIGHLIGHT

Several of the pilots engaged retired employees to help plan complex exercises. The expertise provided by these individuals helped make the scenarios realistic and helped planners better anticipate how utility personnel would react to various situations.

The planning and execution of exercises required participation of a variety of utility and partner organization personnel. Particularly with functional and full-scale exercises, significant coordination was required to ensure that all participants, both from within and outside the utility, were aware of the exercise and the role they had to play. Also, support was needed to develop and execute the desired injects, such as an IT manager overriding ***real-time*** information to inject simulated component alerts into the dashboard.

3.4.2 Summary of Lessons Learned

Success in training and exercises is critical before beginning real-time CWS operation. The pilots found initial training and exercises to be critical for ensuring that personnel could perform their roles and responsibilities during implementation of CWS procedures. This training also served to reinforce key concepts with both internal and external personnel. Transitioning to real-time operation without this verification resulted in frustration and improperly implemented procedures.

Ensure personnel are prepared for exercises. Exercises are valuable in that activities are carried out in real time, allowing personnel to realistically carry out their responsibilities and evaluators to gauge the efficiency and timeline of investigation activities. Thus, it is important that personnel are comfortable with their responsibilities before attempting to perform them in real time.

Ongoing training and exercises are critical to the success of the CWS. All pilots emphasized the importance of ongoing training and exercises in maintaining the ability to properly implement procedures. This was particularly important for procedures that are not frequently performed, such as CM and S&A activities. Training and exercises also ensured that procedures remained relevant and up-to-date and that any updates or changes in procedures were quickly disseminated to all relevant personnel. Maintaining records of participation in training helped to identify training gaps and reinforce the expectation that personnel carry out their assigned responsibilities.

Planning an effective training or exercise takes time and resources. The pilots noted that planning effective training and exercises took more time and resources than originally estimated. For example, the pilots found that it generally took approximately six months to plan a realistic and comprehensive full-scale exercise and the involvement of high-level personnel. Even for simple training activities, careful preparation and identification of training objectives helped improve the efficiency and productivity of the activity and also maximized participant buy-in.

Include all partners in training, drills and exercises. All pilots stressed that external partners need to understand their responsibilities in order to properly implement CWS procedures. Thus, targeted training sessions for partners was valuable, and their involvement in certain activities, particularly full-scale exercises, helped to clarify roles and responsibilities and improve interagency lines of communication.

3.5 Summary of Pilot Experience with System Engineering

The pilots have reported that significant benefits have been realized through the system engineering activities undertaken to implement their CWS. It required a multi-disciplinary approach to system design and integration, which has had the benefit of improving communication and relationships among utility departments. The dashboards developed to support the CWS are currently used for a variety of purposes, including activities unrelated to the CWS and by utility personnel not responsible for CWS operation. The procedures developed for the surveillance components have provided a systematic approach to investigation of any water quality incident. Routine alert investigations have helped utility personnel develop a deeper understanding of the cause and effect relationship between system operations and water quality. Also, the training and exercise program implemented by the pilots has strengthened the relationships between each utility and its external partners.

The most common changes to system engineering design elements since the pilot period ended have been related to data communications. These changes have varied widely across the utilities, but in general have been triggered by frequent communications errors, identification of a more cost-effective solution, or a desire to standardize communications methods across the CWS. Other modifications to system engineering elements include updates to the information management system user interfaces based on user feedback and refinement of alert investigation procedures.

Section 4: Online Water Quality Monitoring

Online Water Quality Monitoring (OWQM) has two essential roles in a CWS: detection of unusual water quality conditions and routine monitoring of water quality in the distribution system. OWQM relies on the fact that typical water quality parameters (e.g., disinfectant residual, pH, specific conductance, total organic carbon (TOC), UV-Vis spectral absorbance, and turbidity) change in the presence of many potential contaminants, as well as during common water quality problems such as low chlorine residual, nitrification, cross connections, and treatment process upsets. Thus, indirect detection of unusual water quality conditions can be achieved by monitoring for changes in these standard parameters.

This section is organized by the OWQM design elements listed in **Table 4-1**. Data communications and data management are also OWQM design elements, but are discussed in Section 3 in the context of the integrated CWS.

Table 4-1. OWQM Design Elements

Design Element	Description
Water Quality Data Generation	Sensors continuously measure water quality parameters at strategically-identified locations throughout the distribution system.
Alert Generation and Investigation	Data is analyzed and an alert is produced if unusual parameter values or changes are detected. Utility personnel are alerted to the anomaly and initiate procedures to determine the cause of the alert and decide if additional actions are necessary.

4.1 Water Quality Data Generation

The water quality data generation design element defines the datastreams available for monitoring distribution system water quality and detecting unusual conditions. This design element consists of three sub-elements: sensor selection, station design, and station placement.

4.1.1 Summary of Implementation Approaches

Sensor Selection

As discussed in Section 1, contaminant coverage was one of the key performance objectives of the CWS pilot program. Thus, all pilots selected a set of water quality parameters that maximized the number of contaminant types that could be detected (Hall et al., 2007). Contaminant coverage was just one consideration, however. Below are examples of additional considerations that influenced the water quality parameters monitored by the pilots.

- *Identifying real-time hydraulic paths*: Two of the pilots specifically sought to understand flow paths and identify the source of water (e.g., a specific treatment plant or storage tank) supplying areas of the distribution system under different conditions. pH and specific conductance were useful for this purpose, as they varied across source waters but were consistent or changed slowly and predictably over time.

> **IMPLEMENTATION HIGHLIGHT**
>
> The pilots did not monitor the same set of parameters at all locations. Several pilots put specialized instruments in areas of interest, such as placing ammonia sensors only in areas with a history of nitrification.

- *Supporting regulatory compliance*: All pilots monitored disinfectant residual due to its value with respect to contaminant detection and routine operations. While the data generated by OWQM was not used directly for compliance monitoring, the real-time water quality data generated by the component provided information that was used to detect and correct problems that could lead to compliance issues.

- *Early identification of nitrification incidents*: Two of the pilots have recurring nitrification episodes in their distribution systems and thus installed ammonia sensors to facilitate early identification of these incidents so that they could respond and minimize the impact.

Table 4-2 summarizes the water quality parameters by the pilots. The final four rows summarize parameters for which derived values were generated by full spectral instruments (sensors did not measure those values directly).

Table 4-2. Summary of Water Quality Parameters Monitored by the Pilots

Parameter		Number of Pilots Monitoring this Parameter	Total Number of Locations where this Parameter is Monitored
Direct Measurement	Conductivity	5	81
	Disinfectant residual[1]	5	84
	pH	5	71
	Temperature	5	16
	Full range spectral absorbance	4	34
	Turbidity	4	39
	Ammonia	2	22
	Oxidation Reduction Potential (ORP)	3	27
	Ultraviolet Absorbance at 254 nm (UV-254)	3	12
	Oil in Water	1	1
	Total Organic Carbon (TOC)	2	18
	Volatile Organic Compounds (VOCs)	1	2
Derived Values	Dissolved Organic Carbon (DOC)	4	34
	Nitrate	4	34
	Total Organic Carbon (TOC)	5	36
	Turbidity	4	34

[1] Four pilots monitored free chlorine and two monitored total chlorine residual (one pilot monitored both)

As shown in this table, all pilots monitored a core set of parameters that included disinfectant residual, pH, temperature, and turbidity. All five pilots also monitored the concentration of organic matter, although UV-254 or the derivative TOC value produced by spectral instruments was more common than TOC due to the significant maintenance requirements for the TOC instruments that used electrochemical analysis methods. Additional parameters were added based on utility objectives (e.g., ammonia for detection of nitrification), or because they came as part of a sensor suite (e.g., the full spectrum instruments automatically provided nitrate values).

There were some sensor types that were tested but not deployed. One pilot investigated use of radiological sensors but concluded that none of the available online instruments had sufficient detection limits to detect radiological contamination at levels of concern. Two utilities tested biomonitors and concluded that current technologies were not practical for distribution system monitoring, largely due to the significant labor hours required to maintain the systems and the need to provide continuous dechlorination of the water feeding the instruments.

Once the pilots decided which parameters to monitor, they researched and selected the actual monitoring technology. Criteria used by the pilots when selecting their equipment included:

- *Costs*: Initial and ongoing parts and maintenance costs were certainly important considerations, as was the expected life of the technology.
- *Installation requirements*: The requirements with the greatest impact on sensor selection were sensor unit size, waste stream disposal, ventilation, and temperature controls.

- *Maintenance requirements*: The pilots avoided sensors that required frequent service visits, as well as technologies that required significant training and time to perform maintenance and calibration activities accurately.
- *Sensor performance*: The pilots leveraged previous utility experience (theirs or others), vendor information, and independent sensor studies (EPA, 2005a; EPA, 2005b; EPA, 2009) when assessing instrument performance. Two utilities also established partnerships with local universities to do a side-by-side comparison of available technologies.
- *Prior experience with vendor and equipment*: All pilots used previous experience with different vendors and hardware models to inform their selection process.

Table 4-3 shows the instruments that were installed by the pilots. It includes both the number of pilots that used each instrument, as well as the total number of locations at which the specific instrument model was installed across all pilots. The multi-parameter probes generally measured chlorine, conductivity, pH, and temperature.

Table 4-3. Summary of Sensor Hardware Deployed by the Pilots

Parameter	Instrument Vendor	Instrument Model	Number of Pilots that Installed this Instrument	Total Number of Locations where the Instrument was Installed
Ammonia	s::can	ammo::lyser	2	22
Chlorine	ATI	Q45H	1	10
	Hach	CL-17	1	12
	s::can	chloro::lyser	3	24
	Wallace & Tiernan	Depolox 3 Plus	2	15
Conductivity	ATI	Q45C4	1	10
	Hach	63C	1	10
	Hach	D3422C3	1	9
	Hach	GLI 3422	1	3
	s::can	condu::lyser	3	26
pH	ATI	Q45P	1	10
	Hach	GLI pHD	1	3
	Hach	P63	1	6
	Hach	Hach pHD sc	1	9
	s::can	ph::lyser	2	20
Oil in Water	Hach	not specified	1	1
ORP	ATI	Q45R	1	10
	Hach	pHD/ORP sc	1	9
TOC	Hach	Astro 1950Plus	1	3
	s::can	carbo::lyser	1	2
	GE	Sievers 900	2	15
Turbidity	ATI	A17-76	1	10
	Hach	1720D	1	3
	Hach	1720E	2	13
UV-254	Real Tech	UV-254	2	10
	Hach	UVAS	1	1
	HF Scientific	AccUView Online UV %Transmission Analyzer	1	1
VOC Analyzer	Inficon	CMS-5000	1	2
Multi-parameter	Hach	GuardianBlue™	2	8
	Intellitect	Intellisonde	2	3
	s::can	spectro::lyser	4	34
	Wallace & Tiernan/US Filter	Depolox 5	2	7
	YSI	6500	1	5

Station Design

Monitoring station design, which encompasses all practical elements required to install the sensors in an operational environment, is closely related to equipment selection. In some instances, pilots had precise installation requirements and selected sensor hardware to fit those constraints (e.g., one pilot wanted to install sensors in existing, small enclosures used for sample collection). An alternate approach used by the pilots was to first select instruments based on other performance criteria and then design stations to accommodate them.

The following considerations were important to station design:

- Cost of building a station
- The physical size and layout of sensors and accessories (e.g., tubing, power, and communications)
- Supplemental equipment needed to ensure proper ventilation and temperature control
- Ease of fabrication and installation
- Protection from environmental conditions and vandalism

> **IMPLEMENTATION HIGHLIGHT**
>
> Several pilots added remotely-triggered sample collection systems to their monitoring stations to support investigation of abnormal water quality. Without this feature, sample collection cannot begin until a sampling crew arrives at the site, by which time the water slug of interest may have completely passed through the station.

Due to the variety of sensors installed and site-specific constraints, all station enclosures were custom-designed and no pilot used the same station design for all of their monitoring locations. Station designs fell into three general categories: (1) stations in which equipment was attached to a board or frame that was either attached to a wall or free-standing, (2) stations in which sensors were installed in enclosed, lockable cabinets, and (3) compact stations in which sensors were installed in a small enclosed space.

Station Placement

At the beginning of the station placement process, all pilots determined the number of new monitoring stations installations. Based on budget and resources available for procuring and maintaining the sensors, the pilots installed between 10 and 19 new stations. They then began the iterative process of identifying locations within the distribution system where monitoring was desired and evaluating the feasibility of installing stations at these locations.

All of the pilots used the Threat Ensemble Vulnerability Assessment – Sensor Placement Optimization Tool (TEVA-SPOT) to support station placement, although the methods of applying TEVA-SPOT varied. Some pilots identified potential physical monitoring locations throughout the system (e.g., all utility and city-owned facilities) and completed a TEVA-SPOT analysis to identify optimal locations from this subset. Others ran TEVA-SPOT over the entire distribution system to identify optimal placement of sensors for contaminant detection and then searched for physical locations where monitoring stations could be installed near these optimal locations. Finally, some pilots ran TEVA-SPOT on targeted portions of the distribution system they knew they wanted to monitor, such as areas with historically low disinfectant residual levels, areas where water quality was not well understood, high-profile locations (e.g., sports stadiums or arenas), and areas serving critical customers (e.g., hospitals).

> **IMPLEMENTATION HIGHLIGHT**
>
> All pilots deployed their monitoring stations in phases, using lessons learned from initial installations to inform subsequent procurements and design. The phased approach also made equipment implementation and operation more manageable as the effort was spread out over time.

Regardless of the approach, the locations identified by TEVA-SPOT provided only a starting point for selecting monitoring sites, and expert judgment of utility personnel was then required to identify final locations. In all cases, significant refinement was required to arrive at the final set of locations because some of the initial sites were found to be impractical based on the factors listed below. **Table 4-4** summarizes the types of locations ultimately selected by the pilots.

- Physical space requirements
- Sample water source with adequate flow and pressure
- Power and drain availability
- Ability to transmit sensor readings to a centralized data repository
- 24/7 site access for troubleshooting and access during alert investigations
- Site security

Table 4-4. Summary of OWQM Station Installation Locations

Location Type	Number of Pilots that Installed a Station at this Location Type	Total Number of Stations Installed at this Location Type
Utility-owned facilities (e.g., pump or valve stations, reservoirs, treatment plants)	5	30
Government- or city-owned facilities (e.g., police departments, fire stations, parks, entertainment venues)	5	38
Private facilities (e.g., hotel, hospitals)	2	3
Public right-of-way (e.g., street-side or sidewalk)	2	3

While all pilots considered use of private facilities, these were the most difficult to implement because the utilities lacked control over the location. All designs and implementation activities had to be approved by managers of the host facility, which caused significant delays in several cases. Site access was also a challenge. In general, private facility partners were financially compensated for hosting a monitoring station through credits to their water bill.

One of the pilots attempted to expand OWQM through partnerships with companies who did their own water quality monitoring, such as beverage producers, to obtain the data already being generated. However, no agreement was reached during the pilot period, primarily due to the companies' legal concerns over the proposed data sharing arrangement.

Four of the pilots installed at least one of their stations outdoors. For example, some monitoring stations were installed on exterior walls or in courtyards of utility facilities. This provided greater accessibility and did not take up space indoors, but these stations were more vulnerable to tampering and the elements (e.g., temperature extremes, precipitation, and humidity). In general, these pilots installed only one or two stations outdoors, as these were largely seen as a proof of concept installations used to evaluate whether sensors could operate reliably outdoors.

One pilot developed a mobile OWQM station with a small footprint that could be relocated as desired. This allowed them to monitor during important events (e.g., major sporting events) and in areas of short-term interest (e.g., downstream of a main break).

4.1.2 Summary of Lessons Learned

Sensor Selection

Test instruments at the utility to assess maintenance requirements and data quality under utility-specific conditions. Some vendors allowed the pilots to test a trial unit for several months to evaluate performance. In other cases, the pilots purchased a small number of instruments initially, later installing more units if performance and maintenance requirements were deemed acceptable.

LESSON LEARNED HIGHLIGHT

It is important to consider water chemistry when selecting monitoring equipment. The high chlorine residual and pH of one utility's water caused aggressive oxidizing of an aluminum tube housing the instrument's optics, necessitating frequent maintenance. The vendor replaced the original housings with stainless steel housings, which resolved the issue.

Consider life cycles costs, including maintenance costs. The pilots found that maintenance costs over the life of the instrument were greater than capital and installation costs for some instruments. In some cases, particularly when equipment required frequent maintenance, travel time to monitoring locations turned out to be a significant contributor to maintenance costs.

Ensure adequate vendor support. Several pilots experienced delays due to instrument vendors that did not provide sufficient or timely supports. Due to lack of response, one pilot never got one of their instruments running correctly.

Standardize equipment. After installing and testing a variety of instruments, all pilots found it most efficient to standardize equipment, using the minimum number of vendors and instrument models across monitoring locations. This reduced training requirements for instrument technicians, the number of vendors the utility had to interact with, and the inventory of spare parts.

The more complex the design of a sensor, the more opportunities there are for malfunction. In particular, utilities found that instruments with a lot of intricate or small-diameter tubing were more prone to clogging than instruments with short, straight water flow paths. Also, systems with more mechanical parts generally malfunctioned more frequently.

Laboratory instruments may not work well for online monitoring. Some pilots attempted to use proven laboratory instruments that had been configured for online monitoring (in particular, online TOC and VOC analyzers). They were generally unable to maintain accurate readings with these units, as laboratory instruments are generally not designed to run continuously or to handle changing environmental and pressure conditions. Data communications was another challenge. Despite significant effort, one utility was never able to successfully transmit the data produced from a retrofitted laboratory instrument. Also, data from advanced instrumentation was difficult to interpret by utility personnel. In particular, it was noted that the interpretation of data generated by the VOC analyzer installed by one utility required significant knowledge of analytical chemistry.

Assign a dedicated technician to complete initial troubleshooting. Many instruments required significant initial troubleshooting. Ensuring that instruments were operating correctly before beginning routine maintenance activities reduced the negative perceptions some utility personnel had toward the new OWQM equipment. Some pilots hired a contractor with experience with the instruments for this role.

Ensure that online instruments produce data of sufficient precision and accuracy. All pilots experienced periods where online instruments generated inaccurate data that compromised the ability of OWQM to meet utility goals. One pilot participated in an extensive study to characterize the accuracy and precision of online water quality monitoring instruments (Rosen, et al., 2012).

Station Design

Flow and pressure sensors provide valuable information during alert investigations. Insufficient flow to sensors is a common cause of inaccurate data. Thus, installation of flow and pressure sensors at each station allowed investigators to quickly confirm or rule out this potential alert cause.

Design stations to easily accommodate new hardware. All of the pilots changed sensor hardware after the initial installation, including installing new technologies and replacing those with inferior performance. Thus, the ability to change hardware without entirely redesigning the station enclosures was extremely valuable.

Consider how hardware will be transported to the monitoring location. In more than one instance, utilities had problems getting the assembled equipment through doors or down stairs.

