United States
Environmental Protection
Agency

Seattle-King County, Washington Community Case Study Report

Security and Preparedness Practices:

A Collaborative Approach to Water Sector Resiliency

Office of Water (4608T)
EPA No. 817-R-08-011
October 2008
www.epa.gov/safewater

Prepared under

Work Assignment No. 2-08
Active and Effective Security Program Support
EPA Contract No. EP-C-05-045
Technical, Analytical, and Regulatory Mission Support for the Water Security Division

DISCLAIMER

The information presented in the Seattle-King County, Washington Community Case Study provides an example of how one area of the country was successful at implementing practices that support preparedness and resiliency, with the expressed intent of using the effort to support water sector protective practices nationally. This document is not intended to serve as guidance. The mention of trade names or commercial products does not constitute endorsement or recommendation for use.

Questions concerning this document or its application should be addressed to:

Laura Flynn
U.S. Environmental Protection Agency
Office of Ground Water and Drinking Water
Water Security Division
1200 Pennsylvania Avenue, NW
Mail Code: 4608T
Washington, DC 20460

ACKNOWLEDGEMENTS

The U.S. Environmental Protection Agency (EPA) and the Seattle-King County, Washington Community Case Study Project Team wish to thank the following individuals and organizations for their participation in support of the project:

Case Study Guidance Team	
Allen Alston, King County Wastewater Treatment Division	Randy Holmes, City of Bellevue Utilities
Mike Boykin, U.S. EPA Region 10	Mike Jackman, City of Bellevue Utilities
Ben Budka, King County Wastewater Treatment Division	Mitzi Johanknecht, King County Sheriff's Office
Shad Burcham, King County Office of Emergency Management	Fred Savaglio, Virginia Mason Medical Center
Scott Decker, Washington State Department of Health	Hal Schlomann, Washington Association of Sewer and Water Districts
Robin Friedman, Seattle Public Utilities	Ron Speer, Soos Creek Water and Sewer District
Brandon Hardenbrook, Pacific Northwest Economic Region	Ted Stencilin, King County Sheriff's Office
Jim Henriksen, Seattle-King County Department of Public Health	Gene Taylor, U.S. EPA Region 10
Area Workshop Participants	
Cedar River Water and Sewer District	Ronald Sewer District
Cingular Wireless	City of Seattle
Coal Creek Utility District	Seattle City Light
Highline Water District	Seattle Fire Department
King County Water District #111	Southwest Suburban Sewer District
Lakehaven Utility District	U.S. Department of Transportation
Northwest Warning, Alert, and Response Network (NW-WARN)	Washington State Association of Counties and Cities
Puget Sound Energy	Washington Military Department, Emergency Management Division
Qwest	Washington State Department of Transportation

EXECUTIVE SUMMARY

A mission within the U.S. Environmental Protection Agency's (EPA's) Office of Water is to provide national leadership in developing and promoting protective programs that enhance the water sector's ability to prevent, detect, respond to, and recover from all-hazards events that may cause harm to consumers and/or utility infrastructure. The term "water sector" is used to describe both drinking water and wastewater utilities. The information contained in this report is a reminder that a protective program is not simply guards and gates, but also an attitude and culture of security and preparedness that is created and maintained throughout the utility.

EPA embarked on the Seattle-King County, Washington Community Case Study (Case Study) project as a strategy to increase awareness about the benefits of implementing an active and effective protective program. EPA turned to the Seattle-King County area because of their history of security and preparedness activity in the water sector. As an example for other communities across the country, the Case Study demonstrates how one area of the country is successful at implementing practices that support preparedness and resiliency.

Drinking water and wastewater utilities across the country are important to EPA's efforts for building relationships at the state and local levels. As such, the broad audience for this Case Study includes water sector utilities of all sizes, elected officials, local and state emergency management agencies, and leaders of critical infrastructure organizations across all sectors. The report should empower other communities and water sector utilities by demonstrating how implementing select practices supports creating an active and effective protective program.