Restrict access to sensor hardware, even at secure facilities. Upon investigating frequent step changes in parameter values, one utility found that utility personnel were frequently adjusting sensor settings if they walked by and observed readings they felt were inaccurate. The resulting changes in data values triggered many automated alerts.

Implement safeguards to prevent flooding. Several utilities experienced significant flooding and damage due to leakage from monitoring stations. To prevent future incidents, they implemented leak detection systems with automatic water shutoff for stations installed in buildings that could be damaged by flooding.

Sensor Placement

Ensure sufficient flow in all conditions. Several pilots were forced to move monitoring stations because there was insufficient flow through the stations as system conditions changed. One installed station was located near a community pool, which had minimal flow in the winter. Another station was at a pump station that was not used during certain operating conditions, causing loss of flow to the station and erratic readings.

Avoid locations with an unpredictable water quality baseline. Pilots found that water quality at some monitoring locations, such as those frequently impacted by operations at one or more utility facilities, was so erratic that the data generated provided little value.

> **LESSON LEARNED HIGHLIGHT**
>
> Although all pilots used TEVA-SPOT and hydraulic models to identify monitoring locations, unpublished studies have found that utility personnel with a strong understanding of system hydraulics and water quality can identify practical monitoring locations that provide operational benefits and have the potential to detect water quality anomalies.

Consider the impact of environmental conditions on sensor performance. In general, outdoor stations (or indoor locations with inadequate environmental controls) required sun shades, ventilation, or heaters to maintain acceptable performance. Also, one utility had to move a monitoring station installed near a furnace because cycling of the furnace caused step changes in sensor readings.

Understand environmental and regulatory requirements. Environmental reviews and permitting for stations installed in the public right-of-way resulted in significant delays at some pilots.

Consider the reliability of the cellular signal at monitoring locations. Even at sites that do not rely on cellular service for data transmission, unreliable cellular service can hamper communications with personnel working at these locations.

4.2 Alert Generation and Investigation

This design element consists of two sub-elements, alert generation and alert investigation. Alert generation includes the ***data analysis*** approach used to generate OWQM alerts. Alert investigation covers the procedures for investigating these alerts.

4.2.1 Summary of Implementation Approaches

Alert Generation

Criteria that the pilots used to select their data analysis solution (also called an event detection system or EDS) are summarized below.

- *Ability to analyze data from any sensor*: Some data analysis solutions considered by the pilots were integrated into sensor hardware units and could not analyze data from external sensors. Because all pilots used sensors from multiple vendors, often at a single monitoring location, this was a significant factor considered in the selection process.
- *Ability to handle complex datastreams*: The spectral instruments used by several pilots produced hundreds of datastreams, corresponding to different wavelengths. The data analysis solutions provided by these equipment vendors were specifically designed to effectively analyze this data, including accounting for the relationship among these datastreams, whereas other solutions were unable to analyze this volume of data efficiently.
- *Available support*: The quality and timeliness of product support was an important consideration. In particular, pilots were skeptical if necessary support would be provided by solution providers who could not provide a formal support agreement.
- *Performance*: The ability of the data analysis solution to detect incidents of abnormal water quality while producing a manageable number of invalid alerts.

IMPLEMENTATION HIGHLIGHT

Although all pilots used specialized data analysis solutions, recent research by EPA has found setpoints to be an effective and easily implemented alternative (Umberg, 2015).

The pilots considered a wide variety of solutions that varied with respect to complexity, analysis approach, and the required level of user expertise. Most products were proprietary and marketed by vendors, though some were developed by researchers and available for free public use. The vendors varied in size, years of experience in the water industry, and location (some companies were international). There was also a mix of centralized (a single instance of the tool was installed at a central location) and distributed solutions (the tool was installed at every monitoring location).

All five pilots applied a rigorous process to select their primary data analysis solution, developing well-defined evaluation criteria and requesting proposals from numerous vendors and algorithm developers. All pilots required solution developers to present their product in person, and three of the pilots formally evaluated the solutions' performance using their own historical data and simulated contamination incidents. They evaluated the number and types of invalid alerts produced, as well as the number of anomalies detected.

Table 4-5 shows the data analysis solutions implemented by the pilots. Four pilots implemented more than one solution in order to compare solutions, or because some products were integrated into sensor equipment that was not installed at all monitoring locations. Note that at the time these systems were implemented, it was believed that sophisticated data analysis techniques were necessary for OWQM, so simpler data analysis solutions, such as parameter setpoints, were not considered.

Table 4-5. Data Analysis Solutions Implemented by the Pilots

Data Analysis Solution - with Vendor / Developer	Number of Pilots that Implemented this Solution	Centralized or Distributed
CANARY - Sandia National Laboratories, EPA	3	Centralized
ana::tool - s::can	3	Distributed
Event Monitor - Hach Company	2	Distributed
BlueBox™ - Whitewater Security	2	One pilot installed Centralized, the other Distributed

CANARY was implemented by several pilots because it was free, could be installed on any workstation, and its data analysis approaches were well documented (as opposed to the "black box" approach of some other solutions). ana::tool and the Event Monitor were integrated into those vendors' sensor hardware, and thus were only considered by the pilots that had selected that hardware. Given that Bluebox™ was a new product, the pilots that chose that solution were prepared to work with the vendor to test and refine the product.

Alert Investigation

Section 3 describes general aspects of alert investigation procedures developed for the pilots that are applicable to all four surveillance components of a CWS. For example, all pilots held classroom training, tabletop exercises, and drills to train personnel on their roles and responsibilities. This section provides additional details about the approach taken by the pilots to implement OWQM alert investigation procedures.

> **IMPLEMENTATION HIGHLIGHT**
>
> At one utility, water quality specialists performed a detailed review of historical data and developed an "investigation guide" for each station, listing steps for investigating alerts at each monitoring location. These guides were updated based on experience gained during alert investigations.

OWQM alerts were displayed on a user interface for all pilots. For four of the utilities, alert notifications were also transmitted via texts or emails to supervisors or managers. These notifications were often sent to multiple personnel to make them aware of the alert, although utility procedures typically assigned the responsibility for initiating the investigation to a specific individual.

At all pilots, investigation of OWQM alerts began with review of water quality at the monitoring location that produced the alert. In many cases, a benign cause was clear and reviewers could note this and close the investigation. If no cause was identified in this first step, additional information was considered, including water quality data from nearby monitoring locations and customer complaint information. Other investigation activities included contacting system operations and distribution maintenance personnel to see if their actions could explain the abnormal water quality data and performing an on-site inspection of the sensors and equipment at the monitoring location.

4.2.2 Summary of Lessons Learned

LESSON LEARNED HIGHLIGHT

The most common cause of invalid alerts for all pilots was inaccurate or incomplete sensor data due to equipment malfunction. The number of invalid alerts generally decreased as equipment issues were addressed and technicians learned the source and resolution of common sensor problems.

Alert Generation

Invalid alerts are inevitable: All pilots found that their initial goal of receiving only a handful of OWQM alerts per year was not possible. The sensor technology available during the pilot projects periodically generated erratic, inaccurate, or incomplete data, which creates a challenge for any data analysis system. Also, valid alerts were occasionally caused by benign water quality incidents, such as those caused by changes in supply and operations.

Consider costs for maintaining and configuring the data analysis solution: All pilots found that the selected solution needed to be regularly reconfigured to maintain acceptable performance. These updates were necessary to accommodate changes in the baseline caused by seasonal effects or different operating conditions, as well as occasional sensor modifications. Thus, the ability of utility personnel to quickly and easily reconfigure the tool was valuable (some solutions selected could only be configured by the tool developer, and others took days of analysis by trained personnel to adjust settings).

Alert Investigation

Alert investigations can often be completed with little effort: As noted above, the pilots learned that invalid alerts are inevitable. However, they also learned that the time required to investigate these alerts was generally much less than originally expected. Alerts could often be determined to be invalid within a few minutes based on review of water quality at the monitoring location, and completion of all investigation activities was rarely necessary.

4.3 Summary of Pilot Experiences with OWQM

The pilots have reported OWQM to be valuable to routine system operations as well as detection of water quality incidents. All pilots continue to operate OWQM, and several have added monitoring locations to provide additional data about distribution system water quality.

OWQM was generally the most expensive component to implement and required skilled technical personnel to implement and maintain. Some of the sensors deployed were technically sophisticated and required additional training for technicians. Several of the data analysis tools implemented were also complex and required specialized knowledge to implement and maintain. OWQM also generally required more personnel hours for routine maintenance activities compared to the other CWS components. This was largely due to the fact that more equipment was installed for OWQM than for the other components. Additionally, personnel responsible for investigating OWQM alerts had to spend time learning typical water quality patterns and conditions that impact water quality at each monitoring location. However, as personnel became familiar with their responsibilities, it took them less time to maintain the component, review data, and investigate alerts. The pilots report that OWQM operation continues to be integrated more seamlessly into their normal distribution system monitoring and management regime.

All pilots modified OWQM from the initial design. All pilots also decommissioned instruments that were found to have excessive maintenance requirements, produce erratic or inaccurate data even when properly maintained, and for which adequate vendor support was not available. Where possible, the pilots also standardized equipment, using the same model and vendor at all installations, which reduced requirements for training and the number of different replacement parts that must be kept in inventory. Also, three of the five pilots now use parameter setpoints for alert generation due to poor performance, lack of support, or difficult maintenance of their original data analysis solution. These changes have markedly improved the sustainability of OWQM.

Section 5: Enhanced Security Monitoring

Enhanced Security Monitoring (ESM) includes the equipment and procedures necessary to detect and respond to intrusions at utility facilities that are vulnerable to contamination. This section is organized by the ESM design elements listed in **Table 5-1**. Data communications and information management are also important design elements for ESM and are discussed in the context of the integrated CWS in Section 3.

Table 5-1. ESM Design Elements

Design Element	Description
Intrusion Detection Equipment	Intrusion sensors and video cameras continuously monitor for unauthorized entry at strategically-identified distribution system facilities.
Alert Generation and Investigation Procedures	Intrusion sensors and video cameras generate an alert when an intrusion has been detected. Utility personnel implement alert investigation procedures to determine the cause of the alert and decide if a response is necessary.

5.1 Intrusion Detection

The intrusion detection design element involves the selection of utility sites for ESM enhancements and equipment to be installed at each ESM site. This design element consists of three sub-elements: site selection, intrusion sensor selection, and video equipment selection.

5.1.1 Summary of Implementation Approaches

Site Selection

When selecting sites for ESM enhancements, the pilots most commonly considered pump stations, reservoirs, and storage tanks. One pilot also considered a large, natural reservoir that was part of their supply system.

Table 5-2 summarizes the ESM site selection methods used by the pilots, which involved the application of one or more of the following three techniques. They are presented in order of increasing complexity, from simple and qualitative to complex and quantitative.

- *Professional judgment*: All of the pilots used some form of professional judgment, which typically consisted of technical experts within the utility operations groups meeting to discuss potential ESM sites and reaching a consensus regarding which sites should be enhanced with security equipment. This method was qualitative and considered a facility's population served, production or volume, existing security system, crime rate, and remoteness of the facility.
- *Vulnerability assessment*: A vulnerability assessment evaluates each utility facility's security system capabilities and its likelihood of, vulnerabilities to, and consequences from an attack. These attributes are quantified for each facility using a standardized scoring framework, which considers the same factors listed above under professional judgment, and an overall risk score is calculated for each. All of the pilots had an existing vulnerability assessment that was conducted as part of the requirements of the Bioterrorism Act, and three utilities considered this information when selecting ESM sites. Utilities ranked potential sites based on the calculated risk value and considered the cost of enhancements at each site when selecting the locations for installing ESM equipment.
- *TEVA-SPOT*: Two pilots used the TEVA-SPOT software tool when selecting ESM sites, although only one pilot performed a TEVA-SPOT analysis specifically for evaluating potential ESM sites. The other pilot leveraged the TEVA-SPOT results generated during design of OWQM to inform the ESM site selection process.

Table 5-2. Approaches used by the Pilots to Select ESM Site

Site Selection Method	Number of Pilots Using this Combination of Methods
Professional judgment only	1
Professional judgment and vulnerability assessment	2
Professional judgment, vulnerability assessment, and TEVA-SPOT	1
Professional judgment and TEVA-SPOT	1

Intrusion Sensor Selection

After sites were selected for ESM enhancements, the pilots selected intrusion sensors for installation. Some pilots chose equipment they were familiar with, while others tried new equipment. The types of technologies implemented are described below and summarized in **Table 5-3**.

- *Door/hatch sensors*: All pilot utilities had existing door and hatch sensors installed at their facilities, usually on exterior entrances. As part of their ESM enhancements, some pilots supplemented these existing sensors with additional sensors on outdoor hatches and on interior doors with access to finished water.
- *Area motion sensors*: Four pilots installed area motion sensors to monitor for break-ins along banks of windows and for detection of intruders approaching a facility.
- *Ladder motion sensors*: One pilot installed ladder motion sensors to detect unauthorized personnel climbing ladders that provided access to finished water (e.g., to the top of an elevated storage tank).
- *Sensor array*: One pilot installed a sensor array on hatches, which included a hatch sensor and a seismic transducer. The hatch sensor would detect an intruder opening the hatch and the seismic transducer would detect any attempts to bypass the hatch sensor by penetrating the hatch without opening it. The sensor and transducer were connected to a microprocessor that generated an alert when an attempted hatch opening or penetration was sensed.

Video Equipment Selection

All pilots installed video cameras as part of their ESM enhancements. They chose cameras with different features depending on the application.

- *Fixed-position vs. pan-tilt-zoom*: All pilots installed pan-tilt-zoom cameras, although fixed cameras were also used for applications where only a stationary view of a well-defined area was needed.
- *Day-night vs. infrared vs. thermal*: Day-night, low-light cameras were used in most cases, although infrared cameras or thermal imaging cameras were used for certain outdoor locations. Supplemental indoor lighting that energized when an intrusion was detected was implemented in some video applications to improve the night-time image resolution of day-night cameras.
- *Analog vs. Internet Protocol (IP)-based video*: Analog cameras were used when it was the utility's standard and to maintain compatibility with legacy systems. IP cameras were used when the utility wanted to use Ethernet cabling and network infrastructure, digital processing of the video datastream, or network-enabled storage methods.

IMPLEMENTATION HIGHLIGHT

Because complete video coverage was infeasible, one pilot deployed cameras on a mobile platform so that they could be easily relocated as needed.

All pilots connected their video cameras to a digital video storage device, such as a digital video recorder (DVR) or a network video recorder (NVR), to store the continuous video data generated by the cameras. The video storage devices were typically located at the remote facility and configured to only transmit video of intrusions when they were detected, a mode of operation referred to as incident-driven video. Incident-driven video minimized the bandwidth load on the communications infrastructure and eliminated the need for security personnel to continuously monitor video screens. Archived video data could be reviewed as part of active investigations, exported as evidence for law enforcement officials, or used to develop training materials.

Table 5-3. ESM Equipment Installed by the Pilots

Equipment Type		Number of Pilots Using this Equipment Type
Intrusion Sensors	Door and hatch sensors	4
	Area motion sensors	4
	Ladder motion sensors	1
	Sensor array	1
Video Cameras	Fixed	4
	Pan-Tilt-Zoom	5
	Day-night	5
	Infrared	4
	Analog	2
	Internet Protocol (IP)	3
	Video Storage and Transmission	5

5.1.2 Summary of Lessons Learned

Site Selection

Relatively simple methods are effective for selecting sites for ESM enhancements. The pilots all used some form of professional judgment and most used their existing vulnerability assessments to select sites and ESM equipment. The utilities' in-depth knowledge of each facility's hydraulic characteristics, security features, surroundings, and criticality provided a simpler and more informed means of ranking each facility for ESM enhancements relative to more sophisticated methods.

Equipment Selection

Use video monitoring systems that are compatible with other system elements. Equipment from different video manufacturers took time and resources to integrate and troubleshoot. Use of equipment designed for compatibility minimized communications failures between devices and reduced integration and maintenance costs.

Video monitoring equipment at sites subjected to environmental extremes may require more frequent maintenance. For most pilots, the NVRs at sites such as pump stations, storage tanks, and reservoirs were subjected to environmental factors (e.g., temperature variances, chlorine fumes, and dust). These conditions required hardening and more frequent maintenance or replacement.

Ensure that continuous power is available at remote sites. One utility experienced nuisance ESM equipment outages when non-ESM equipment on the same circuit overloaded the breaker. These sporadic gaps in ESM detection capability were eliminated by providing a dedicated circuit breaker for the ESM equipment. Another utility experienced nuisance alerts caused by brief power outages and brownouts at locations that were not equipped with an uninterruptable power supply (UPS). UPS units were subsequently installed at these facilities to address this issue. ESM sites that were designed to accommodate loss of power, using UPS units and surge arrestors, did not experience gaps in service due to power interruptions.

Develop a Security Master Plan. One utility had incompatible access control systems at three of their main facilities because security improvements, which were part of much larger capital improvement projects, were not coordinated. Because of this, updates needed to be made to all three systems whenever personnel were hired or terminated, and employees had to wear three unique badges. The utility addressed this issue by developing a 5-year Security Master Plan to coordinate security projects, personnel, and protocols under a unified program. Key features of the Security Master Plan included an integrated access control system and a centralized communications network to transmit access control and video data. The Security Master Plan also created a position for a security system coordinator, who was responsible for implementing the security master plan and promoting a security culture within the utility.

5.2 Alert Generation and Investigation

This design element consists of two sub-elements, alert generation and alert investigation. Alert generation includes the methods used to generate ESM alerts. Alert investigation covers the procedures for investigating these alerts.

5.2.1 Summary of Implementation Approaches

Alert Generation

ESM alerts were generated by one of three methods: intrusion sensors, video analytics, or human reporting. A discussion of each method is provided below, and use of each method is summarized in **Table 5-4**.

- *Intrusion sensors* included the following:
    - *Door/Hatch sensors*: A magnetic reed built into the sensor opened or closed a contact when it was within a preset distance from a magnetic target.
    - *Motion sensors*: A microprocessor located in the sensor housing used an algorithm that continuously analyzed the sensor's microwave and infrared detection beams and generated an alert when both beams sensed motion.
    - *Sensor array*: A microprocessor located in the sensor array housing used an algorithm that continuously analyzed data from a seismic transducer. The algorithm was designed to detect an intruder sawing, grinding, or drilling through a hatch while ignoring environmental noise from wind, rain, hail, etc. The hatch sensor in the array used a magnetic reed mechanism, as described above.
- *Video analytics* consisted of an algorithm that continuously analyzed a camera's datastream for human motion, unexpected objects, and other unauthorized activity. The algorithm ran on a microprocessor in the camera or on a video recorder located at the remote site. Though all five pilots used video surveillance, only three pilots implemented video analytics. One pilot used video analytics on a mobile trailer to detect suspicious behavior at a large natural reservoir, while the other two pilots used video analytics at typical distribution system facilities, including an application where video analytics was used to detect an intruder climbing a ladder.
- *Human reporting* included eyewitness reports of suspicious activity and threatening phone calls, emails and letters to the utility. One of the pilots developed ESM procedures, checklists, and scripts to respond to human-reported alerts.

Table 5-4. Overview of ESM Alert Generation Methods

Method	Number of Pilots Using this Method
Intrusion sensors	5
Video analytics	3
Human reporting	1*

* The other 4 pilots used existing procedures to respond to human-reported alerts.

Alert Investigation Procedures

Section 3 describes general aspects of alert investigation procedures developed for the pilots that are applicable to all four surveillance components of a CWS. For example, all pilots held classroom training, tabletop exercises, and drills to train personnel on their roles and responsibilities. This section provides additional details about the approach taken by the pilots to implement ESM alert investigation procedures.

An important investigative tool for ESM was the use of video from suspected unauthorized intrusions. Video imagery of intrusions was used to confirm if an employee inadvertently caused an alert or if the alert was due to unauthorized entry, reducing the number of time-consuming on-site investigations initiated by invalid alerts. Additionally, video imagery had the potential to show whether an intruder was intent on theft, vandalism, or contaminating the water supply.

The pilots also created the following ESM-specific job aids to educate law enforcement officers about water utility facilities, improving their ability to distinguish between normal work activities and suspicious activities.

- *Training Videos*: One pilot developed a training video for each law enforcement district in the utility's service area. These videos were intended to assist law enforcement officers with responding to utility facilities by describing site-specific features and potential signs of tampering at each utility facility in the applicable district.
- *Training Brochures*: One pilot developed a training brochure for local law enforcement to help them identify illegal connections to fire hydrants. The utility was concerned about cross-connections and wanted to empower law enforcement officers to proactively address situations that could lead to contaminant introduction through a fire hydrant. The brochure described key "dos and don'ts," provided photographs of legal and illegal hydrant connections, and documented steps to take if an illegal connection was suspected.

Effective communication was essential to investigating ESM alerts and involved coordination with local law enforcement. Pilots established points-of-contact, rendezvous protocols, and other means of collaboration as described below.

- *Fusion Center*: One pilot worked with their city's police department to engage the existing law enforcement Fusion Center, which provides a point of contact for federal law enforcement and all police substations within the city. The center shares intelligence, investigates crimes, and reports crime trends. The Fusion Center can provide extra police patrols if crime rates are trending upward near a utility facility, and the utility can request additional police presence when a difficult employee termination occurs or suspicious activity is observed. The utility's security coordinator established an ongoing relationship with the Fusion Center, and the center participated in utility-led exercises.
- *Communication Plan*: One utility implemented a communication plan to streamline information exchange between law enforcement and utility personnel when source water quality or quantity may have been impacted by a natural or human-caused incident. The communications plan has been incorporated into the police and utility's Standard Operating Procedures (SOPs).

- *Scripts*: One pilot developed pre-scripted messaging templates for utility investigators to use when contacting local law enforcement and the utility's emergency response manager. Different scripts were used depending on the entity contacted and whether video information was available. The scripts were developed to include placeholders for pertinent information recorded on an ESM alert investigation checklist. Use of these scripts ensured that the utility investigator provided all of the necessary information when contacting law enforcement to report an ESM alert.

5.2.2 Summary of Lessons Learned

Alert Generation

Video data must be transmitted quickly for operators to use it. At one of the pilots, the operators usually chose not to view video clips of intrusions because too much time was required to transmit the video clip. This pilot migrated their communications to a faster technology, which significantly increased the download speed and allowed operators to view video in near real time. Following the communications upgrade, the operators used the video feature regularly.

A diligent commissioning effort is essential to minimizing invalid alerts. All of the pilot utilities experienced a high level of invalid alerts after ESM startup as a result of inadequate commissioning efforts by the installation contractor. Motion sensors and video analytics systems were especially prone to invalid alerts if the sensitivity of the sensors and systems were not properly calibrated to the baseline conditions of the monitored area. Some systems needed periodic recommissioning because baseline conditions changed and the device's sensitivity drifted over time. Commissioning was also important when installing video cameras to ensure that the image was not obstructed by objects or blinded by lighting at night. Improper commissioning caused excessive invalid alerts with video analytics when viewing an area that included frequent motion under normal circumstances (e.g., a jogging path or busy street).

LESSON LEARNED HIGHLIGHT

Many ESM alerts are triggered by individuals with no intention of contaminating the water, such as utility personnel or intruders there to steal copper. Thus, it is valuable to locate video equipment to allow investigators to determine if water was tampered with.

Motion sensors may not be sustainable in some locations. The benefits of motion sensors must be weighed carefully against the drawbacks of potential nuisance alerts. One pilot found that the detection zone of ladder motion sensors drifted downward over time, and people walking under the ladder eventually caused alerts. This same utility also had a motion sensor that generated a significant number of invalid alerts caused by vehicles on a nearby roadway. Another pilot received feedback from local law enforcement during a drill debriefing that motion sensors tended to be prone to invalid alerts. Based on this input and other implementation issues, the utility replaced their ladder motion sensors with ladder guards and hatches that were monitored by hatch sensors.

Involve video analytics vendors early in the process. The video analytics vendor provided input to ensure that the areas monitored by their system were well-suited for their detection algorithm. This also allowed designers to select other intrusion detection methods for areas where video analytics could not be used effectively. Making these decisions at the design stage reduced invalid alerts and saved considerable labor and cost during system implementation and start-up.

Consider allowing remote access to the video analytics system. The pilots found that video analytics system commissioning and troubleshooting required multiple iterations with the vendors to adjust the configuration and achieve acceptable performance. Remote access to the video analytics system minimized effort and costs by reducing vendor travel expenses. One pilot's video analytics vendor was reluctant to travel to the utility beyond their budgeted number of site visits. This pilot was not able to provide remote access to the video analytics vendor, resulting in a prolonged commissioning effort during which a higher-than-expected frequency of invalid alerts was generated. Remote access should be discussed early in the design process with the IT department to identify a viable solution that is consistent with the utility's cybersecurity policies.

Alert Investigation

Collaboration with internal and external partners may require more time than anticipated. Pilots recommended including adequate time in the project schedule for meetings and document review when developing materials that involve external agencies (e.g., training materials, communications plans, policies, and procedures). It is important for all stakeholders to work together to form a consistent communication approach when investigating alerts.

Training videos of utility facilities were useful for engaging law enforcement. In addition to the operational benefit of improving law enforcement officers' knowledge of water security, this collaborative effort by one of the pilots and their police department strengthened their strategic relationship at the management level. The training videos were well-received, and the police districts and police academy currently use these videos in their ongoing training cycles.

Drills with law enforcement can strengthen relationships and yield valuable feedback. ESM drills involving local law enforcement built a stronger relationship between the utility and police. Collaboration during the planning stages of a drill allowed management from both organizations to interact and work toward a common goal. Feedback from local law enforcement shared during drill debriefings was insightful. In one case, the pilot implemented changes to their procedures and ESM equipment to incorporate suggestions from participating law enforcement officers.

Routine interaction with law enforcement is mutually beneficial. Three pilots joined their city's Fusion Center, routinely staffed the city's emergency operation center, or had law enforcement assigned to the utility. They found individual accountability to be an excellent means of building relationships with local and federal law enforcement agencies.

5.3 Summary of Pilot Experiences with ESM

All pilots have noted the value of improved communication and coordination with law enforcement that was established during development and exercising of ESM alert investigation procedures. Relationships and information sharing were strengthened, which improved overall readiness for responding to any security incident. Another benefit of ESM experienced by the pilots has been improved system security, particularly through the addition of video monitoring. This enhancement provides real-time awareness of site conditions and reduces the number of time-consuming on-site investigations conducted in response to invalid alerts.

One challenge encountered by the pilots as they continue to operate ESM is the need to consider rapidly evolving technology, particularly for motion and video surveillance. They must consider how the potential benefits of new technology compare with the costs. While few significant modifications have been made since initial implementation, one utility has hired a security manager and another is integrating their ESM system with their previous security system so that all sites can be monitored from the same user interface.

Since the conclusion of the pilots, the utilities have maintained the equipment and relationships developed as part of ESM, and two utilities have added additional ESM sites. The utilities maintain a security culture and foster relationships with local law enforcement.

Section 6: Customer Complaint Surveillance

Customer Complaint Surveillance (CCS) monitors water quality complaint data in call and work management processes to identify abnormally high volumes or spatial clustering of complaints that may be indicative of deteriorating water quality and potential contamination incidents. This section is organized by the CCS design elements listed in **Table 6-1**. Data communications and data management are also critical elements and are discussed in the context of an integrated CWS in Section 3.

Table 6-1. CCS Design Elements

Design Element	Description
Comprehensive Complaint Collection	A "funnel" for directing all water quality complaints into a central management system.
Alert Generation and Investigation	Systems and procedures for analyzing customer complaints, generating alerts when thresholds are exceeded, and investigating the alerts.

6.1 Comprehensive Complaint Collection

The comprehensive complaint collection design element consists of three sub-elements: communicating water quality concerns, consolidating water quality complaints, and defining complaint categories.

6.1.1 Summary of Implementation Approaches

Communicating Water Quality Concerns

CCS relies on communication from utility customers about indicators of potential contamination, particularly unusual taste, odor, or appearance. The effectiveness of this component requires that customers know how to report concerns about their drinking water quality to their drinking water utility.

Four pilots relied on existing business processes and customer education efforts to communicate water quality concerns. Only one pilot undertook new efforts to improve communication of water quality concerns. A phased, multi-channel advertising campaign was implemented that included printed information in local and neighborhood newspapers, internet advertising, billboards (as shown to the right), bus wraps, television commercials, and on-street information distribution tents. The primary intent was to inform customers that water quality concerns could be reported by calling 311.

After the public outreach campaign was initiated, the utility saw an increase in the number of calls to the 311 call center each month. Because implementation of the outreach campaign was phased (e.g., only print and online advertising was implemented in the first stage), the utility could measure the effectiveness of each advertising type. The utility initially experienced no increase in calls following the print and online ads. However, calls increased with each subsequent advertising method implemented, with television being the most effective medium for reaching its customers.

Consolidating Water Quality Complaints

Comprehensive complaint collection ensured that all complaints were effectively documented and available for analysis in a timely manner. While two pilots determined their existing process using 311 systems was adequate, three pilots implemented new strategies for consolidating water quality complaints. The approaches are presented below.

- *Consolidating communication options*: One pilot phased out all numbers previously used to report complaints and directed all customers to use the 311 number. Customer Service Representatives (CSRs) then used a web-based form to enter customer complaint information. Another pilot was losing water quality calls to the city call center. To address these lost calls, the utility implemented a procedure that allowed the city call center to transfer water quality calls to the front of the utility call center queue.
- *Updating work management systems*: Two pilots implemented new work management systems to ensure customer complaint calls could be successfully received and documented at a single call-handling facility. The updated systems allowed for documenting follow up on customer water quality concerns and streamlined procedures for the consistent handling of water quality customer complaints.
- *Implementing revised procedures*: All pilots held training for call center operators and water quality personnel, ensuring they understood and consistently applied procedures for triaging calls and entering data. The pilots that upgraded their work management system provided training on its use.

Complaint Descriptions and Categories

Precise water quality complaint categories were developed to support alert investigations and allow event detection systems to be configured to focus on complaints potentially indicative of water contamination. One pilot held a workshop specifically to discuss new water quality categories and alert thresholds for each category because it lacked preexisting categorization. The other pilots leveraged existing complaint categories.

IMPLEMENTATION HIGHLIGHT

One pilot allowed customers to self-classify their water quality complaint when they called through an Interactive Voice Response system.

There are no industry standards for customer complaint categories. Each pilot identified their own unique categories, using vernacular they were comfortable with and replacing the technical terms with more common descriptions. To support data analysis and alerting, the categories were arranged into 'tiers' based on the potential severity of the condition that prompted the call. Use of such tiers allowed utilities to set different thresholds for each tier, with the lowest threshold assigned to tiers representing the most severe conditions. **Table 6-2** describes the tiers used by the pilots. The final column gives example sub-categories that the pilots used to further classify the complaints. More detailed categories were used for common issues (e.g., rusty water, air bubbles during cold weather).

Table 6-2. Water Quality Complaint Categories

Tier	General Description	Example Complaint Sub-categories
1	Illness	Illness
2	Taste and odor	Chlorine, chemical, bitter / metallic, musty / stale, sewer
3	Dirty water	Dirty, discolored
4	Other	Particles, oil / greasy, cloudy / milky, rusty / brown

Once developed, the categories were applied by CSRs as they entered information into the work management systems. CSRs were given key words for each category to help ensure the correct coding of complaints. Two utilities used in-house call centers, two used a 311 call center, and one used utility CSRs embedded within a 311 call center. Regardless of which type of call center was used, water quality calls were transferred to utility experts after the call was triaged and logged.

6.1.2 Summary of Lessons Learned

Communicating Water Quality Concerns

As noted in Section 6.1.1, only one pilot proactively sought to improve customer communication of water quality concerns. Specific lessons learned from its public outreach campaign included:

Use personnel trained in public communication. If possible, work with a team that is experienced in public outreach. The pilot was able to involve their internal Communications and Public Outreach Division. The Division was an invaluable asset during all phases of the project. Component teams did not have the experience or resources necessary to efficiently and effectively implement complex communication strategies, so using experienced professionals from outside of the component team was necessary.

Take advantage of free and low-cost advertising. The pilot posted notices on the utility website, utilized social media websites, and included the message in periodic newsletters (electronically or as a bill insert).

Be responsive to customer complaints. Timely and thorough response to customers' water quality concerns is necessary for customers to continue to report their concerns to a utility.

Consolidating Water Quality Complaints

A single point of contact for water quality-related complaints enhances customer service. Redistributing the responsibility for water quality complaints from various organizational groups to one entity made it easier to implement consistent protocols for assessing and responding to water quality issues. Customer service was enhanced by providing a consistent customer complaint reporting process within a single system.

Update data capture protocols to highlight water quality-related issues and document call details in a consistent manner. All pilots trained CSRs on new procedures to ensure that CSRs consistently provided customers with the appropriate response to their complaints. One utility created a thorough "Water Quality Body of Knowledge" consisting of training and reference material to educate CSRs on triaging water quality-related calls.

Complaint Descriptions and Categories

Use broad, meaningful categories for classifying water quality complaints. Customer-friendly taxonomy proved to be more useful than a list of technical terms for every possible type of complaint. For example, the taste tier was broadly viewed as a high priority for all pilots, second only to illness.

Free text entries are useful for capturing complaint details. In free entry fields, users enter their own text instead of choosing from a pre-defined list of selections. While this information was not helpful from a surveillance perspective because the automated algorithms used could not analyze this information, it was useful during CCS alert investigations and response to customer complaints.

6.2 Alert Generation and Investigation

The alert generation and investigation design element involves the implementation of systems and procedures to analyze CCS data and generate alerts when unusual conditions are detected. This design element consists of three sub-elements: automated event detection, developing thresholds, and alert investigation.

6.2.1 Summary of Implementation Approaches

Automated Event Detection

The pilots developed processes to identify when the frequency of similar water quality complaints surpassed an established threshold, likely indicating a significant change in water quality. Four of the five pilots used automated event detection as a means of detecting these occurrences. The other pilot developed procedures to manually track complaints as they were received, and regularly compare the total number of complaints to thresholds.

All four pilots that implemented automated event detection were able to analyze call data and configure thresholds on a single system that could accommodate all monitored datastreams (e.g., call or work management systems). These pilots also incorporated automated daily call summary reports, event notification, and mapping to routinely monitor customer complaints. Four pilots used a rolling time window for analysis, such as the previous 24 hours from the current time.

Three pilots received alerts based on spatial clustering analysis and applied separate algorithms to unique hydraulic or administrative units such as zip codes or distribution system pressure zones. One pilot used an algorithm to scan for active work orders using a fixed radius around each complaint, which was useful to the investigation of distribution system work as a potential cause of complaints. Another pilot applied their algorithms to "mega-pressure zones," where common source water was the overarching factor for determining the likelihood of contamination to a specific population. Within each mega-pressure zone, separate thresholds were set such that alerts could be associated with a common source water. The two pilots that did not automatically analyze data within spatial units instead used GIS manually to investigate the spatial relationship among complaints.

Developing Thresholds

Different thresholds were used for different complaint categories, such as those listed in Table 6-2. In general, the pilots used a low threshold for the illness complaint type category. The pilots utilized a variety of approaches to establish the thresholds. Four pilots analyzed historical data to establish thresholds, while the final pilot elected not to analyze historical data but instead relied on professional judgment to identify unusual water quality complaint clusters.

Statistical methods utilized by pilots include analysis of variance (ANOVA) with the Kruskal-Wallis test and standard deviation. Another pilot used the *Alarm Estimation Tool* (AET) developed by EPA. This tool was developed specifically for CCS and uses historical complaint data to predict alert frequency at different threshold settings. The tool output was then used as guidance for targeting appropriate thresholds to avoid invalid alerts but maintain the sensitivity necessary to detect a valid contamination incident. Two other pilots used a similar level-of-effort method where the utility developed thresholds based on a reasonable number of expected investigations in a given period of time.

Alert Investigation

Section 3 describes general aspects of alert investigation procedures developed for the pilots that are applicable to all four surveillance components of a CWS. For example, all pilots held classroom training, tabletop exercises, and drills to train personnel on their roles and responsibilities. This section provides additional details about the approach taken by the pilots to implement CCS alert investigation procedures.

All pilots developed CCS investigation procedures, which included information sharing with personnel outside of the CCS team. This allowed for improved communication and alert investigation, should the investigation evolve beyond CCS. One pilot created a utility-wide assessment team that was sent all text and email alerts for review, even if it was anticipated that the assessment team would not be needed for the investigation. Similarly, another pilot utilized an on-call water quality engineer who was informed of all CCS alerts to ensure the assessment of all information from all components. This notification took place even if the cause of the CCS alert was known.

6.2.2 Summary of Lessons Learned

Event Detection Algorithms

Multiple algorithms may overlap, creating duplicate alerts. One pilot realized that many of the automated spatial algorithms overlapped. For example, three alerts were generated based on the same set of calls for algorithms that scanned for clustering at the zip code, community and city-wide levels. Generation of multiple alerts from the same customer complaints created an unnecessary burden on utility personnel conducting investigation procedures. Adjustments were made to use fewer algorithms.

Developing Thresholds

Alert frequency may deviate from expectations. The pilot that used the AET for estimating alert frequency anticipated that they would receive approximately nine alerts for any three-month time period. The actual number of alerts was 15 for the first month of operation, 15 total for the next three months, and 14 for the following month. This was a total of 44 for the first five months of CCS operation. The AET did not perfectly match expectations; however, the results of the actual alert frequency were at a rate where only minor adjustments to alerting criteria were needed to lower the alert occurrence rate to a more reasonable range. Other pilots also had to adjust their thresholds after implementation.