The primary goal of the Case Study was to identify and document select examples of protective practices being implemented within the Seattle-King County area that validate the key features of an active and effective protective program developed by the National Drinking Water Advisory Council's (NDWAC or Council) peer-led working group; the Critical Infrastructure Partnership Advisory Council (CIPAC) Metrics Workgroup for Water would subsequently revise these key features. The features were developed as elements that, when applied individually or together, would help improve the water sector's ability to protect its systems, respond effectively to all types of emergencies, and safeguard public health and safety.

The Case Study report outlines the process EPA used to coordinate stakeholder participation, collect information, and select practices that would provide the water sector with detailed examples across a broad spectrum of possibilities. The practices center on activities that support all phases of security and preparedness. The purpose of this Case Study was to identify and describe security and preparedness practices water sector utilities are implementing in the Seattle-King County area, and provide a case study methodology that is easily replicated and can serve as a model for other communities and water sector utilities across the country.

A project team comprising key staff from EPA Office of Water, Computer Sciences Corporation (CSC), CH2M HILL, and Ross & Associates, formed a guidance team from 16 agencies, comprising 11 utilities and 5 state and local agencies to advise them on the effort and to provide feedback on the practices. In addition, a workshop was held with representatives from participating utilities and agencies, to discuss specific security and preparedness needs and practices. (Refer to the Acknowledgements for a list of guidance team members and workshop participants.)

The project team selected 23 practices from the many activities taking place in the Seattle-King County area to highlight the features of an active and effective protective program. To do this, the project team held a workshop with participants that included a cross-section of staff from water sector utilities, private sector, other infrastructures such as energy, and other response agencies such as law enforcement, fire, and emergency management. The result was a robust display of activities in the Seattle-King County area from which to match the features to demonstrate that all sizes of utilities could implement protective practices.

Case Study Findings:

The following recommendations should be considered to ensure the water sector is successful in implementing active and effective protective programs:

Partnership is Essential: Enhancing water sector security and preparedness requires collaborative partnerships with other interdependent sectors.

Think Long Term: Create a protective mindset and commit to a long-term strategy of continual security and preparedness improvements.

Secure Leadership Support: Engage municipal and county elected officials and encourage regional emergency operations staff to reach out to other interdependent sectors.

Think Broadly: Collaborate with other utilities, other sectors, state primacy agencies, public health community, and law enforcement and other first responders to collect and share essential information.

EPA's support of this Case Study is to raise awareness and encourage adoption of effective practices that individual communities and utilities may determine appropriate. EPA's involvement with documenting practices is not a promulgation of guidance or requirements.