Do not assume all spatial areas should have the same threshold. Three pilots found that complaint rates differ across spatial units, and that a single threshold applied to all areas was overly conservative, resulting in a high occurrence of invalid alerts. These pilots subsequently implemented unique thresholds for each spatial unit.

Tracking and analysis of customer complaints improves the understanding of distribution system operations and water quality issues. Three pilots reported that personnel were able to match a change in complaint volume to locations of distribution system activities, such as hydrant flushing and main breaks, using the CWS dashboard. This improved understanding of the impact of distribution system work activities on customer perceptions of water quality improved customer service.

Alert Investigation

Provide alert details to multiple teams or personnel. The timeliness and thoroughness of investigations was improved by providing alert information to multiple teams of trained utility personnel. All pilots ultimately developed and implemented a tiered approach to alert investigations, with water quality experts investigating the alerts after CSRs triaged and filtered out any benign causes of a complaint.

Limit personnel access based on investigation role. Building distinct access levels into a configurable dashboard was recognized as a best practice leading to efficient CCS investigations. When trained personnel were given the precise information they needed to investigate alerts, rather than all possible information available to the utility, the investigation times were decreased.

Include information relevant to investigations in email notifications. Investigators were able to quickly rule out invalid alerts when complaint details such as locations and descriptions of the complaints were transmitted with the alert.

6.3 Summary of Pilot Experiences with CCS

In general, the pilots have found CCS to be the most cost-effective CWS component. It does not require new equipment, and the systems and procedures developed fully support efficient and effective customer service in general. Consolidation of information into one system has streamlined information flow and investigation procedures. Development of complaint categories allows for quick, precise, and consistent information to be captured for each call received. And the alert investigation procedures developed for CCS result in improvements to procedures for processing normal complaints, allowing for more timely and effective response to customer calls.

Relatively few modifications to the initial design have been required to make CCS effective and sustainable. The most common changes have been adjusting the thresholds used for event detection and eliminating redundant algorithms. These changes have resulted in fewer invalid and redundant alerts.

Section 7: Public Health Surveillance

Public Health Surveillance (PHS) serves two essential roles in a CWS: (1) analyzing public health data to identify patterns or changes in the health status of a community that may be indicative of waterborne illness and (2) optimizing communication and coordination between public health partners and water utility personnel who are responsible for monitoring public health datastreams and investigating alerts. The three main public health partners that have a role in PHS include the health department, Poison Control Centers (PCCs), and healthcare professionals (including infection control practitioners, physicians, nurses, pharmacists, and emergency responders).

This section is organized by the PHS design elements listed in **Table 7-1**. Data management is also an important PHS design element and is discussed in the context of an integrated CWS in Section 3.

Table 7-1. PHS Design Elements

Design Element	Description
Communication and Coordination	Relationships between public health partners and water utility personnel with a role in a CWS and a mutual understanding of each organization's capabilities.
Public Health Datastreams	Routine monitoring of public health datastreams for indicators of possible exposure to contaminated drinking water. This includes case-based surveillance that relies on direct observations by healthcare professionals and syndromic surveillance that monitors indirect indicators of illness in the population.
Alert Generation and Investigation	The tools used to generate PHS alerts and the procedures used by public health partners and water utility personnel to investigate alerts.

7.1 Communication and Coordination

The communication and coordination design element involves strengthening the relationships between a water utility and its public health partners. This includes clearly defining roles and responsibilities during routine monitoring of public health data and during investigation of PHS alerts that indicate possible drinking water contamination. Effective communication and collaboration with public health partners was critical for the success of the component, as investigation and interpretation of public health data was outside the core competency of utility personnel.

7.1.1 Summary of Implementation Approaches

The manner in which the pilots approached this design element depended on their existing relationships with public health partners. The utilities also considered the structure and jurisdictions of various public health partners, which impacted the number of agencies that needed to be engaged in order to provide adequate coverage of their distribution system.

The pilots implemented a variety of strategies to improve communication and coordination with and among the public health partners, as presented below:

- *Identifying public health partners and scheduling kick-off meetings*: All of the pilots held kick-off meetings with public health partners within their respective service areas to convey the goals of the CWS, assess the partners' existing capabilities (e.g., datastreams currently being monitored), and determine the partners' willingness to support design and implementation of the component. **Table 7-2** presents a summary of public health partners that were engaged by the pilots. An outcome of these meetings was to establish the core partners that would be involved in the project. Subsequently, collective decision-making among the partners was used to identify gaps in PHS capabilities and select enhancements that were mutually beneficial to the pilots and their public health partners.

Table 7-2. Public Health Partners Engaged for PHS

Partner	Number of Pilots
Health department (city or county)	5
Poison Control Center	3
Healthcare professionals[1]	1
Fire Department	2
Pharmacy retailers	1

[1] The remaining four pilots indirectly engaged healthcare professionals through the health department.

- *Convening routine meetings*: Two of the pilots used routine workgroups or meetings to improve communication with public health partners. One pilot established a Public Health User's Group, which included representatives from the utility and public health partners (e.g., city and county health departments, fire department, PCC, and Federal Bureau of Investigation field office) in order to coordinate efforts across all entities. Regular meetings provided a forum to discuss issues related to the CWS and issues that impact both the public health community and the utility. In another pilot, health department representatives were invited to participate in the utility's Water Quality Committee, which meets on a regular basis to proactively identify issues, develop non-emergency materials for use by the utility's public affairs division, and develop documents which include provisions for risk communication and public notification.
- *Conducting stakeholder outreach*: In one pilot, the health department conducted activities to build upon existing regional health partnerships for the purposes of enhancing capabilities to detect and respond to water contamination incidents. One of these efforts involved recruiting public health and emergency response agencies that have a role in the CWS to participate in an existing workgroup focused on public health emergency planning for regional response and resource sharing during a water contamination incident. The group collaboratively established a regional framework for communication, notification and post-incident activities. The health department also delivered presentations to raise awareness about PHS to healthcare professionals and emergency planners in order to improve awareness of indicators of drinking water contamination.
- *Increasing awareness of public health partner capabilities*: One pilot collaborated with the local PCC and gained an increased familiarity with the extensive toxicological knowledge offered by specialists responsible for handling calls at the PCC. Drills and exercises conducted during the pilot demonstrated the value that this specialized knowledge could bring to the investigation of a possible contamination incident, particularly the ability of PCC personnel to deduce probable contaminants based on reported symptoms.

7.1.2 Summary of Lessons Learned

Leverage preexisting joint utility and public health projects to strengthen relationships. Prior to building PHS, several of the pilots had already implemented joint projects with public health partners, including collaboration to investigate and combat *Legionella* outbreaks or to monitor gastrointestinal illness occurrence as part of a utility's filtration avoidance requirements. These collaborations provided a well-established foundation for the interagency coordination necessary for PHS.

LESSON LEARNED HIGHLIGHT

Forming relationships with public health partners can provide access to established PHS capabilities that can be leveraged for detection of possible water contamination.

Increase the awareness of public health partners regarding routine utility practices. Relationships that were formed or strengthened through the pilots provided public health partners with a greater understanding of utility operations. This knowledge allowed the public health partners to understand specific information (e.g., field or laboratory testing results or customer water quality complaints) that can be provided by the utility that may be useful to an ongoing public health investigation.

Develop a strategy to maintain relationships with public health partners. Fostering relationships with public health partners during non-emergency times is important for effective collaboration between the utility and public health partners during response to a possible water contamination incident.

Formalize communication procedures. All of the pilots reported improved working relationships with their public health partners as a result of documenting PHS communication procedures.

7.2 Public Health Datastreams

This design element describes the approaches taken by the pilots to evaluate and implement public health datastreams to improve monitoring of public health data for indicators of possible water contamination. These datastreams include 911 calls, Emergency Medical Services (EMS) runs, PCC calls, emergency department (ED) cases, over-the-counter (OTC) medication sales, surveillance of communicable diseases, clinical laboratory test results, and nursing home surveillance.

7.2.1 Summary of Implementation Approaches

To determine which public health datastreams to incorporate into PHS, each of the pilots first considered the potential of existing public health datastreams to detect possible water contamination. In the case of syndromic surveillance, this assessment also required identification of the subset of syndromes that would be monitored as indicators of possible water contamination. Datastreams were also evaluated with respect to contaminant coverage, considering contaminants with either rapid or delayed symptom onset. Another consideration was the timeliness of information flow from data sources to the surveillance system, which could range from minutes to days. For datastreams that were limited to a jurisdictional boundary that did not cover the entire distribution system area, the percentage of the population captured by the datastream was estimated. Finally, the completeness and accuracy of the data delivered to the surveillance system was assessed.

All of the pilots also considered adding new public health datastreams to address gaps in monitoring and surveillance capabilities. Assessment of new datastreams included all of the factors considered for existing systems as well as: (1) the willingness of the data provider to participate in PHS and supply data for analysis on an ongoing basis, (2) the cost to build or purchase software necessary to implement the surveillance system, (3) the availability of personnel with appropriate expertise to monitor a new datastream and interpret the data, and (4) the availability of technical personnel to maintain the system.

Prior to the CWS project, there was significant variability among the five pilots with respect to PHS capabilities. Public health partners associated with three of the pilots had capability to monitor ED data. Furthermore, those partners associated with two of the pilots had overlapping surveillance capabilities through the use of a variety of tools to monitor multiple public health datastreams. In general, pilots with limited preexisting PHS capabilities incorporated new datastreams, whereas those with existing, mature PHS capabilities chose to optimize existing systems.

Only two pilots implemented surveillance of new public health datastreams (911 calls, EMS runs, PCC calls, and ED cases) to: (1) increase coverage of contaminants producing rapid symptom onset or (2) receive data that was more timely, such as 911 and EMS. For these new datastreams, data was delivered to end users through a variety of methods, such as a dedicated PHS user interface, email notifications, or alerts displayed on the CWS dashboard.

The remaining pilots chose to enhance existing PHS capabilities through the following implementation approaches:

- Two pilots optimized information flow from data sources to surveillance systems for the ED datastream by upgrading an existing data management system or purchasing a new data management system. This upgrade also improved data collection, automated and improved data analysis, and allowed for remote user access via a Web portal.
- Two pilots updated the automated event detection system for ED data to include new water-related syndromes (e.g., adding logic to detect gastrointestinal, rash, or neurological symptoms).
- One pilot combined surveillance systems for two previously separate datastreams (OTC medication sales and anti-diarrheal medication sales) to provide better geographic coverage and to reduce the level of effort required to monitor these datastreams.
- One pilot implemented statistical methods (e.g., analysis of call volume) and non-statistical surveillance methods (e.g., keyword match searches) at their PCC to improve capabilities for identifying cases of possible water contamination.
- Three pilots incorporated public health datastreams (ED cases or OTC medication sales) into their CWS dashboard to allow overlay of alert locations on utility pressure zones.
- Four pilots improved spatial display of data through enhancement of existing user interfaces.

Table 7-3 provides a summary of the number of pilots that incorporated either new or existing public health datastreams into PHS, those that made the data available to the utilities, and those that incorporated the data into the CWS dashboard. Any public health data that was provided to the utilities was de-identified to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and was filtered to provide information that would be meaningful and useful, particularly for cross-component investigations involving temporal and spatial comparison of multiple datastreams. For example, while HIPAA restricts release of patient addresses, patient zip codes could be provided.

Table 7-3. Number of Pilots that Incorporated Public Health Datastreams into PHS

Datastream	Incorporated Datastream into PHS	Provided Data to Utility	Data Included in CWS Dashboard
911 calls	1	1	-
EMS runs	1	1	-
ED cases	4	3	3
PCC calls	1	1	-
OTC medication sales	1	1	1
Communicable disease reporting	1	1	1
Clinical laboratory monitoring	1	-	-
Nursing home surveillance	1	-	-

7.2.2 Summary of Lessons Learned

Selecting Public Health Datastreams

The ED cases datastream is valuable and reliable. Pilots characterized the ED datastream as providing reliable data, informed by assessments conducted by healthcare professionals, which can be readily interpreted during investigation of an alert.

The PCC calls datastream adds depth to PHS and can be easily implemented. One pilot incorporated this datastream into PHS and found that the toxicological expertise of PCC specialists was a highly reliable surveillance technique. These specialists were trained to consider water contamination when handling poisoning calls where the source of exposure was uncertain, which enhanced the capability to detect contaminants producing rapid symptom onset.

Balance timeliness of public health data against the amount of case detail included in an alert. Some types of public health data, such as 911 calls or EMS runs, can be available for analysis soon after data is generated. However, pilots that implemented these timely datastreams found them to be less useful than the ED or PCC datastreams because the level of case detail for 911 and EMS is limited and requires more effort to interpret when investigating an alert.

Integrate public health datastreams that support multiple goals. Public health datastreams that offered benefits to the utility and public health partners beyond detection of contaminated water were incorporated into PHS. For example, the public health department involved in one pilot used the data generated by new and existing surveillance systems for injury surveillance.

LESSON LEARNED HIGHLIGHT

The OTC medication sales datastream presented several challenges. Some pharmacies were concerned about proprietary business information and there was often incomplete participation by enrolled stores. Also, unknown factors can dramatically impact OTC medication sales such as promotional sales.

Consider the impact of resource limitations on the sustainability of potential public health datastreams. Some of the pilots noted challenges which prevented implementation of new public health datastreams, including limited availability of key personnel, limited funding, competing priorities within health departments and data providers, and data use restrictions. If a new public health datastream is incorporated into PHS, it will likely be the responsibility of the public health partner to maintain the surveillance capability.

Providing Data Access and Management

Address data sharing limitations when evaluating potential datastreams. Data sharing must comply with all HIPAA requirements. Utility personnel should be aware of the HIPAA requirements when using PHS data, including the limitations that these requirements place on the granularity of spatial data provided through the PHS system.

Be aware of state laws which limit access to public health data. Some pilots were unable to integrate public health datastreams based on state laws that restrict access to certain public health datastreams (e.g., 911 calls).

Maintain open communication with data providers. The success of PHS depends on the ability to collect the necessary information from local health departments and other data providers. To foster continued involvement, it is important to regularly communicate to the partners that provide PHS source data (e.g., fire department for 911 data and hospitals for ED data) the importance of their role in the component.

7.3 Alert Generation and Investigation

The alert generation and investigation design element involves implementation of systems and procedures to analyze PHS datastreams, generate alerts when unusual conditions are detected, and investigate those alerts in a timely manner.

7.3.1 Summary of Implementation Approaches

Alert Generation

Pilots started by evaluating data analysis and alert generation systems already in use by public health partners. If existing systems were found to be inadequate to meet CWS goals and objectives, the cost and level of effort to enhance an existing system or implement a new system were assessed. The pilots also considered the ability of the data analysis approach to provide a linkage to the case details (such as symptoms and demographic information) that would be needed for alert investigations. Finally, a method for providing alert notifications and details to designated personnel was identified or developed.

In most cases, pilots leveraged existing systems that employed statistical methods to analyze public health data and generate alerts when anomalies were detected. **Table 7-4** provides an overview of the public health datastreams along with the algorithms or analysis methods that were used by the pilots. The four data types analyzed by these tools included incident codes, syndrome, keyword, and medication sales. Datastreams were analyzed using tools such as SaTScan™, EARS, ESSENCE, and EpiCenter.

Table 7-4. Overview of PHS Datastreams and Analysis Tools

Datastream	Data Type	Analysis Tool	Analysis Methods
911 calls	Incident codes	SaTScan	Space-time statistical models
EMS runs	Syndrome	CDC EARS[1], ESSENCE[2]	Temporal statistical models
ED cases	Syndrome	EpiCenter, ESSENCE, SaTScan	Space-time statistical models, temporal statistical models, cumulative sum method, geographic clustering
PCC calls	Syndrome, keyword	National Poison Data System	Statistical methods and keyword searches
OTC medication sales	Medication sales	SAS[3], CDC EARS	Temporal statistical models, cumulative sum method, regressions to remove seasonal and day-of-week trends

[1] Centers for Disease Control, Early Aberration Reporting System
[2] Electronic Surveillance System for the Early Notification of Community-based Epidemics
[3] Statistical Analysis System

Methods used by the pilots to provide PHS alert notifications to users included email, web portals, or display on a CWS dashboard. Generally, alerts contained aggregated data from the case records associated with the alert (e.g., syndrome, age of patient, and location). Two pilots implemented new, automated methods for analysis of public health datastreams.

Alert Investigation

Section 3 describes general aspects of alert investigation procedures developed for the pilots that are applicable to all four surveillance components of a CWS. For example, all pilots held classroom training, tabletop exercises, and drills to train personnel on their roles and responsibilities. This section provides additional details about the approach taken by the pilots to implement PHS alert investigation procedures.

All of the pilots recognized the importance of investigating the relationship between PHS data and utility data during PHS alert investigations to identify possible correlations. Three pilots reviewed existing procedures, such as Cryptosporidium Action Plans, and communication plans to inform the development of PHS alert investigation procedures. An important consideration for PHS alert investigations was the decision regarding which entity (the utility or public health partners) would be responsible for initiating the investigation when an alert was generated. Four pilots assigned primary responsibility for initial alert investigations to the public health partners, and if water contamination could not be ruled out, public health partners would notify the utility to initiate a joint investigation. One pilot trained utility personnel to investigate all PHS alerts for possible correlations with the other component datastreams using the CWS dashboard. The health department would only be engaged when a correlation was identified that indicated the possibility of water contamination. This process was established to utilize the expertise of epidemiologists at the health department only when it was truly needed and minimized the burden of dealing with many "nuisance" alerts.

Two of the pilots also developed procedures for activating emergency notification and communications systems to support timely PHS alert investigations. These procedures involved activation of emergency auto-dialers that contacted utility and public health personnel with a message providing instructions for subsequent investigative activities, such as holding a conference call to share information. Both pilots tested and evaluated their communications systems during CWS drills and exercises. One of the pilots conducted routine tests of the emergency communications system to maintain proficiency with its use.

7.3.2 Summary of Lessons Learned

Alert Generation

Regularly review source data. Periodic review of the source data is important because circumstances of the data providers can change, impacting data completeness (e.g., hospital closures or expansions, pharmacy mergers or movement to electronic data reporting). Ideally, the owner of the surveillance system would conduct periodic reviews of the source data to ensure completeness, accuracy, and quality of the data.

Obtain precise location data for PHS alerts. All pilots noted the importance of mapping the location of a PHS alert and the underlying cases on a distribution system map in order to investigate clustering and the potential causal relationships with utility operations as might be evidenced through data from utility monitoring and maintenance activities. For some datastreams, only zip codes were available, which limited the ability to correlate to a precise location available from the other CWS components. One utility worked with their health agency to develop a way to report fuzzy locations, such as closest intersection, because HIPAA precluded exact patient location information from being released.