TABLE OF CONTENTS

LIST OF ACRONYMS

AWWA – American Water Works Association

CID – Criminal Investigation Division

CIPAC – Critical Infrastructure Partnership Advisory Council

CIPP – Critical Infrastructure Protection Plan

CSC – Computer Sciences Corporation

DEP – Department of Environmental Protection

DEQ – Department of Environmental Quality

DHS – U.S. Department of Homeland Security

DOE – U.S. Department of Energy

EMS – Emergency Medical Services

EOC – Emergency Operations Center

EPA – U.S. Environmental Protection Agency

ERP – Emergency Response Plan

FEMA – Federal Emergency Management Agency

GETS – Government Emergency Telephone Service

HAZMAT – Hazardous Materials

HSIN – Homeland Security Information Network

HSPD – Homeland Security Presidential Directive

IC – Incident Commander

ICS – Incident Command System

IT – Information Technology

MOU – Memorandum of Understanding

NDWAC – National Drinking Water Advisory Council

NIMS – National Incident Management System

NIPP – National Infrastructure Protection Plan

NW-WARN – Northwest Warning, Alert, and Response Network

OEM – Office of Emergency Management

PIO – Public Information Officer

PNWER – Pacific Northwest Economic Region

POTW – Publicly Owned Treatment Works

RAM-D – Risk Assessment Methodology for Dams

RAM-W – Risk Assessment Methodology for Water

RCAP – Rural Community Assistance Partnership

RPTB – Response Protocol Toolbox

SCADA – Supervisory Control and Data Acquisition

SSP – Sector-Specific Plan

TEWG – Terrorism Early Warning Groups

TSP – Telecommunication Service Priority

UASI – Urban Area Security Initiative

VA – Vulnerability Assessment

VSAT – Vulnerability Self Assessment Tool

WaterISAC – Water Information Sharing and Analysis Center

WEF – Water Environment Federation

WMD – Weapons of Mass Destruction

WPS – Wireless Priority Service

SECTION 1: INTRODUCTION

1.1 Background

The Seattle-King County, Washington Community Case Study (Case Study) was initiated to increase awareness of the benefits of implementing an active and effective protective program. Seattle-King County was invited to participate because of the area's reputation in providing active leadership in water sector security and preparedness efforts. The Case Study is a model for other communities across the country. It demonstrates how one area was successful at implementing practices that support preparedness and resiliency. The intent of using this effort is to support drinking water and wastewater (water sector) protective practices nationally.

Following the events of September 11, 2001, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), requiring drinking water utilities across the nation to conduct vulnerability assessments of their systems and to update or create emergency response plans. EPA was tasked with overseeing security and preparedness efforts in the water sector pursuant to Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection." Under this directive, EPA has the authority to improve security and preparedness that protects critical infrastructure and key resources within the water sector. Although wastewater utilities were not required to conduct a vulnerability assessment under the Bioterrorism Act, EPA included both drinking water and wastewater utilities in their efforts to promote security and preparedness activities.

In addition, the President issued HSPD-8, "National Preparedness." The purpose of HSPD-8 is to "establish policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities." Moreover, EPA has additional responsibilities under HSPD-5, "Management of Domestic Incidents," HSPD-9, "Defense of United States Agriculture and Food," and HSPD-10, "Biodefense for the 21st Century."

HSPD-8 ushered in a new way of thinking about the role of utility staff in an emergency. Utility personnel are now considered first responders under HSPD-8, and this changes their interactions with traditional first responders such as police and fire agencies. Recent natural disasters and terrorist incidents underscore the critical nature of protecting water sector infrastructure and the need for coordinated response efforts.

In the fall of 2003, the National Drinking Water Advisory Council (NDWAC or Council) convened a peer-led working group within the water sector to consider and make recommendations on water protection issues. The work group included stakeholders from many disciplines and used a consensus-based collaborative problem-solving approach to develop its findings. The group presented its findings to the NDWAC, which unanimously adopted the findings as Council recommendations[1].

The NDWAC identified key features of active and effective protective programs that are important to increasing security and preparedness, and are relevant across the broad range of utility circumstances and operating conditions. While identifying common features of active and effective protective programs, the NDWAC emphasized that "one size does not fit all" and that there will be variability in protective approaches and tactics among utilities, based on utility-specific circumstances and conditions. The key features are based on an integrated approach that incorporates a combination of public involvement and awareness, partnerships, and physical, chemical, operational, and design controls to increase overall program performance. In addition, they address utility security and preparedness in four functional categories: organizational, operational, infrastructure, and collaborative.

[1] The NDWAC Report is available at http://www.epa.gov/safewater/ndwac/pdfs/wswg/wswg_report_final_july2005.pdf.

As part of the charge provided to the Critical Infrastructure Partnership Advisory Council (CIPAC) Metrics Workgroup for Water, the NDWAC's key features were revised for alignment with the Water Sector-Specific Plan for Critical Infrastructure Protection (Water SSP). The key features will align closely with the SSP goals and objectives, making them consistent with the document that acts as the baseline or standard for all-hazards, risk management efforts.

1.2 Case Study Goals and Objectives

Water sector security and preparedness are the foundation for mitigating consequences to people and property. Implementing key features of an active and effective protective program, should better position water sector utilities to protect their facilities and the people they serve. Highlighting the features demonstrates the importance of collaboration and relationship building at the local and state level. The "one size does not fit all" approach towards protecting the water sector is evidence of the flexibility the practices provide all water sector utilities.

The following goals and objectives guided the work of the project team and provided the guidance team with a framework for supporting the Case Study effort.

Goals:

- Document and demonstrate how water sector utility practices that implement one or more of the key features of an active and effective protective program can achieve benefits, protection, and better resiliency.
- Develop a case study methodology that is easily replicated and can serve as a model for other communities and water sector utilities across the country.

Objectives:

Collaboration: Improve understanding among participants of the relationship between implementing key features of an active and effective protective program and how other agencies in the community are linked through these practices.

Multiple Benefits: Document how implementing key features of an active and effective protective program provides benefits to the utility and the community.

Barriers and Mitigation: Identify barriers to implementing protective programs and document how barriers were mitigated.

Performance Measures: Identify and document success measures from implementing practices.

Next Steps for Seattle-King County: Present the Case Study findings to elected officials to raise awareness of the importance of making policy decisions that encourage and enable implementing active and effective protective programs in the water sector.

Next Steps for the Nation: Promote the Case Study model in other areas of the country to raise awareness about successful practices in Seattle-King County, explore existing practices being implemented in those areas, and encourage water sector utilities in those areas to implement key features of an active and effective protective program.

1.3 Audience and Content

The audience for this Case Study is broad and includes water sector utilities of all sizes, elected officials, local and state emergency management agencies, and leaders of critical infrastructure organizations across all sectors. The report provides a valuable message to the entire spectrum of stakeholders about the importance and feasibility of implementing security and preparedness practices that make our water sector infrastructure and communities safe and resilient. In addition, these practices may assist the water sector in building upon or modifying programs already in place.

SECTION 2: SELECTING SEATTLE-KING COUNTY FOR THE CASE STUDY

2.1 Why Seattle-King County?

Officials in Seattle-King County have a track record of developing protective features, practices, staffing networks, and relationships between multiple agencies. In addition, proactive planning by officials has resulted in successes in securing grants, and industry-wide recognition of the region's status as a leader in addressing water sector security and preparedness. This responsibility to preparedness has prospered in Seattle-King County, even as disaster planning has lost momentum in other regions of the United States.

Another key to inviting Seattle-King County to participate in the Case Study is the high level of support shown by local elected officials, including the Mayor of Seattle, Greg Nickels. Mayor Nickels challenged the city and region to be among the best in the nation in addressing water sector security and preparedness.

The region also has been able to tap into a network of resources across the state, and even in other states, by working with organizations such as the Pacific Northwest Economic Region (PNWER). PNWER is a public/private partnership promoting sustainable economic development and environmental stewardship in five U.S. states, two Canadian provinces, and one Canadian territory. For example, Seattle-King County was involved in the Blue Cascades preparedness exercise series organized by PNWER and supported by the U.S.'s Federal Emergency Management Agency, among others.

2.2 Current Collaboration in Seattle-King County

The Regional Disaster Plan in Seattle-King County promotes community involvement and collaboration and incident managers can escalate an emergency to the County level, as needed. This process has fostered mutual aid planning within the County and altered the culture of agencies by promoting cross-disciplinary teamwork. Teamwork also helps to integrate critical infrastructures, such as drinking water and wastewater utilities, into the bigger picture of regional disaster planning.

In support of HSPD-8, the Seattle-King County water sector has taken steps to build relationships with fire, police, and public health agencies. Several utility representatives joined regional security and preparedness committees and, with the HSPD-8 designation, the water sector became eligible for federal Urban Area Security Initiative (UASI) funds to support ongoing security and preparedness programs. Tabletop exercises and monthly regional committee meetings also foster important relationships between the water sector and other agencies, many of whom received UASI funding.

In addition, Seattle-King County agencies have agreed on the need for more security and preparedness training and drills to identify gaps and establish effective communications and relationships among agencies. By standardizing data flows and communication methods, utilities and collaborative partners hope to better communicate with each other during emergency events, and also hope to share response capabilities that each can supply during an emergency.

SECTION 3: CASE STUDY APPROACH

EPA established a project team that included staff from the Office of Water, contractor CSC, and subcontractors CH2M HILL and Ross & Associates. The project team was responsible for Case Study design, identifying the Case Study area, facilitating workshops and meetings, and documenting the Case Study findings and practice descriptions.

3.1 Case Study Guidance Team

A Case Study guidance team, recruited from 16 organizations, comprising 11 utilities and 5 state and local agencies to advise on the effort and to provide feedback on the practices, was chartered to assist the project team in identifying tangible benefits to the water sector and local community (see Appendix A for a list of guidance team members). Guidance team members shared roles and responsibilities, and had equal standing to participate and provide guidance to the project team. The guidance team promoted active participation in the Case Study, identified mutual benefits to the community, and provided the project team with strategic direction and feedback throughout the Case Study project. This assistance was essential to the success in identifying and validating the practices used in the community, adding credibility to the project findings.