Consider the time delays associated with PHS alerts. The pilots noted the challenge of interpreting PHS alerts due to the time delay between utility data and PHS data. In particular, contaminants with delayed symptom onset may not generate a PHS alert until days or weeks after the contaminated water was in the distribution system. Thus, other CWS components, such as OWQM and CCS, could generate alerts much earlier than PHS under some scenarios.

Alert Investigation

Enhance collaborative decision-making. All pilots tested and evaluated investigation procedures during PHS drills and exercises and emphasized the importance of collaborative investigation of alerts. Collaboration among multiple agencies allowed for greater confidence in decision-making, especially when the investigation involved comparison and correlation of utility and public health data.

Use electronic tools to enhance information sharing. The pilots that incorporated either a web portal or a CWS dashboard that could be accessed by utility personnel and public health partners were able to share data much more rapidly. This facilitated the joint discussion of findings from the investigation of utility and public health datastreams and decreased the time needed to conduct a PHS alert investigation.

Understand the external factors that can generate PHS alerts. PHS alert investigations can be improved through an enhanced understanding of patterns in the datastreams. For example, seasonal events such as flu or excessive heat may cause an increase in PHS alerts unrelated to the quality of the drinking water.

Implement a process to access ancillary data during alert investigations. Metadata associated with the monitored datastream is often needed to interpret and fully investigate a PHS alert. In particular, the underlying case data (such as symptoms, location of exposure and patient demographics) is useful for investigating the potential cause of a PHS alert. Typically, public health partners, who have some exemptions from HIPAA, could obtain these case details from public health data providers.

Use live communications systems during alert investigations. Use of conference calls or other live communications systems allowed for the first-hand presentation of data to all partners resulting in faster analysis and more informative discussions during investigation of PHS alerts.

Test emergency communication. Drills and exercises provided an efficient method for evaluating and subsequently improving communication protocols. Routine tests of communications systems can provide an effective means of ensuring up-to-date contact information.

Emergency communications systems can serve a variety of purposes. Two of the pilots indicated that the emergency notification and communications systems established for PHS provided benefits beyond the CWS, as the protocols can be utilized for communication during non-drinking water emergencies.

7.4 Summary of Pilot Experiences with PHS

Two of the utilities already had strong and long-standing partnerships with their local health departments, and all five of the pilot utilities reported that newly established or improved relationships are highly valued and anticipated to be sustainable with minimal cost. The improved communication allows for an increased awareness of partners' abilities and organizational structures. Furthermore, the pilots recognize that communication and collective decision-making procedures developed and practiced during drills and exercises can be applied during a variety of public health emergencies (e.g., natural disasters, pandemic influenza, or non-water related terrorist attacks).

However, several pilots have noted that PHS can be challenging to maintain. PHS relies heavily on public health partners, both to monitor public health datastreams and to provide the specialized knowledge necessary to interpret this data. These partners may find it difficult to allocate time and resources to PHS over the long term unless the component has been designed to provide value to their routine job duties or other public health initiatives. For example, datastreams monitored for PHS could be utilized to conduct other types of disease surveillance.

The most significant change the pilots have made to their PHS systems has been to eliminate datastreams that provide marginal value. One pilot has discontinued monitoring of OTC medication sales due to the unreliability of data reporting from pharmacies. In another pilot, the 911 and EMS datastreams have been repurposed as a resource for the investigation of alerts rather than as primary detection streams because the 911 and EMS datastreams are considered less reliable than ED and PCC datastreams. In the end, all pilots find PHS to be sustainable, provided that their public health partners continue to participate.

Section 8: Consequence Management

Consequence Management (CM) consists of actions taken to investigate, respond to, and recover from possible drinking water contamination incidents detected through the CWS surveillance components. These procedures are documented in a Consequence Management Plan (CMP) and a Risk Communication Plan (RCP). The CMP outlines roles and responsibilities, notification protocols, and response procedures. The RCP documents a process for providing appropriate and useful information to the public and stakeholders in an effective manner. This section is organized by the CM design elements listed in **Table 8-1**.

Table 8-1. CM Design Elements

Design Element	Description
Response Partner Networks	Identifying and creating relationships with local, state, and federal agencies that may become involved in the response to water contamination.
Incident Response Procedures	Developing a step-wise framework that guides investigation, response, and risk communication activities during an incident.
Communication Equipment and Methods	Identifying equipment and establishing methods for communication among response partners during incident response.

8.1 Response Partner Network

A response partner network facilitates coordination between a utility and its response partners so they can effectively and efficiently execute their responsibilities during a water contamination incident. For all of the pilots, the response partner network included utility, local, state, regional, and federal partners.

8.1.1 Summary of Implementation Approaches

Prior to the start of the pilot program, all utilities had response partner networks in place to address and respond to incidents such as natural disasters and public health emergencies. As part of CM implementation, these were enhanced to improve understanding of partner roles and responsibilities during suspected or confirmed water contamination incidents. Common partners and their responsibilities are summarized in **Table 8-2**.

Table 8-2. Common Response Partners and their Scope of Responsibilities

Response Partner	Common Roles and Responsibilities
Federal, State and Local Regulatory Agencies	Supported investigative and response actions in a wide array of capacities such as data analysis, regulatory implementation, and public notification.
Local Government	Provided expertise and an operational understanding of emergency response capabilities within the water distribution service area.
Law Enforcement	Served as first responders when criminal activity was suspected.
Public Health Services	Provided expertise and resources related to the healthcare sector.
HazMat Response Units	Helped identify and remediate the hazardous materials and supported site characterization activities in potentially hazardous field environments.
Laboratory Partners	Provided analytical support for a variety of contaminants including chemical, radiological, and biological agents.
Emergency Management Agencies	Supported the response and recovery capabilities of first responders.

To streamline coordination between internal and external partners, several pilots designated a response coordinator. The coordinator served as a main point of contact for response planning, played an important role within the Incident Command System (ICS), and was typically responsible for maintaining the CMP and RCP. Additionally, response coordinators often acted as the lead facilitator in both internal and external training and exercises.

All pilots conducted multi-disciplinary training exercises to refine utility response plans (e.g., CMP and RCP), train all participants on their roles and responsibilities, and test and evaluate those plans. Response partner participation in these exercises aided in:

- Defining criteria for the notification of specific response partners in order to involve them at an appropriate phase of the investigation without placing an undue burden on their time. For example, one pilot's public health partners requested to be notified any time possible contamination was suspected. Other partners, such as HazMat crews, required notification only in cases where a site investigation required their unique skills.
- Outlining response partner communication procedures during each phase of the investigation and response process
- Clarifying utility and partner roles and responsibilities through the development of an ICS
- Testing incident response procedures to identify gaps in the response partner network

RESPONSE PARTNER NETWORK IMPLEMENTATION CASE STUDY

While all pilots conducted workshops with external response partners to clarify roles and responsibilities, one pilot classified partners based on their level of involvement in the CM threat level determination process. The following classifications were defined:

Active Responder: A response partner which partially or fully assumed a primary responsibility within the CMP. Active responders may be involved with decision making during an incident.

Active Support: A response partner that implemented its individual responsibilities to support the utility during response to an incident. For example, this could include providing relevant information to support the CM threat level determination process.

Passive Support: A response partner that has been notified of a possible contamination incident, but is not actively providing assistance. Passive support may become active support as the threat level escalates.

8.1.2 Summary of Lessons Learned

Designate a primary utility point-of-contact. Several pilots created an internal point of contact who served as a liaison between the utility and partner organizations. This improved both internal and external coordination by funneling communication through one person.

Clearly define each response partner's unique responsibilities. In some cases, the scope of a particular response partner overlapped with other partners and required additional clarification. Working sessions enhanced relationships and resulted in an improved operational understanding of each partner's unique role during investigation of and response to a water contamination incident.

Clearly define each response partner's ability to respond. The pilots found it necessary to clearly define and document each partner's business hours, availability to respond to emergencies during off-hours, and the time required for them to mobilize.

LESSON LEARNED HIGHLIGHT

One pilot found the toxicological expertise of PCC specialists to be extremely beneficial. During exercises, these specialists were able to narrow down the list of suspected contaminants based on patient symptoms, significantly expediting the threat level determination process.

Develop a well-defined internal process to review alerts before involving external partners. The pilots developed comprehensive procedures to ensure that response partners were notified only when a possible contamination incident had been detected and verified. This helped minimize the burden on response partners.

Consider methods to facilitate data sharing among partners. The format and types of data produced by external partners varied significantly. It was necessary to develop methods to share information in a format that was useful to all partners.

8.2 Incident Response Procedures

Incident response procedures serve a fundamental role within CM by formally documenting the steps required to respond to suspected drinking water contamination incidents in a comprehensive manner. The following section describes the development process, method of documentation, and content used for the CM incident response procedures, as well as training on these procedures.

8.2.1 Summary of Implementation Approaches

Incident Response Development Process

All pilots followed a similar process to develop and implement CM incident response procedures. All pilots completed a gap analysis, where existing plans were identified, reviewed, and evaluated to facilitate an understanding of current response capabilities and determine which components could be leveraged and improved upon in the CMP and RCP. Existing emergency response procedures and the *Interim Guidance on Developing Consequence Management Plans for Drinking Water Utilities* (EPA, 2008) served as the basis for the development or refinement of the CMP and RCP.

All pilots had an existing 'all-hazards' emergency response plan to respond to an array of potential emergencies which provided a foundation for CM incident response procedures. Also, all pilots had an existing ICS, which defined the roles and responsibilities of response personnel. The pilots updated and refined their ICS, with emphasis placed on clearly defining actions and responsibilities during specific threat levels in response to suspected drinking water contamination incidents.

IMPLEMENTATION HIGHLIGHT

Processes found within existing response plans that were frequently leveraged included provision of alternate water supplies, site characterization protocols, and risk communication procedures.

Although the degree of initial emergency response capabilities varied from pilot to pilot, all pilots invested resources to improve and standardize procedures. The level of effort required to develop CM procedures differed considerably among the pilots due to the varying degree of initial capabilities. One pilot had an existing CMP, and thus required only modest effort to refine their procedures. Pilots without an existing CMP spent more time developing their response procedures in collaboration with partners.

Documenting Incident Response Procedures

The development of an organized structure was necessary to outline the key components of the CMP and RCP. Documentation of these procedures included the following high-level topics, which are further described in this section.

- Roles and Responsibilities
- Detailed Procedures
- Training and Exercises
- Plan Maintenance
- Supplemental Materials such as checklists, flow diagrams, and sample notification messages

All pilots developed flow diagrams to depict processes documented in the CMP and RCP. In general, two formats were utilized, with generic examples of each provided in **Figure 8-1**. The most common format was a decision tree, in which key decisions and tasks were presented in a step-by-step manner and often represented as nodes. In the swim-lane format, procedures were organized based on the personnel or response partner responsible for the completion of each step, with one row for each role identified.

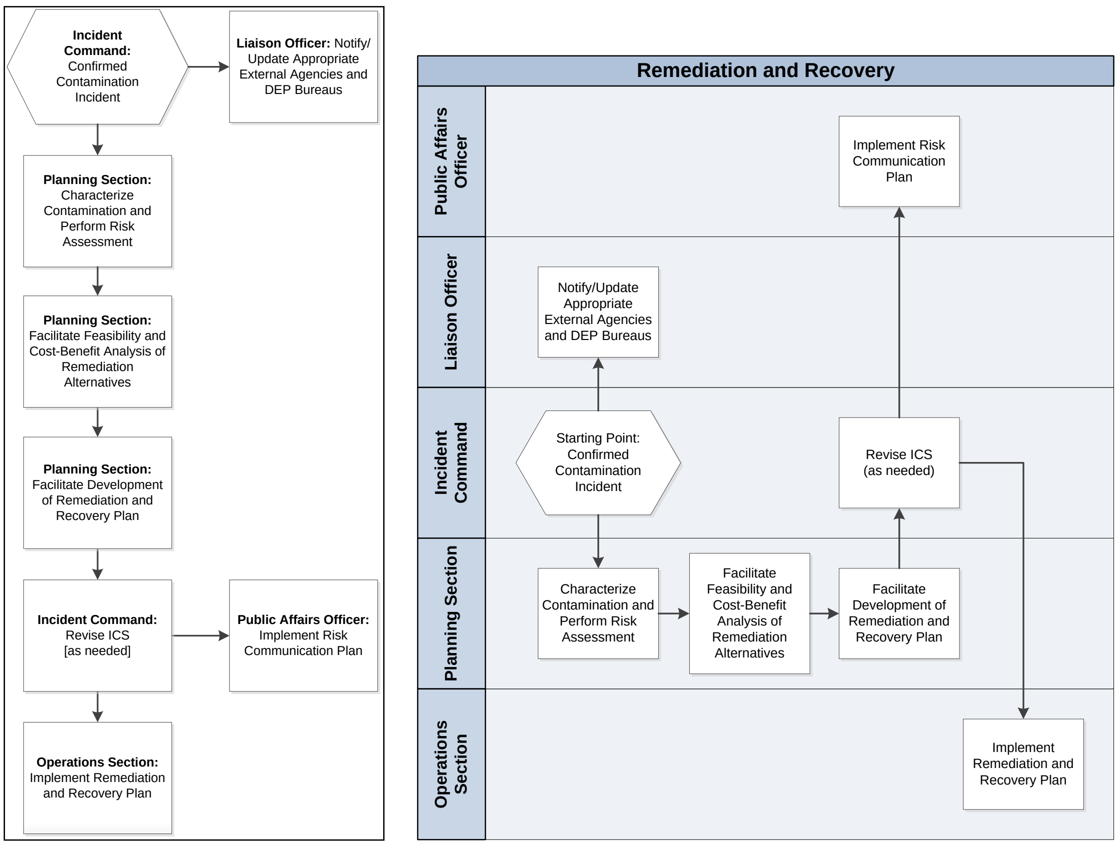

Figure 8-1. Examples of Decision Tree (Left) and Swim-Lane (Right) Process Flow Diagrams

To improve implementation of CM procedures and document activities, all pilots developed a series of checklists to be utilized in conjunction with process flow diagrams. These checklists provided step-by-step instructions for implementing the procedures graphically depicted in a corresponding process flow diagram.

CMP Content

Each of the pilot CMPs was structured in a progressive manner, outlining general utility and response partner roles and responsibilities before proceeding to investigation, response, and recovery processes. Key response procedures within the pilot CMPs included the following.

- *Internal utility response structure*: Specific roles and responsibilities for utility personnel for each threat level were typically presented in an ICS 'top-down' manner, progressing from command personnel to general positions.
- *External response partner structure*: External response partners' roles and responsibilities were typically classified based on their emergency support function and the threat level(s) in which they participated.
- *Incident investigation procedures*: Process-flow diagrams were incorporated to provide a graphical outline of key decision points, including a detailed summary of the steps and procedures to be completed at the possible, credible, and confirmed threat levels.
- *Operational response*: Methods to minimize the extent of contamination, such as isolation and flushing, were typically included.
- *Emergency resources and facilities*: Several pilots incorporated detailed information on the resources, facilities, and equipment available for use in the event of water contamination.
- *Public notification*: Several pilots included a brief summary of the public notification tasks to be completed at different threat levels; however, the RCP served as the main resource for communication procedures, as discussed in the next subsection.
- *Remediation and recovery*: Guidance on the steps and actions required to return to normal system operations were included. This section of the CMP generally included a description of the individuals, groups and resources potentially needed during this phase.

IMPLEMENTATION HIGHLIGHT

While component alert investigation procedures were generally completed before CM was initiated, one pilot incorporated alert investigation procedures directly into the CMP through use of an additional phase, denoted as "potential contamination."

INCIDENT CLASSIFICATION-EMERGENCY ACTION LEVEL CASE STUDY

While all pilots incorporated possible, credible and confirmed phases of the threat level determination process, two of them expanded upon this convention by developing additional descriptive phases known as Emergency Action Levels (EALs). EALs, also known as severity levels, were centered on response actions. For example, a credible incident that has potential health impacts will have a different EAL than a credible incident without potential health impacts. In this example, the EAL for the credible scenario *with* health impacts may require activating the City ICS, while the EAL for the scenario *without* health impacts might continue within the utility ICS.

RCP Content

The following implementation approaches and key procedures were found within all pilots' RCPs.

- *Roles and responsibilities of response personnel*: Primary roles within the incident communication process such as public information officers, communication advisors, public affairs specialists and spokespersons were described in detail. Tasks such as the development of situation-specific messages, organization of press conferences, maintenance of internal communication, and preparation of draft notification letters were assigned to specific individuals to ensure effective incident response. Roles and responsibilities for risk communication were integrated into the ICS.
- *Distribution of materials*: The process for distribution of risk communication materials was defined and included coordination with a variety of external response partners and mass media outlets. Communication procedures and public notification actions, if applicable, were defined for each threat level and common activities in the pilots' RCPs are highlighted in **Table 8-3**. Spreadsheets containing the name, position, and contact information for internal and external communication personnel were often developed to expedite the preparation and delivery of incident-related messages.

- *Templates*: All pilots incorporated pre-prepared communication documents, such as press releases, door hangers, public notification letters, and media statements within an appendix to the RCP. These templates streamlined communications during a water contamination incident.
- *Plan development and maintenance*: Policies and procedures were outlined to ensure that the RCP was continually updated to reflect changes in the contact information for key personnel, revisions to communication protocol, and modifications to notification templates.

Table 8-3. Common RCP Actions for a Specified Threat Level

Threat Level	Common RCP Actions
Possible Contamination	Mobilize internal communication personnel, review operational checklists for each threat level, and contact external response agencies to initiate a coordinated response
Credible Contamination	Continue to collect information on the contamination incident and commence preparation of communication materials such as public advisories and press releases
Confirmed Contamination	Continue to collect information on the contamination incident such as the specific areas affected and fully mobilize communication partners to review and finalize messages prior to release
Remediation and Recovery	Coordinate ongoing public notification to provide information on the status of the incident, guidance on use restrictions, sources of alternative water supplies, and progress on system remediation and recovery

Training and Exercises

A key aspect of developing and implementing incident response procedures involved training and exercises. First, discussion-based exercises were conducted by all the pilots to develop procedures, identify and include missing response partners, improve lines of communication, and educate utility and response partner personnel on the procedures. Several pilots also conducted specialized one-on-one training seminars for key individuals within the CMP and RCP response process, such as command personnel and public information officers.

All of the pilots followed their discussion-based exercises with operations-based exercises to test and comprehensively evaluate aspects of incident response procedures. Through the use of full-scale exercises, pilots were able to extract information on the operational performance of the CMP and RCP. Furthermore, familiarity with plans and procedures was readily assessed through use of these exercises. Performance metrics, such as the effectiveness of communications, timeliness of response actions, and accuracy of decisions, were evaluated. Revisions and updates were made to response procedures, as necessary, following each exercise.

In addition to utility-specific training, all pilots required key response personnel to complete FEMA's ICS training courses (FEMA, 2011). **Table 8-4** outlines the number and type of ICS trainings required across the pilots. Note that training requirements were based on responsibilities in the ICS and only key personnel were required to attend all of these courses.