3.2 Area Workshop

A key element of the Case Study was conducting a workshop to explore and expand on previously gathered information about practices being implemented in the Seattle-King County area. The Area Workshop brought together stakeholders from a broad spectrum of disciplines and members of the guidance team (see Acknowledgments for participant list). The workshop's objectives were to:

- Explore collaborative practices and interdependencies among the water sector and other sectors in effectively preventing, detecting, mitigating, responding to, and recovering from an all-hazard event.
- Discuss a list of Seattle-King County practices captured earlier in the study and explore how agencies were using them.
- Provide an opportunity for participants to learn more about how to help each other in security and preparedness.

The workshop built upon a list of practices and interdependencies in the region already identified through discussions with water sector utilities and focused on the collaborative practices employed in the region. Workshop participants reviewed the practices and identified interdependencies, barriers, incentives, and multiple benefits. Attendees participated in five collaborative practice workgroups in the morning and five collaborative agency workgroups in the afternoon. Morning workgroup participants discussed detailed information on specific collaborative practices; afternoon workgroup participants discussed inter-agency needs and connections or linkages. Workshop session leaders also invited attendees to participate in a discussion to generate recommendations for future case study workshops.

3.3 Sample Practice Selection and Information Gathering

Following the Area Workshop, the guidance team reviewed key findings from the workshop, determined which practice discussions should occur, and provided feedback on the format and content of a sample practice description.

The guidance team used the following criteria to select practices:

- ✓ Active
- ✓ Effective
- ✓ Sustainable
- ✓ Current
- ✓ Exemplary
- ✓ Performance tested
- ✓ Information available
- ✓ Relevant to the features

Not all practices met every criterion listed above, but 23 practices with the most information were developed into detailed practice descriptions. The practice descriptions are included in Section 5 as examples for stakeholders to use in developing their own customized approaches to security and preparedness. Workshop participants mentioned many additional practices, but specific details were not available within the time frame of the Case Study. These practices were still found to be relevant and worth exploring further in future case studies and are captured as a list of additional practices in Appendix B. In all, the project team conducted in-depth discussions with 16 participating water sector utilities during the summer of 2006, which resulted in the 23 practice descriptions highlighted in this report.

3.4 Case Study Results Review

The guidance team met to review the draft Case Study report, evaluate the effectiveness of the Case Study, discuss plans for presenting results to local public officials, and suggest next steps for the Seattle-King County area. The guidance team also provided recommendations to EPA on a plan to disseminate the Case Study results and conduct future case study projects in other locations around the country.

SECTION 4: RESULTS

The Case Study is the first comprehensive effort to document the practices water sector utilities are implementing to improve the security and preparedness of their systems and protect the people and community they serve. The Case Study produced results that were both anticipated and surprising, and begins to answer questions other utilities have about the types of practices that are being implemented to make water sector facilities more secure and protect the public. The Case Study team anticipated answering utility questions about protective practices. What surprised the project team is the number of elected officials and leaders from other sectors and business that are interested in the practices because of the interdependent relationship between other sector facilities, such as hospitals and food production, which rely on a secure and resilient water sector.

Although the 23 documented sample practices are from a single region, the lessons learned can be adapted to other communities across the country to increase local and regional awareness, and give utilities examples of practices currently being used by their peers. The Case Study provides a methodology that can be replicated in other parts of the country and a framework for documenting additional practices by other utilities that supports expanding active and effective protective programs.

4.1 Benefits of Implementing Practices to Utilities

Utilities that implement practices built around an active and effective protective program are able to achieve benefits that result in reduced risk to their system and the communities they serve. For example, enhanced protection of bulk water metering stations at one utility led to increased protection of the distribution system and substantial cuts in operating costs that, by themselves, were enough to justify the practice (refer to Practice Description #12). This particular practice also improved the monitoring of bulk water usage, which resulted in a significant drop in water quality complaints caused by hydrant abuse that affected water quality. More reliable systems, cost savings from mitigating effects of an event, and increased customer confidence and satisfaction are just a few of the potential benefits.