Table 8-4. ICS Training Courses Required by the Pilots

Course ID	ICS-100	ICS-200	ICS-300	ICS-400	IS-700	IS-800
Number of Pilots Requiring this Course	5	4	3	3	5	3

8.2.2 Summary of Lessons Learned

Development of incident response procedures is an iterative process. The development and refinement of incident response procedures required collaboration among a diverse group of partners over an extended period of time. Multiple workshops, planning sessions, and exercises were completed with internal utility personnel and external response partners to evaluate response plans and identify areas requiring improvement. Lessons learned were identified after each exercise and incorporated into revisions to the response plans. This process was repeated until the response procedures were deemed complete and accurate.

Include a diverse group of personnel during development of incident response procedures. The pilots recognized that the creation and implementation of robust procedures required input from a wide variety of utility personnel and departments. Specifically, participation of executive-level personnel was critical to utility-wide acceptance of procedures.

Plan for sample analysis turnaround time. For some contaminants, the turnaround time to receive analysis results can be several days. This potential delay should be considered when developing procedures.

A "field-ready" version of the CMP was helpful for implementation of procedures. Upon conducting discussion-based and operations-based exercises, several pilots recognized the need for a more concise version of the CMP. A "field-ready" guide was better accepted by response personnel and resulted in improved performance during drills. Several pilots also observed that storing the CMP in a readily accessible location enhanced its utilization.

Conduct an end-to-end test of incident response procedures. Although completion of exercises required a significant commitment of resources, all pilots found the comprehensive end-to-end testing of procedures extremely valuable. Implementation of procedures through training and exercises yielded considerable improvements in personnel awareness and familiarity with incident response procedures.

LESSON LEARNED HIGHLIGHT

All pilots emphasized the importance of having well-defined protocols for updating incident response procedures. Typically, updates were completed based on the improvement plan resulting from a drill or exercise or a response to an actual incident.

Ensure that all communication personnel have an understanding of the RCP. Several pilots noted that a lack of familiarity with the RCP among utility communication personnel resulted in inconsistencies and deviations from established protocol. Meetings and refresher workshops were scheduled on a regular basis to review incident procedures and outline updates or changes to the RCP. Process-flow diagrams and checklists were included for easy use so that personnel better understood their roles throughout all phases of incident response.

Maintain up-to-date contact information for key personnel. During several exercises, inaccurate contact information for key individuals resulted in delayed press releases to the media. A schedule was developed to periodically review the information to maintain accuracy.

8.3 Communication Equipment and Methods

A variety of equipment and methods can be used to communicate information regarding a possible contamination incident, both within the utility and with external partners.

8.3.1 Summary of Implementation Approaches

Most pilots conducted a comprehensive inventory of existing communications equipment to assess the strengths and weaknesses in current communications technologies. Through the inventory process, utilities were able to categorize and improve the primary types of equipment utilized during both day-to-day and emergency-related operations.

All pilots implemented a series of communications system improvements to streamline incident response capabilities. These enhancements included the following.

- Several pilots replaced analog bandwidth radios with digital systems to expand the range of coverage.
- Two pilots purchased 800-MHz radios for key personnel within the ICS to provide a reliable and secure means of communication with response partners, such as law enforcement and HazMat response teams.
- Several pilots purchased rugged laptops and broadband cards to allow response personnel to rapidly transmit and receive information, particularly with field personnel.

In addition to the enhancements above, all five pilots implemented information management systems for sharing information during CM activities. Four pilots implemented dashboards, which are discussed in Section 3.2, and the other pilot set up a SharePoint site. These systems served as an important tool by keeping individuals informed of the status of investigation and response activities in real time. The systems also enabled all partners to remotely access information and rapidly exchange data, while assessing information from multiple datastreams concurrently.

All pilots had procedures for assembling personnel at a central operations center during an incident, which served as the primary location for internal and external communication. Some pilots leveraged an existing city-wide Emergency Operations Center (EOC) structure, which was utilized by a number of different municipal and emergency response partner agencies.

The amount and type of equipment in the utility operations center varied from pilot to pilot, though all were equipped with telecommunications systems, computers, and internet access. After conducting a review of the functionality of their operations center, one pilot implemented a number of significant improvements, including the addition of:

- A large LCD TV to display critical information
- Several landline telephone lines to allow for more robust communication, particularly during loss of cellular service
- Digital speaker phones to improve conference call performance

IMPLEMENTATION HIGHLIGHT

One pilot implemented a virtual EOC, which allowed most ICS personnel to remain at their workstations rather than gather in a central command center, giving them access to their resources and personnel. Communications were maintained through routine conference calls and a SharePoint site available through remote access.

8.3.2 Summary of Lessons Learned

Ensure equipment compatibility among response partners. After completing field exercises, several pilots identified significant gaps in communication due to incompatible systems. The gaps were addressed through focused upgrades.

Use of field equipment resulted in improved response times. The addition of 800-MHz radios, rugged laptops, and SharePoint or dashboard information exchange platforms resulted in enhanced operational efficiency by providing personnel with access to field data in real time.

8.4 Summary of Pilot Experiences with CM

The pilots have indicated improved emergency response capabilities as a result of implementation of CM. Working relationships between internal and external partners were developed and reinforced through participation in workshops, drills, and exercises. Additionally, training and exercises enhanced personnel awareness of emergency policies and the ICS, which improved the utility's response posture. By thoroughly testing emergency response capabilities through drills and exercises, pilots were able to identify shortcomings and areas of potential improvement.

The biggest challenge for CM has been the coordination required among utility departments and with external partners to maintain familiarity with response procedures. However, the partners that continue to participate in coordination activities have generally found the experiences to benefit their own state of preparedness. All pilots continue to actively maintain their response partner networks and CM procedures.

Section 9: Sampling and Analysis

Sampling and Analysis (S&A) involves the collection and analysis of water samples to confirm or rule-out contamination and is initiated in response to surveillance component alerts after the investigation has led to the conclusion that contamination is possible. All of the pilots developed detailed procedures for routine operation and response and enhanced field and laboratory capabilities. This section is organized by the S&A design elements listed in **Table 9-1**.

Table 9-1. S&A Design Elements

Design Element	Description
Field Capabilities	The equipment, supplies, quality assurance/quality control (QA/QC), and staffing for all activities that would be performed in the field in response to possible, credible, or confirmed water contamination incidents. This design element also involves planning with emergency response partners for contaminants or contamination scenarios that may require their support.
Laboratory Capabilities	The equipment, analytical methods, supplies, QA/QC, and staffing for all activities required to perform laboratory analyses in response to possible, credible, or confirmed water contamination incidents. This design element also involves planning with emergency response partners and laboratories for contaminants or contamination scenarios that may require their support.
Routine S&A	The process of establishing and maintaining baseline contaminant occurrence and method performance data for all pre-established methods that could be used during response to possible water contamination.
Response Procedures	Development and testing of response procedures for all field and laboratory methods and activities as well as procedures for internal and external notifications and communication.

All pilots worked to achieve broad contaminant coverage by incorporating field or laboratory methods to cover the majority of contaminant classes of concern to water security (**Table 9-2**). To determine their contaminant design basis, the pilots reviewed EPA's list of priority contaminants (EPA, 2013), which are contaminants that could cause significant public health or economic consequences, if introduced into the distribution system. Some pilots also reviewed other contaminant lists developed by water quality instrument vendors, water sector trade associations, and state laboratory networks or included contaminants of regional concern (accidental and natural contamination threats).

Table 9-2. Contaminant Classes of Concern to Water Security

Chemicals		Pathogens	Biotoxins	Radionuclides
• Carbamate pesticides • Organophosphate pesticides • Rodenticides • Herbicides • Fluorinated organic compounds • Mercury compounds	• Arsenic (III) compounds Heavy metal compounds • Cyanide compounds • Petroleum products • Persistent chlorinated organics • Chemical warfare agents • Pharmaceuticals	• Bacteria • Viruses • Protozoa • Rickettsia	• Animal toxins • Plant toxins • Bacterial toxins • Algal toxins • Fungal toxins	• Alpha emitters • Beta emitters • Beta + gamma emitters

9.1 Field Capabilities

Field capabilities consist of the sub-elements presented in **Table 9-3**, which are discussed in the following subsections.

Table 9-3. Field Capabilities Sub-Elements

Design Sub-Element	Description
Water Quality Parameter Testing	Test kits or instruments used to determine pH, disinfectant residual, conductivity, temperature, turbidity, and other water quality parameters in water samples that may reveal water quality anomalies when compared to baseline data.
Site Safety Screening	Visual hazard assessment to recognize hazardous situations and portable instruments used to detect site hazards, such as radiation and volatile or combustible gases.
Rapid Field Testing	Kits or instruments used to test water samples for general toxicity, specific contaminants or contaminant classes such as free cyanide, chemical warfare agents, arsenic, volatiles, and radiation screening.
Quality Assurance	Ensuring high quality data during field S&A by including a demonstration of capability and QA/QC for all pre-established field methods and by incorporating all field methods into the utility's QA/QC program.
Sample Collection	Preparation of sampling supplies for contaminants or contaminant classes that the utility or laboratory partners would analyze in response to possible contamination.
Field Staffing	Identification of personnel, training, cross-training, and development of contingency plans in the event that there are contamination scenarios for which the utility would require the support of emergency response partners such as HazMat or similarly qualified emergency response partners.
Field Safety	Planning for the health and safety of employees who may be involved in field response activities, including review of Health and Safety Plans to ensure they cover non-routine activities or sampling locations and development of safety precautions the utility would implement when responding to possible contamination when the contaminant has not yet been identified.

9.1.1 Summary of Implementation Approaches

The pilots used a combination of the following approaches to build the desired field testing capabilities for response S&A.

- *Utilized existing field test kits and instruments*: All pilots had some field test kits and instruments available in-house that were already being used routinely for compliance monitoring or for other ongoing S&A efforts. A review of these existing capabilities and the contaminant coverage they provided was an important initial step.
- *Purchased new field test kits or instruments*: All of the pilots identified gaps in their existing capabilities. When selecting new kits or instruments to fill these gaps for site safety screening and rapid field testing, the pilots relied upon information available on EPA's Environmental Technology Verification Program website and from manufacturers or vendors to evaluate factors such as test kit or instrument cost, sensitivity, reliability, potential interferences, false positive/false negative results, field portability, maintenance costs, shelf-life of reagents, and the time required for periodic personnel training.
- *Determined the capabilities of local HazMat units*: All pilots partnered with their local HazMat units to plan for contamination scenarios that involved the discovery of hazardous materials or indicators of hazardous materials. Pilots that chose to complement their local HazMat unit capabilities mostly invested in rapid field testing equipment and supplies specific for water samples that the HazMat unit did not have.

Water Quality Parameter Testing

The water quality parameter testing capabilities used by the pilots are summarized in **Table 9-4**. All of the pilots had existing capabilities to test water samples for pH, chlorine residual, conductivity, and turbidity prior to implementation of the CWS.

Table 9-4. Water Quality Parameter Testing

Parameter	Number of Pilots
pH	5
Disinfectant residual	5
Specific conductance	5
Turbidity	5
TOC	1
UV-Vis absorption	2
ORP	2
Dissolved oxygen	1

One utility performed basic water quality parameter testing in the field and transmitted the data using hand-held digital assistants. This allowed for near real-time transfer of water quality parameter data to the Laboratory Information Management Systems (LIMS) and CWS dashboard. Furthermore, a charting tool in the dashboard allowed easy access to additional data to determine whether an abnormal result at a given location was a one-time occurrence or part of a site specific or temporal trend.

Site Safety Screening and Rapid Field Testing

All pilots trained field sampling teams to conduct a visual inspection during site approach to identify hazardous materials or situations that might require HazMat response. In addition, all pilots implemented site safety screening capabilities (summarized in **Table 9-5**) by leveraging existing in-house instruments, identifying local HazMat capabilities, and purchasing new instruments to enhance existing capabilities.

Table 9-5. Site Safety Screening Performed by the Utility

Screening Type	Number of Pilots
Gas monitoring (multi-gas and volatile organic compounds)	4*
Ambient radiation	4*
Chemical warfare agents and industrial chemicals	1

* Also available through HazMat

Most pilots leveraged existing rapid field test kits or purchased new test kits and the resulting capabilities are summarized in **Table 9-6**. One pilot purchased a chemical warfare agent test kit but did not consider it sustainable because of the maintenance costs, the time required to maintain proficiency, and limited applicability beyond response S&A.

Table 9-6. Rapid Field Testing

Parameter	Number of Pilots
Cyanide	4
Arsenic	1
Volatile organic compounds (headspace)	2
Rapid acute toxicity	4
Chemical warfare agents	1

Rapid acute toxicity testing was evaluated by four of the pilots. Many pilots experienced difficulty with the use and performance of the DeltaTox and Eclox toxicity test kits such as interferences, complicated user instructions or variability of results among different field personnel. Some pilots discontinued use of these kits, while others determined that they would continue to use them during response S&A but only by highly trained analysts in a laboratory or other controlled environment. One pilot determined that the results from these kits would only be considered under the circumstance that none of the other field tests yielded positive results. Because of potential toxicity concerns with cyanide standards and test reagents, two pilots did not transport these into the field.

Quality Assurance

Field testing methods for which the utility was already certified or accredited did not require additional QA/QC for S&A. However, existing Standard Operating Procedures (SOPs), Quality Assurance Project Plans, and Quality Management Plan documents were reviewed to ensure that they adequately addressed the data collection and reporting needs of S&A.

New methods for both baseline monitoring and response S&A were integrated into the utilities' existing QA/QC programs. This included an initial demonstration of capability, establishing data quality objectives, point-of-use quality control, and developing SOPs. During this process, the pilots recognized that there was not an existing certification or accreditation program for many of the site safety screening or rapid field testing methods. Thus, they had to develop their own QA/QC criteria for these methods.

Sample Collection

Sampling kits were designed to include the sample collection containers, reagents, supplies, and preservatives for methods that would be performed in response to possible contamination. Sampling kits were replaced periodically based on the shelf life of the materials in the kits. In general, the pilots either purchased custom emergency response sampling kits or had utility personnel assemble the kits. These sampling kits were generally deployed one of the two following ways:

- Stored at the utility laboratory where sampling teams can readily access them prior to deploying
- Staged at strategic locations through the distribution system that could be rapidly accessed

> **IMPLEMENTATION HIGHLIGHT**
>
> One pilot developed a mobile lab to store sampling and testing equipment for rapid deployment. This allows personnel to perform field tests in a controlled environment and functions as a mobile command center for incident response.

All of the pilots recognized the importance of collecting large volume samples (10-L to 100-L) to support analysis of biological contaminants. Dilute contaminants in large volume samples can be concentrated using ultrafiltration to improve the sensitivity of methods. Two of the pilots performed ultrafiltration of large volume water samples in their laboratories with one of the two also evaluating ultrafiltration in the field. Ultimately, one utility decided to conduct ultrafiltration at its laboratory as opposed to in the field. The second pilot did not maintain ultrafiltration capability in-house and limited their process to collecting bulk samples for transport to their state public health laboratory for analysis.

Field Staffing and Field Safety

Four of the pilots identified personnel with various specialties such as treatment, pumping, distribution, field sampling, and chemistry who could comprise a field team as needed to support response S&A. These personnel were designated as Site Characterization Teams that would perform sampling, site safety screening, and rapid field testing under low hazard conditions. If hazardous materials or indicators of hazardous conditions or criminal activity were discovered, field personnel were trained to withdraw and an appropriate emergency response partner would be notified. Cross-training of personnel was essential given that response S&A may be necessary at any time of the day or night. While one pilot did have field personnel trained to support sampling and basic water quality parameter testing for compliance monitoring, it did not build a specially trained Site Characterization Team because it had internal access to the city's departmental HazMat unit, which could be activated to support response S&A if necessary.

All pilots reviewed existing Health and Safety Plans to ensure they were appropriate for activities that would be conducted by utility personnel under low-hazard conditions, and Health and Safety Plans were revised to cover field activities performed at new sampling locations identified during CWS implementation. The four pilots that built Site Characterization Teams for response S&A conducted training on the use of field test kits and instruments and donning of personal protective equipment. Various approaches were used to provide hazard awareness training to utility personnel who would support response S&A, including internally-provided training at the utility, use of state training resources, or EPA-provided training.

9.1.2 Summary of Lessons Learned

Site Safety Screening and Rapid Field Testing

Consider the sustainability of new equipment prior to purchase. Besides the initial investment to acquire site safety screening and rapid field testing equipment and supplies, these capabilities required additional personnel training, periodic calibration, maintenance, and regular use to maintain analyst proficiency. Pilots were more likely to maintain equipment and supplies that could be used for applications outside of response S&A. For example, if volatile/combustible gas monitoring equipment was purchased for site safety screening in response S&A, it could also be used for confined space entry in other utility programs.

Evaluate vendor support prior to purchasing field test kits and instruments. Some pilots noted that unresponsive vendors can make it difficult for utilities to troubleshoot performance issues related to field test kits or instruments. Vendors that are responsive and flexible to the needs of the utility can contribute to the long-term use of newly purchased field test kits and instruments.

Determine the role of the utility at sites of suspected contamination. S&A drills and exercises elucidated situations in which the pilots would activate an emergency response partner, such as HazMat, to characterize sites of suspected contamination before utilizing their own personnel to perform response S&A. Consideration of the hazards that may be encountered during response S&A and the capabilities of a HazMat response partner can inform the decision on whether or not to purchase field test kits or instruments for site safety screening and rapid field testing.

LESSON LEARNED HIGHLIGHT

All pilots found that HazMat units were proficient with site safety screening instrumentation but many lacked experience in collection and analysis of water samples.

Consider how advanced planning can reduce field response times. The pilots were able to reduce response times up to 50% with minimal effort by preparing sampling kits with pre-labeled bottles, field testing instruments and supplies, investigation aids (e.g., field guides and checklists), and personal protective equipment in advance. This equipment was generally stored in a designated closet or vehicle and verified periodically (e.g., batteries were checked and expired supplies were replaced).

Adverse weather conditions can impact field testing. Poor weather conditions presented challenges for operating field test equipment properly, which affected the quality of field data. One pilot addressed this challenge by purchasing and equipping a van to allow field personnel to perform testing in a controlled setting. Other pilots conducted testing inside buildings or purchased tents and tables for field testing.

Quality Assurance

Consider the time required to establish and maintain proficiency. Establishing proficiency with site safety screening or rapid field test kits and instruments may require practice several times per week for several weeks and, depending on the test kits or instruments selected, can require routine use to maintain long-term proficiency.

> **LESSON LEARNED HIGHLIGHT**
> Having a well-established quality assurance program provided the confidence in the field testing results needed to make informed response decisions.

Consider QC that can be done at the laboratory instead of in the field. Calibration of equipment at the utility prior to field deployment saves time and can yield higher quality data.