Utilities that implement protective practices and make their customers aware of their efforts typically increase customer satisfaction. This satisfaction comes from the awareness of the important role that protective practices play in keeping facilities secure, and more often the satisfaction comes from a feeling that the utility is committed to keeping its customers safe.

For drinking water utilities, a survey of critical customers such as those on dialysis machines can improve the utilities' ability to respond to special needs customers in the event of an emergency while also educating customers on the need to assess personal vulnerabilities and prepare accordingly. The more community awareness there is about potential risks, the greater the opportunity for utilities to work in partnership with local officials and the community at large to encourage and improve practices that support a safe and reliable water sector.

Many practices illustrate the benefits of collaboration between agencies. For example, water sector collaboration with law enforcement and public safety agencies enhances local emergency response and improves the effectiveness of regional disaster preparedness exercises (refer to Practice Description #6). These collaborative practices can also create a sense of ownership and responsibility between agencies and lead to faster response times, foster trust among local emergency responders, and create a more efficient working environment during an emergency. Active participation by the water sector in collaborative practices enables traditional first responders to recognize water utilities as an essential team member in emergency preparedness planning and a partner in first response, as defined in HSPD-8.

Another benefit of promoting active and effective protective programs is that employees well-trained in disaster response are able to analyze their systems and recognize opportunities to improve operations on a daily basis (refer

to Practice Description #23). Preparedness training for employees also benefits the broader community because the better people understand their role in an emergency; the better able they are to handle the response. Additionally, worker safety often improves when utilities update their policies to conform to new security and preparedness practices.

4.2 Benefits to Case Study Participants

In addition to benefiting from the information contained in the practice descriptions, utilities and agencies who actively participated in the Case Study also benefited from the personal interactions during Case Study meetings and the area workshop. The interactive format of the meetings and workshop encouraged participants to work collaboratively in groups to complete meeting objectives and fostered further collaboration after the Case Study.

Additional benefits to Case Study participants include:

- Greater awareness of resources available for planning and for assistance
- New found understanding of practices used by other agencies to improve response coordination during emergencies
- Increased understanding and familiarity of practices and terminology between agencies and staff
- Cross-sector cohesiveness, networking, and collaborative practices generated by gathering a diverse group of participants from the water sector, fire, police, telecommunications, power, and other agencies
- Potential to collaborate
- Exposure of participants to existing resources or services, such as the Wireless Priority Service (WPS), Government Emergency Telephone Service (GETS), and Telecommunication Service Priority (TSP), that allow a utility's calls to receive top priority when telephone networks are stressed during an emergency or disaster

4.3 Challenges in Developing a Security and Preparedness Culture

The Case Study revealed a persistent theme about the water sector's view of its role in an emergency and the views outside agencies have of the water sector's role in an emergency. The water sector and other sections within public works traditionally are considered a low priority for security and preparedness funding by the traditional first responder groups that receive federal money, which further limits the opportunity to focus on security planning and preparedness. In addition, within the sector, opportunities to plan and prepare for a future crisis are often deferred to meet the demands of daily operations.

Many utilities acknowledged that preparedness practices are expensive to implement and/or maintain, and that training can be costly and time-consuming. Overall within the region's water sector, there has been a general lack of support for security and preparedness initiatives and this lack of resources remains a significant barrier. Despite these difficulties, the water sector in the Seattle-King County area was able to implement the 23 described active and effective protective practices, and receive funding assistance by coordinating with traditional first responders.

4.4 Key Findings

The Case Study findings listed below are fundamental to ensure the success of local communities and the water sector in implementing security and preparedness programs.

Partnership is Essential: *Enhancing water sector security and preparedness requires partnerships with other interdependent sectors.*

Seattle-King County's experiences and practices point clearly to the need for water sector utilities to build partnerships with community emergency management, public health, hospitals, law enforcement, transportation, telecommunications, and other agencies/sectors to ensure a comprehensive approach to security and preparedness.

A first step in building these partnerships is to generate understanding about the critical aspects of drinking water and wastewater provision within a community, and the first responder role that water sector utility staff will play during an emergency.

Think Long Term: *Developing an active and effective protective program is a long-term process—iterative and at times frustrating.*

Water sector utilities and their community partners should feel comfortable adopting practices incrementally and anticipate the need to adapt practices as experience reveals opportunities for continual improvement. Communities should also promote a more collaborative emergency management culture so that sectors now operating in isolated "stovepipes" can work to break down barriers, improve communication, and readily share expertise and resources. A critical lesson learned in the Seattle-King County area was the need for a fundamental shift in thinking about culture and long-term commitment. Implementing practices that support an active and effective protective program is part of a long-term strategy for continual improvement.

Secure Support from Leadership: *Initiating and sustaining an active and effective protective program requires strong support from elected officials and emergency operations leaders.*

Seattle-King County partners identified two factors critical to the region's success: (1) strong support from municipal and county elected officials; and (2) efforts by regional emergency operations staff to reach out to other interdependent sectors. These factors point to the importance for leaders in government, utilities, and emergency management to set the tone for implementing active and effective protective programs, and to work collaboratively on continuous improvement.

Think Broadly: *Pursuing a collaborative and community-oriented active and effective protective program produces multiple benefits*.

Collaboration leads to faster response times and a more effective and efficient working environment during an emergency. Other practices produce direct and operational cost savings, improved protection, and decreased operating costs. In addition, improved protective practices boost customer satisfaction and customer awareness of security and preparedness.

SECTION 5: PRACTICES

Strong security and preparedness is not an end state, but a process. For Seattle-King County agencies, as for any utility or community, improvements are gradual and continuous. By building from earthquake and storm events, local agencies like the King County Office of Emergency Management were able to reach out to each other and galvanize collaboration among utilities and other agencies within the region. The water sector in any community can benefit from the efforts in Seattle-King County by reviewing their region's practices and enacting/enhancing their own program to reduce risk with an all-hazards approach to preparedness.

There are hundreds of highly effective practices in use today by the water sector and other sector infrastructures. Many are in collaboration with community partners, while others are implemented solely by a utility. This Case Study report is considered a beginning; by describing 23 of them, EPA hopes to capture and share many more practices identified in future efforts across the country.

This EPA report, and others that may follow, represent the consensus judgment of EPA, water sector, and public sector organizations that have participated in a community case study project. This and succeeding reports and practice descriptions are neither official EPA guidance nor requirements.

Sample Practices

For the purposes of the Case Study, a practice is defined as an action area that includes specific tools, behaviors, activities, systems, policies, and/or procedures that promote a protective posture and enhances the process for planning, mitigating, responding to, and recovering from all-hazards events.

The project team identified practices under one or more of the key features of an active and effective protective program (Appendix C) recommended by the NDWAC. At least one practice was identified as meeting each of the key features.

Practices were evaluated to determine if they fell into one or more of the following categories:

Organizational practices relate to the agency's overall structure and administration.

Operational practices relate to activities, often daily routines, required to meet the agency's mission.

Infrastructure practices relate to the physical system.

Collaborative practices involve interaction with one or more outside agencies.

Although many practices identified during the Case Study straddled categories, the project team selected one category for each practice to streamline organization of the report. For example, enhancing law enforcement response with video assessment involves the "infrastructure" activity of installing a video surveillance system, but is also "collaborative" due to the coordination with a law enforcement agency. For the purposes of this report, the sample practice was categorized as "infrastructure" because the video assessment was the primary focus of the practice (see **Table 5-1**). The amount of information provided is related to the amount of information made available to the project team. All summaries provide the reader with enough information to understand the meaning, context, and applicability to the reader's organization.

Table 5-1 lists the 23 practices from Seattle-King County described in the report and identifies which of the key features (Appendix C) corresponds to each. In several examples, the practice includes more than one feature category for that practice. The complete practice descriptions (approximately two pages each) are included immediately following Table 5-1. The practice descriptions are a sampling and do not represent the full range of water sector security and preparedness practices taking place in Seattle-King County.