Sample Collection

Identify and prepare for site-specific sampling requirements. Some sampling locations required special sampling equipment based on accessibility at a facility, analytical parameters to be tested, and personnel safety considerations. Collection of large volume samples was not possible at some sampling locations due to confined space or inability to increase water flow to achieve reasonable sample collection times. One pilot used a fire hydrant adapter to regulate the flow of water into the sample bottles, making it easier to collect samples from fire hydrants.

Consider collecting bulk samples for rapid field testing. Collection of a 5 gallon bulk sample enabled sub-sampling for rapid field testing and laboratory analysis so that testing was conducted on the same sample and various test results could be compared. Additionally, it was deemed unsafe or impractical to collect multiple small volume samples at some sampling locations, such as confined spaces. However, plans for sample transport should be made as a 5 gallon bulk sample weighs approximately 42 pounds.

Field Staffing and Field Safety

Train multiple personnel to support field activities to promote sustainability. Cross-trained personnel provided redundancy in skill sets for field S&A and guarded against the possibility of skills being lost due to personnel turnover.

Minimize risks to field sampling teams by implementing proper safety practices. Training on hazard awareness, safe work practices, and use of personal protective equipment was especially important for preparing personnel to respond during the early phases of investigation when hazards may not have been fully characterized. Hazard awareness training and practice for routine S&A was also beneficial in the event field personnel discovered hazardous materials or situations during their routine job duties.

9.2 Laboratory Capabilities

Laboratory capabilities consists of the sub-elements presented in **Table 9-7**.

Table 9-7. Laboratory Capabilities Sub-Elements

Design Sub-Element	Description
Contaminant Coverage	The contaminants and contaminant classes for which the utility prepares for in advance by identifying methods and laboratory partners.
Quality Assurance	Ensuring high quality data during response S&A by including a demonstration of capability and QA/QC for each pre-established laboratory method and by incorporating all laboratory response methods into the utility's QA/QC program. Also, ensuring a demonstration of capabilities has been performed and proper QA/QC is in place for analyses conducted by partner laboratories.
Staffing	Planning for staffing involves identifying and training personnel in the use of laboratory methods and procedures and developing contingency plans in the event that there are contamination scenarios for which the utility would require the support of partner laboratories.
Safety	Planning for the health and safety of personnel who may be called on to respond to water contamination incidents involves review of existing Health and Safety Plans to ensure they address any modified or additional safety precautions the utility may implement when responding to incidents in which the contaminant has not yet been identified.
Mutual Aid Laboratory Networks	Mutual aid laboratory networks are formal alliances whereby laboratories share resources during an emergency. Establishing these relationships in advance can ensure that the utility has access to the resources they need during response S&A. Mutual aid agreements that include the utility's emergency response analytical needs can reduce the typical response gap between local and statewide agreements as they do not require emergency declaration prior to activation.

9.2.1 Summary of Implementation Approaches

This section describes the approaches implemented by the pilots to build laboratory capabilities in preparation for response to possible water contamination incidents.

Contaminant Coverage

To evaluate existing laboratory capabilities and determine enhancements to pursue, all pilots first identified existing laboratory methods and then compared these to their contaminant design basis to determine gaps in contaminant coverage. When determining how to address gaps, the decision to build new capabilities in-house or expand capabilities through a partner laboratory included evaluation of: (1) cost of new instrumentation, (2) operation and maintenance costs, (3) required expertise and availability of utility laboratory analysts, (4) ability to use new instrumentation to support goals beyond the CWS, and (5) safety requirements associated with the method and target analyte(s).

IMPLEMENTATION HIGHLIGHT

Though designated as a response component, the grab samples collected through routine S&A provide the ability to detect foreign substances in the distribution system.

Ultimately, all pilots achieved broad contaminant coverage through a combination of leveraging existing capabilities, building new in-house capabilities, and identifying partner laboratories. Three pilots had combined water-wastewater laboratories with extensive existing in-house laboratory capabilities and did not incorporate significant in-house enhancements into S&A. Other pilots built new in-house capabilities, identified nearby commercial laboratories, or made arrangements with local and state environmental and public health laboratories to provide analytical support during specific contamination scenarios. Most pilots identified who their partner laboratory would be for overflow capacity or for analysis of samples possibly containing biological select agents and toxins (as declared by the Department of Health and Human Services), radiochemicals, non-select toxins, or chemical warfare agents.

The pilots researched EPA's Compendium of Environmental Testing Laboratories to help identify potential laboratory partners. Commercial partner laboratories were evaluated based on analytical capability and capacity, procedures for emergency access, rapid turn-around, reporting procedures, and availability of a quality management program.

One pilot's approach to building laboratory capabilities for S&A was to establish internal analytical capabilities to cover as many contaminant classes as possible in an effort to reduce reliance on outside entities that may not always be available to respond quickly. The utility laboratory was equipped with extensive instrumentation prior to the pilot and had highly technical and well-trained laboratory personnel, which allowed for easy incorporation of new, sophisticated instrumentation purchased in support of the pilot. Several rapid screening methods were implemented using existing capabilities to expedite analysis and increase the number of target analytes. This pilot had extensive pathogen detection capabilities using various PCR platforms. They also had LC-MS/MS capabilities for chemical warfare agent degradation products, pharmaceuticals, and biotoxins. This laboratory also had ICP-MS capabilities for metals and became licensed to perform radiochemistry methods.

Four of the pilots participated in a Water and Wastewater Agency Response Network to enable mutual aid and assistance among water and wastewater utilities in their state to respond to and recover from emergencies by sharing resources. When specified in the agreement, utilities can access supplemental assistance from other utilities such as equipment, field crews, or laboratory services to support S&A in an emergency. One pilot also participated in a state laboratory network, which consisted of regional and state public water utility system laboratories, the EPA regional laboratory, and the state public health laboratory.

Quality Assurance

Laboratory methods for which the utility was already certified or accredited did not require additional QA/QC for S&A. However, existing SOPs, Quality Assurance Project Plans and Quality Management Plan documents were reviewed to ensure they adequately addressed the data collection and reporting needs of response S&A. For methods supported by commercial partner laboratories, the pilots selected laboratories certified or accredited for the method and analyte of concern. Some utilities that built in-house capabilities did not elect to get certified or accredited in the method and analyte of concern but did a rigorous demonstration of capability and incorporated the method into the laboratory's QA/QC program.

Staffing

All pilots relied upon existing personnel to support laboratory analyses for S&A. Contingency staffing plans were developed to provide 24/7 laboratory support, expedited analysis of samples, increased capacity, and contingency plans if the laboratory experienced instrument failure or if personnel were unavailable. Some pilots cross-trained personnel to perform multiple roles. Contingency plans also noted partner laboratories that would conduct sample analyses for scenarios which the utility deemed too hazardous for its laboratory personnel.

Safety

The pilots reviewed, and in some cases modified, existing laboratory safety programs to include the unique safety requirements of response S&A. Example modifications included identification of dedicated storage areas for response samples, working with samples in a fume hood, use of additional personal protective equipment, and proper sample disposal.

9.2.2 Summary of Lessons Learned

Contaminant Coverage

Consider sample analysis turnaround time when evaluating potential laboratory partners. The turnaround time for samples can vary widely across laboratories. Critical factors to consider include the time to transport samples to the laboratory, their mobilization time, their operating hours, and their ability to analyze samples during non-business hours.

Identify partner laboratories capable of performing confirmatory analyses. Some pilots developed analytical capabilities for contaminants such as chemical warfare agent degradation products or biological select agents. However, if the utility laboratory detected these target contaminants, a qualified laboratory would be needed to confirm the results, such as a laboratory qualified to analyze for chemical warfare agents or with Biosafety Level 3 capabilities (e.g., state public health laboratory).

LESSON LEARNED HIGHLIGHT

Specific procedures must be followed to access the capabilities the Laboratory Response Network. Requests usually have to be initiated by the local health department.

Provide field testing results to laboratory partners to determine an analytical testing strategy. During a true unknown contaminant scenario, the pilots recognized that it would be unrealistic to request that a laboratory partner test for "everything." Therefore, available information from the CWS surveillance components and field testing results would be provided to the laboratories and supporting agencies to help narrow down the laboratory analyses and determine potential interferences with the laboratory methods that would be used.

Consider laboratory instrumentation that can provide analytical capability to meet multiple goals. One pilot justified purchase of a new LC-MS/MS for screening of a broad range of organic contaminants in support of response S&A. The instrument was also used to screen and test watershed samples for emerging contaminants, such as pharmaceutical products and chemicals used during the hydraulic fracturing process. Another pilot purchased a GC-MS to enable in-house analysis of samples for regulated and unregulated semi-volatile organic compounds.

Evaluate unconventional methods for sample analysis in support of response S&A. Validated drinking water methods were not available for some contaminants. In addition, some methods were extremely time-consuming, resulting in a very long sample turnaround time. Thus, several pilots considered and evaluated rapid screening methods or methods not validated for use in drinking water samples to support the goals of response S&A. Advanced expertise among the in-house laboratory analysts provided an opportunity to conduct method development research. Also, custom methods developed for the CWS, which are not used for regulatory compliance, may be exempt from common reporting requirements.

Consider emergency response modifications. Methods used by the utility for compliance monitoring may be able to be modified for emergency response. For example, mass spectrometry instrumentation could potentially be operated in full-scan/semi-quantification mode to detect tentatively identified compounds.

Laboratory Partnerships

Include laboratory personnel early in planning. Laboratory personnel were often needed for additional roles in response S&A from sample receipt and disposition, notification of partner laboratories, and data review and reporting. Planning for their multiple roles in response S&A helped to identify areas for cross-training.

Plan for a variety of scenarios. There may be contamination scenarios under which the utility would not have sufficient capability or capacity to support the response. The pilots identified partner laboratories for scenarios in which they would not or could not use utility personnel even if they had the method capability in-house.

Consider the importance of communicating field observations and testing results. It was critical to provide information gathered during field response to all personnel handling those samples so that appropriate safety procedures could be implemented.

Indicate to laboratory personnel when they will be analyzing samples collected during incident response. Because laboratory analysts may need to apply certain procedures when analyzing samples in support of response S&A, the pilots recognized the necessity of clear communication with the laboratory.

9.3 Routine S&A

Routine S&A consists of the sub-elements presented in **Table 9-8**, which are discussed separately in the following subsections.

Table 9-8. Routine S&A Sub-Elements

Design Sub-Element	Description
Establishing Baseline Data	Data established by mining routine historical data, using data collected from previous incidents, using data collected through one-time special utility projects or exercises, or by performing new baseline monitoring.
Maintenance Monitoring	Data collected during routine S&A to maintain baseline data, analyst proficiency, and instrumentation readiness for all pre-established methods the utility would use during response S&A.

9.3.1 Summary of Implementation Approaches

Establishing Baseline Data

All pilots developed a sampling and analysis plan for establishing baseline data for the field and laboratory methods that would be used during response S&A based on consideration of the following factors:

- Parameters that were measured by water quality parameter testing, site safety screening equipment, or rapid field test kits
- Contaminant design basis, including contaminants of concern to water security and any contaminants of concern in the pilot's distribution system
- Availability of historical data
- Critical locations such as storage tanks, pumping stations, or locations where the utility had OWQM stations
- Sources of variability (e.g., different treatment plants, different source water, seasonal effects)
- Representative sampling locations, including spatial distribution, source water type, water age, and distribution conditions that could result in variability or method interferences
- Accessibility to sampling sites

All pilots conducted baseline monitoring quarterly or monthly for at least one year. Some target analytes and parameters were analyzed through existing S&A efforts being conducted to support compliance monitoring. For new target analytes, most pilots established a more frequent S&A schedule to establish a sufficient baseline. One pilot collected samples for metals analysis from hydrants during flushing during the baseline monitoring period to better understand accumulation of metals in hydrant barrels. This allowed the pilot to evaluate whether hydrant sampling is representative of the distribution system water quality with respect to metals occurrence.

Three of the pilots had a LIMS at the start of the project to manage baseline data and to provide access to historical data relevant to the target analytes for S&A. One of the pilots acquired a LIMS and another installed a new LIMS during the course of the pilot project. Analysis of the baseline data enabled the pilots to establish parameter or analyte specific control limits that allowed personnel to identify field or laboratory testing results that deviated from normal baseline data. All pilots ensured that baseline data and control limits were readily accessible to utility managers and others who needed it during response (either via paper copy, a LIMS, or a CWS dashboard). User-friendly summary reports in graphical or tabular formats were also developed to communicate results with higher-level utility managers or partner laboratories when S&A results deviated from the baseline, indicating possible water contamination.

One pilot developed a database that contained extensive information on over 1,000 contaminants of concern and 185 for which the utility could provide screening or confirmation. The database contained method information (such as chromatograms, detection limits, etc.) toxicity data, baseline contaminant occurrence, and a field operator's guide containing summary information that could be of use to the utility's field personnel or first responder organizations.

Maintenance Monitoring

Upon completion of baseline monitoring, all pilots transitioned to maintenance monitoring to maintain the baseline water quality profile and the proficiency of analysts who would perform field or laboratory methods during response S&A. The frequency of sample collection and analysis was reduced for maintenance monitoring in some cases. Some of the target analytes were covered through ongoing compliance monitoring. For certain contaminants, pilots determined that no maintenance monitoring would be performed given the low likelihood of occurrence in the distribution system or the fact that the contaminants were never detected during baseline monitoring.

Some pilots conducted additional activities under the maintenance monitoring program including:

- Monthly review of field capabilities to maintain equipment and supplies, and training of new employees. Monthly inspections included a quality check of instrument use to ensure response readiness and to provide ongoing demonstration of capability.
- Continued quantitative analysis of target analytes beyond those required for compliance monitoring, including samples collected at locations beyond the utility's routine sampling locations.

9.3.2 Summary of Lessons Learned

Leverage existing monitoring capabilities and programs. Baseline and maintenance monitoring programs were more cost-effective and sustainable when the pilots leveraged existing efforts to monitor water quality such as regulatory compliance, process control, and analyses performed in response to customer complaints.

Consider locations where water samples would be collected during response S&A when designing a baseline monitoring program. It was important to characterize baseline contaminant occurrence and method performance at locations that may be sampled during incident response. This allowed the pilots to have adequate historical data that could be used for comparison of results during response S&A.

Consider the importance of rapid access to S&A data when determining how to store and manage baseline and maintenance monitoring data. Pilots found the use of a LIMS or other database to be essential for storing and managing the large volume of field and laboratory data generated during baseline and maintenance monitoring. A LIMS or database also enabled rapid access to historical water quality data to help determine if response S&A results exceeded baseline levels. Some pilots configured their LIMS to generate alerts if there were changes in source water or finished water quality.

Updating of baseline data through maintenance monitoring provides benefits beyond S&A. Continued analysis of samples during maintenance monitoring allowed the pilots to maintain the baseline water quality profile. This provided an enhanced ability to evaluate and respond appropriately to anomalies in distribution system water quality through identification of changes in source water quality, treatment processes changes, or distribution system changes.

9.4 Response Procedures

Response procedures consists of the sub-elements presented in **Table 9-9**, which are discussed separately in the following subsections.

Table 9-9. Response Procedures Sub-Elements

Design Sub-Element	Description
Identification and Development of Response Procedures	Identifying S&A activities that could be performed by the utility in response to possible, credible, or confirmed water contamination incidents. Modifying existing procedures or developing new procedures to document the utility's planned response activities, internal and external contacts, and communication methods.
Testing and Refinement of Procedures	Testing and refining response procedures through training of S&A personnel and through intra- and inter-component drills and exercises with other surveillance component personnel or the utility's S&A emergency response partners and laboratories.

9.4.1 Summary of Implementation Approaches

After developing field and laboratory capabilities that would be used for response S&A, the pilots determined whether existing procedures for those capabilities needed to be modified or if new procedures were necessary (e.g., for new field or laboratory instrumentation). Furthermore, the pilots developed new procedures to document actions the utility and its response partners would take during incident response related to site characterization, notifications, communication, sample disposition, and chain-of-custody. Examples of activities that required development of response procedures by the pilots included:

- Site characterization and sampling
    - Mobilization and deployment to the field
    - Site approach
    - Site safety screening and hazard assessment
    - Water quality parameter testing and rapid field testing
    - Sample collection, including site-specific sampling procedures
    - Labeling and packaging samples for transport to the laboratory
    - Decontamination of sample bottles and personnel
    - Exiting the site
- Activation of HazMat
- Communication between the Incident Commander and the Site Characterization Team leader
- Sample handling, transport, and disposition at the laboratory
- Sample screening
- Communication from the utility analytical services requestor to partner laboratories (including threat evaluation and site characterization information, requested turnaround time, and reporting instructions)

In addition to written procedures that were developed, most pilots also developed ancillary supporting documentation including checklists and standard forms to minimize the time required to conduct site characterization. Often these materials were based on forms provided in Module 3 of the Response Protocol Toolbox (EPA, 2003). Examples included:

- Field supply checklist
- Field testing results form
- Field safety form
- Chain-of-custody form
- Emergency contact information for utility and partner laboratory personnel

Recognizing that incident response could transition to a criminal investigation depending on the results of the field investigation, or other information received from outside sources, some pilots worked with law enforcement to develop specific processes to maintain the credibility of criminal evidence at all times. For example, measures were implemented to:

- Avoid moving or disturbing items that may become evidence in a criminal investigation
- Perform field activities away from items that may become evidence in a criminal investigation
- Handle samples as evidence and maintain chain-of-custody
- Record observations in writing and with photos

All pilots tested and refined S&A procedures in a step-wise approach beginning with training of personnel responsible for supporting S&A through classroom-style presentations and workshops. Training allowed personnel to develop proficiency using field and laboratory methods and enforced roles and responsibilities that would apply during response S&A. As personnel became more familiar with the procedures, the pilots expanded to intra-component drills (which involved personnel testing a group of S&A procedures) and inter-component drills and exercises (involving multiple components) to practice response S&A in the context of a variety of contamination scenarios with various surveillance component alerts. The general approach to training and exercises is discussed further in Section 3.4.

9.4.2 Summary of Lessons Learned

Develop a clear understanding of utility and HazMat roles and responsibilities. All pilots found that developing, testing, and refining response procedures elucidated the specific roles and responsibilities of utility personnel and HazMat during incident response. Collaboration between these entities allowed the pilots to recognize the limitations of utility personnel in responding to some types of scenarios, and also identified the characteristics of high hazard situations which would require support from HazMat to perform site characterization activities.

> **LESSON LEARNED HIGHLIGHT**
>
> Testing utility S&A procedures with partners helped the partners refine their own internal procedures or identify new procedures that needed to be developed.

Prepare easily accessible physical copies of procedures and forms to facilitate incident response. All the pilots found it helpful to compile response procedures and supporting documentation (e.g., site characterization results forms, notification protocols, chain-of-custody forms) into a notebook or binder. Some of the pilots also prepared multiple copies of large print, laminated versions of procedures to facilitate their use in the field.

Routine field or laboratory procedures may require modification for response S&A. Many pilots found that initial drafts of response procedures required revision to incorporate lessons learned from training, drills, and exercises. Incident response required that S&A personnel apply a different mindset with respect to safety or maintaining the credibility of criminal evidence, as compared to processes conducted for routine utility operations. Working with HazMat was beneficial when refining certain procedures that were not traditionally performed by pilots (e.g., using appropriate personal protective equipment and decontamination procedures).

9.5 Summary of Pilot Experiences with S&A

One of the most significant benefits realized by the pilots though implementation of S&A has been increased preparedness for providing S&A support during any emergency. This benefit has been derived by adding in-house field and laboratory capabilities for a wide variety of contaminants and contamination scenarios by cultivating relationships with Hazmat, identifying partner laboratories for emergency response, and documenting response procedures.

A significant challenge in maintaining S&A capabilities recognized by all pilots is maintaining proficiency in the implementation of procedures not used during routine utility operations, including routine and baseline monitoring. The solution to this challenge is to routinely practice these procedures through drills and exercises. These do not need to be HSEEP compliant exercises, but rather simple training sessions that give utility personnel the chance to practice use of response S&A procedures and equipment. The need to engage partners in these training activities has also been recognized.

To improve sustainability of S&A, several pilots have modified the component over time. After initially establishing baseline contaminant occurrence for a pre-selected suite of methods, some of the pilots have adopted a reduced-frequency monitoring schedule to maintain baseline data, analyst proficiency, and instrument readiness. Some pilots have also discontinued use of field testing equipment that is expensive or difficult to maintain.

Section 10: Sustainability

All five pilots have found that the benefits derived from their CWS justify the cost to implement, operate, and maintain the systems. Benefits reported by the pilots include:

- Improved knowledge of distribution system water quality to support system operations, including more efficient management of residual disinfectant and distribution system storage facilities
- Additional information that supports investigation of and response to customer complaints
- More efficient ways to access and interpret data related to distribution system water quality, operations, and customer complaints
- Improved coordination among utility departments and improved communication with external partners
- More timely detection of water quality incidents in the distribution system including nitrification, low chlorine residual, and changes resulting from treatment process upsets
- More effective investigation of and response to water quality incidents
- Confidence that, should distribution system contamination occur, the utility would be able to detect the incident early and respond to it quickly and effectively

Each of the pilots has made modifications to their original CWS designs to make their system more sustainable by maximizing benefits while minimizing costs and the level of effort necessary to maintain the system. The most common changes are described below. Additional component-specific modifications can be found in the summaries to Sections 4 through 9.

- *Refining component operating procedures*: Through routine operation of the components, investigation of alerts, and drills and exercises, the pilots have identified ways to streamline activities to make investigations shorter and more effective.
- *Updating response plans*: CMPs have been updated and optimized based on the results of drills and exercises and lessons learned from responding to real-world water quality incidents in the distribution system.
- *Refining the user interface*: Through regular use of the information management system user interfaces developed to support the CWS, utility personnel have identified potential refinements to make data access and analysis more efficient and effective.
- *Refining data analysis methods*: OWQM, CCS, and PHS use configurable algorithms to analyze the monitored datastreams and produce alerts. Based on experience investigating alerts, all of the pilots have adjusted, and in some cases simplified, the algorithms to minimize the number of invalid alerts. Enhancements have included increasing alert thresholds, changing the period of data considered in analysis, and working with algorithm vendors to eliminate bugs and include new logic for suppressing recurring invalid alerts.

> **LESSON LEARNED HIGHLIGHT**
>
> The user interfaces developed for the CWSs were found to provide significant day-to-day benefit because they conveyed useful information to utility personnel, including those who may not be directly involved with the CWS. Thus, effort spent on designing and refining these interfaces to meet user needs resulted in broader acceptance of the entire CWS.

Significant lessons learned related to sustainability of the CWS include:

Ensure organizational support for the system: Diligent execution of roles and responsibilities is crucial for project success, but personnel were often resistant to assuming the new, often significant responsibilities associated with the project. In order to obtain support for the project, it was valuable to communicate the goals and objectives for the CWS, as well as to consistently communicate expectations related to CWS operations.

Leverage existing resources and procedures. Use of existing resources and procedures for the CWS clearly saved time and money. It also resulted in greater system acceptance by personnel as the responsibilities for CWS operations were integrated into their existing roles and responsibilities.

Do not rush real-time system operation. It was important to conduct significant system testing and optimization before starting real-time operation. Premature transition to real-time operation and alert investigations left personnel disenchanted with the system, as time was wasted responding to issues and invalid alerts that would not have occurred had time been spent working out problems before starting real-time operations. Sufficient off-line training and exercises helped personnel become familiar with procedures before they were asked to investigate alerts in real time. Finally, some pilots took a phased approach to the transition so as to not overwhelm personnel with a large increase in responsibilities all at once. For example, one utility transitioned to full deployment by asking personnel to fully investigate a few alerts per week, increasing this number until all alerts were investigated in real-time.

Alerts are inevitable but sustainable. All of the pilots received more invalid alerts from all of the components than they originally planned for and believed they could manage. However, as investigation procedures were refined and personnel became experienced, the time necessary to investigate alerts drastically decreased. By the end of the pilot period, most investigations across components could be completed in less than ten minutes, and the pilots found the effort required for alert investigations to be sustainable. None of the pilots had to activate the CMP in response to a component alert.

Plan and design in phases. In some cases, the pilots found it beneficial to design and implement the system in phases, using lessons learned from previous phases in future designs. For example, all of the pilots designed and installed OWQM stations in phases, using experiences with installed equipment to decide if the same or alternate equipment would be used at new locations.

The most powerful testament to CWS sustainability is the continued maintenance and operation of the systems by all five pilots. The pilots have incorporated the cost to maintain their CWS into their annual operating budgets and continue to evaluate ways to enhance the value of the system.

Section 11: Summary and Conclusions

The five WSI pilots successfully implemented operational CWSs over a two to three year period using EPA grant funding. While they were required to include all six components depicted in Figure 1-1, they had flexibility with respect to design of the individual components, as well as the manner in which the project was managed and implemented.

The information collected from the five WSI pilots demonstrates that CWSs can be beneficial and sustainable, as discussed in Section 10. This conclusion has been reinforced by utilities who have implemented their own systems (Umberg, 2012), through conversations with stakeholders, and through research by the EPA on system performance (Allgeier, et al., 2013; EPA, 2014). Also, an independent evaluation of the pilots by the Critical Infrastructure Protection Advisory Council (CIPAC) concluded that CWSs can be effective, implementable and sustainable if designed to meet utility-specific goals. For this reason, the CIPAC recommended that EPA promote flexibility in the design of these systems (WSCC/WGCC, 2012). Note that the CIPAC was comprised of a number of subject matter experts from the drinking water sector and was formed under the auspices of the Water Sector Coordinating Council (WSSC) and Water Government Coordinating Council (WGCC).

While the pilots were largely successful, the designs implemented by the pilots may not be a suitable model for all utilities for the following reasons. First, the primary design objective of the pilots, as required by EPA, was to improve the utility's ability to detect and respond to drinking water contamination incidents. Systems independently implemented by other utilities should be designed to meet utility-specific goals, which may prioritize monitoring and management of distribution system water quality above early detection of contamination incidents. Furthermore, the pilots received large grants from EPA which afforded them the opportunity to develop advanced surveillance and response capabilities. Finally, the pilots were encouraged to try a variety of products and techniques, including novel and developing technologies. However, even with these caveats, the lessons learned from the WSI pilots are relevant and useful to other utilities planning to improve their distribution system surveillance and response capabilities.

As noted in Section 1, EPA has acted upon the recommendations of the CIPAC and has transformed the contaminant-focused CWS concept into the broader concept of a Water Quality Surveillance and Response System (SRS). EPA plans to promote and support SRS implementation by providing guidance and training to utilities. The SRS program will incorporate lessons learned from the WSI pilots, but will also consider how utilities can leverage existing resources and capabilities to implement a beneficial, cost-effective SRS. Visit EPA's *Water Quality Surveillance and Response Website* (EPA, 2015) for more information.

Section 12: Pilot Materials in the Public Domain

The final reports submitted to EPA by the pilots are not available to the public. This document summarizes major approaches and findings. However, more details on implementation and experiences of individual pilots can be found in these publicly-available resources.

Greater Cincinnati Water Works

EPA conducted an extensive evaluation of the Cincinnati CWS pilot. Documents available at water.epa.gov/infrastructure/watersecurity/lawsregs/initiative.cfm include:

- *Post Implementation System Status of the Cincinnati CWS Pilot*
- *System Evaluation of the Cincinnati Contamination Warning System Pilot*
- *Evaluation of the Water Quality Monitoring Component of the Cincinnati CWS Pilot*
- *Evaluation of the Enhanced Security Monitoring Component of the Cincinnati CWS Pilot*
- *Evaluation of the Customer Complaint Surveillance Component of the Cincinnati CWS Pilot*
- *Evaluation of the Public Health Surveillance Component of the Cincinnati CWS Pilot*
- *Evaluation of the Consequence Management Component of the Cincinnati CWS Pilot*
- *Evaluation of the Sampling and Analysis Component of the Cincinnati CWS Pilot*

Philadelphia Water Department

The Philadelphia Water Department produced the following white papers providing guidance based on their approaches and lessons learned. The link to the PDF for each paper is given.

- *How to Select an Online Water Quality Monitoring Data Management System*
  ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Data-Management-Selection.pdf
- *Selection of Online Water Quality Monitoring Technologies and Station Design*
  ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Quality-Monitoring.pdf
- *Guidance for Locating Online Water Quality Monitoring Stations using TEVA-SPOT*
  ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Quality-Monitoring-TEVA-SPOT.pdf
- *Developing and Maintaining a Baseline for Water Quality Monitoring*
  ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Water-Quality-Baseline.pdf
- *Exercises and Lessons Learned to Improve Response Preparedness for Site Characterization and Sampling*
  ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Improve-Response-Preparedness.pdf
- *Site Characterization and Water Sampling Guidance*
  ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Site-Characterization.pdf
- *Development of Control Limits for Baseline Water Quality Monitoring*
  ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Water-Quality-Control-Limits.pdf

- *Safety Screening for Radiological Contaminants During Site Characterization* ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Safety-Screening-Radiological-Contaminants.pdf
- *Enhanced Security Monitoring Guidance* ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Enhanced-Security-Monitoring-Guidance.pdf
- *Customer Complaints Surveillance Guidance* ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Customer-Complaints-Surveillance-Guidance.pdf
- *Public Health Surveillance Guidance* ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Public-Health-Surveillance-Guidance.pdf
- *Dashboard Development Guidance* ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Dashboard-Development.pdf
- *Development of User Requirements and Use Cases for a Contamination Warning System Dashboard* ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Warning-System-Dashboard-Requirements.pdf
- *Consequence Management Guidance* h2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Consequence-Management-Guidance.pdf
- Burlingame, B., Wiggind, C., and Ogino, C. (2012). "Responding to contamination: where do I sample?" *Opflow*. 38:3. ch2m.com/sites/default/files/content/article/attachments/CH2M-HILL-Responding-to-Contamination.pdf
- Eyring, A. (2012). Using a Portable UV-Vis Probe for Detecting Contamination Events. *AWWA Water Security Congress*. St. Louis, MO.

References

Allgeier, S., Agarwal, S., Umberg, K., Owens, C., and Pollak, A. (2013). *Evaluating Alternative Configurations for Water Quality Surveillance and Response Systems.* Proceedings of AWWA Water Quality and Technology Conference, Long Beach, California.

EPA. (2003). *Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents. Module 3: Site Characterization and Sampling Guide* water.epa.gov/infrastructure/watersecurity/upload/epa817d03003.pdf

EPA. (2005a). *Environmental Technology Verification Report: Hach Company Water Distribution Monitoring Panel and the Event Monitor Trigger System*. cfpub.epa.gov/si/si_public_file_download.cfm?p_download_id=504173

EPA. (2005b). *Environmental Technology Verification Report: Analytical Technology, Inc. Q45WQ Continuous Multi-Parameter Water Quality Monitor*. cfpub.epa.gov/si/si_public_file_download.cfm?p_download_id=504165

EPA. (2008). *Interim Guidance on Developing Consequence Management Plans for Drinking Water Utilities*. epa.gov/sites/production/files/2015-06/documents/wsi_interim_guidance_on_developing_consequence_management_plans_for_drinking_water_utilities.pdf

EPA. (2009). *Distribution System Water Quality Monitoring: Sensor Technology Evaluation Methodology and Results.* cfpub.epa.gov/si/si_public_file_download.cfm?p_download_id=493756

EPA. (2013). *Water Security Initiative: Guidance for Building Laboratory Capabilities to Respond to Drinking Water Contamination.* water.epa.gov/infrastructure/watersecurity/lawsregs/upload/epa817r13001.pdf

EPA. (2014). *Water Security Initiative: System Evaluation of the Cincinnati Contamination Warning System Pilot.* water.epa.gov/infrastructure/watersecurity/lawsregs/upload/A_System-Evaluation-Report.pdf

EPA. (2015). *Water Quality Surveillance and Response Website.* water.epa.gov/infrastructure/watersecurity/lawsregs/initiative.cfm

FEMA (Federal Emergency Management Agency). (2011). *National Incident Management System Training Program*. training.fema.gov/emiweb/is/icsresource/TrainingMaterials.htm

FEMA. (2013). *Homeland Security Exercise and Evaluation Program* fema.gov/media-library/assets/documents/32326

Hall, J., Zaffiro, A., Marx, R., Kefauver, P., Krishnan, E., Haught, R., and Herrmann, J. (2007). "On-line Water Quality Parameters as Indicators of Distribution System Contamination." *Journal AWWA.* 99:1.

Rosen, J., Schurmann, T., Specht, D., Rogers, R., Kopanski, R., and Brock, G. (2012). *Precision and Accuracy of On-line Water Quality Measurements.* Proceedings of AWWA Water Quality and Technology Conference, Toronto, Ontario, Canada.

Umberg, K. and Allgeier, S. (2015). "Parameter Setpoints: An Effective Solution for Real-time Data Analysis." Submitted to *Journal AWWA.*

Umberg, M. (2012). *Utility Experiences with Online Water Quality Monitoring in the Distribution System*. Presented at the Ohio Water Lab Analyst Workshop. ohiowater.org/otco/new%20site/docs/presentations/2012/Water_Lab/Umberg%20-%20WLA%20Workshop%20Presentation_2012-05-17.pdf

WSCC/WGCC (Water Sector Coordinating Council and Water Government Coordinating Council). (2012). *Contamination Warning System CIPAC Workgroup Final Report*. awwa.org/Portals/0/files/legreg/security/CWSFINALREPORT.pdf

Glossary

alert. An indication from a CWS surveillance component that an anomaly has been detected in a datastream monitored by that component. Alerts may be visual and or audible, and may initiate automatic notifications such as pager, text, or e-mail messages.

component. One of the primary functional areas of a CWS. There are four surveillance components: Online Water Quality Monitoring; Enhanced Security Monitoring; Customer Complaint Surveillance; and Public Health Surveillance. There are two response components: Consequence Management and Sampling and Analysis.

Consequence Management (CM). One of the response components of a CWS. This component encompasses actions taken to plan for and respond to possible drinking water contamination incidents to minimize response and recovery timelines, and ultimately to minimize consequences to a utility and the public.

Contamination Warning System (CWS). An integrated system of monitoring and surveillance components designed to detect contamination in a drinking water distribution system. The system relies on integration of information from these monitoring and surveillance activities along with timely investigative and response actions during consequence management to minimize the consequences of a contamination incident.

Customer Complaint Surveillance (CCS). One of the surveillance components of a CWS. CCS monitors water quality complaint data in call or work management systems and identifies abnormally high volumes or spatial clustering of complaints that may be indicative of a contamination incident.

dashboard. A visually-oriented user interface that integrates data from multiple CWS components to provide a holistic view of distribution system water quality. The integrated display of information in a dashboard allows for more efficient and effective management of distribution system water quality and the timely investigation of water quality incidents.

data analysis. The process of analyzing data to support routine system operation, rapid identification of water quality anomalies, and generation of alert notifications.

datastream. A time series of values for a unique parameter or set of parameters. Examples of SRS datastreams include, chlorine residual values, water quality complaint counts, and number of emergency department cases.

design element. The functional areas which comprise each component of an SRS. In some cases design elements are divided into design sub-elements. In general, the information presented in SRS guidance and products is organized by design elements and sub-elements.

Enhanced Security Monitoring (ESM). One of the surveillance components of a CWS. ESM includes the equipment and procedures to detect and respond to security breaches at distribution system facilities that are vulnerable to contamination.

information. Any data generated or used by a CWS. Information includes the raw data generated by CWS surveillance components, alerts generated by the components, ancillary data used to support data analysis or alert investigation, details entered during alert investigations, and documentation of Consequence Management activities.

information management. The processes involved in the collection, storage, access, and visualization of information.

invalid alert. An alert from a CWS surveillance component that is not due to water quality incident or public health incident.

monitoring station. A configuration of one or more water quality sensors and associated support systems, such as plumbing, electric and communications that is deployed to monitor water quality in real time at a specific location in a drinking water distribution system.

Online Water Quality Monitoring (OWQM). One of the surveillance components of a CWS. OWQM utilizes data collected from monitoring stations that are deployed at strategic locations in a distribution system. Monitored parameters can include common water quality parameters, such as disinfectant residual, pH, specific conductance, and turbidity. Advanced parameters, such as total organic carbon and UV-Vis spectral data, may also be monitored. Data from distribution system monitoring locations is transferred to a central location and analyzed for water quality anomalies.

passive support. A response partner that has been notified of a possible contamination incident but is not actively providing assistance. Passive support may become active support as the threat level escalates.

pilot. One of the five water utilities, along with their local partners, that received direct financial and technical support from EPA to deploy a CWS.

Public Health Surveillance (PHS). One of the surveillance components of a CWS. PHS involves the analysis of public health datastreams to identify public health incidents and the investigation of such incidents to determine whether they may be due to drinking water contamination.

real-time. A mode of operation in which data describing the current state of a system is available in sufficient time for analysis and subsequent use to support assessment, control, and decision functions related to the monitored system.

Sampling and Analysis (S&A). One of the response components of a CWS. S&A is activated during Consequence Management to help confirm or rule out possible water contamination through field and laboratory analyses of water samples. In addition to laboratory analyses, S&A includes all the activities associated with site characterization. S&A continues to be active throughout remediation and recovery if contamination is confirmed.

site characterization. The process of collecting information from the site of suspected distribution system contamination. Site characterization activities include the site investigation, site safety screening, and rapid field testing of the water and sample collection.

Water Quality Surveillance and Response System (SRS). A system that employs one or more surveillance components to monitor and manage distribution system water quality in real time. An SRS utilizes a variety of data analysis techniques to detect water quality anomalies and generate alerts. Procedures guide the investigation of alerts and the response to validated water quality incidents that might impact operations, public health, or utility infrastructure.