TABLE 5-1: Twenty-three Practices from Seattle-King County

ID Number	Sample Practice	Collaborative	Infrastructure	Organizational	Operational	Corresponding Feature and Number (see Appendix C)
1	Interdependencies forum to build regional preparedness	✓			✓	Business Continuity Planning; and Partnerships (7 & 8)
2	Utilities helping utilities through mutual aid and assistance agreements	✓			✓	Business Continuity Planning; and Partnerships (7 & 8)
3	Regional contamination response network	✓			✓	Contamination Detection; and Partnerships (3 & 8)
4	Conducting disaster exercises for regional preparedness	✓			✓	Business Continuity Planning; and Partnerships (7 & 8)
5	Educating public officials	✓				Communications; and Partnerships (9 & 8)
6	Water sector collaboration with law enforcement to enhance local emergency response	✓				Communications; and Partnerships (9 & 8)
7	Drinking water and wastewater agency collaboration with other sectors on regional emergency planning	✓			✓	Business Continuity Planning; and Partnerships (7 & 8)
8	Supplying emergency water via temporary piping		✓			Infrastructure Resiliency (6)
9	Enhancing law enforcement response with video assessment	✓	✓			Access Control; and Partnerships (5 & 8)
10	On-site sodium hypochlorite generation for wastewater disinfection		✓			Infrastructure Resiliency (6)
11	Securing utility information		✓			Access Control (5)
12	Enhanced security of distribution system through bulk water metering stations		✓			Access Control; and Infrastructure Resiliency (5 & 6)
13	EPA assistance for water contamination events	✓			✓	Contamination Detection; and Partnerships (3 & 8)
14	Emergency preparedness survey of critical customers	✓			✓	Partnerships (8)

ID Number	Sample Practice	Collaborative	Infrastructure	Organizational	Operational	Corresponding Feature and Number (see Appendix C)
15	Funding security enhancements				✓	Business Continuity Planning; Security Resources/Measures; and Access Control (7, 2, & 5)
16	Using a clear message for risk communications	✓			✓	Communications (9)
17	Security and emergency response metrics				✓	Security Resources/Measures; and Vulnerability Assessment (2 & 4)
18	Radiological contamination event procedure for a combined sewer system				✓	Security Resources/Measures; and Partnerships (2 & 8)
19	Utility response to changing threat levels				✓	Threat-Level Based Protocols (10)
20	Procedures for contractor and vendor access		✓		✓	Access Control (6)
21	Updating a vulnerability assessment				✓	Vulnerability Assessment (4)
22	Creating and maintaining a security culture			✓		Explicit Commitment/Promote Awareness; and Defined Roles (1 & 7)
23	Training on security and emergency response			✓	✓	Explicit Commitment/Promote Awareness; and Defined Roles (1 & 7)

1: Interdependencies Forum to Build Regional Preparedness

Corresponding Feature Description:

Emergency Response Plan (ERP) Tested and Updated; and Partnerships

Category Type:

Collaborative; Operational

General Description: Officials in King County, Washington, hosted their first Interdependencies Forum (Forum) in November 2005. King County is the most populous county in the state and is designated as Washington State Homeland Security Region 6, one of nine Homeland Security Regions in the state. The one-day Forum brought together representatives from the 17 federally recognized critical infrastructures and was driven by requirements contained in the Washington State Homeland Security Region 6 Critical Infrastructure Protection Plan (CIPP), a decision-making tool for prioritizing infrastructures and allocating funding resources.

The Forum helps infrastructure representatives to:

- Connect with other owners and operators in their sector to share best practices and identify the most critical assets within their sector.
- Provide information on initiatives and tools that may assist with assessing vulnerabilities.
- Understand their dependencies related to other infrastructure sectors.
- Connect with other sectors to identify and protect the cross-sector assets that are considered most vital to the health and safety of the communities, the economy, and the environment.

Resources Required: The Forum hosts were able to keep the costs manageable by using existing County personnel to organize, conduct, and report on the Forum activities. Additional funding to support the Forum was secured through U.S. Department of Homeland Security (DHS) grants and from the private sector. Members of the Forum planning team invested approximately 4–8 hours per month in meetings and document preparation. A consultant initially assisted with facilitation of the Forum; however, future plans call for members of the region's Critical Infrastructure Protection Workgroup to assist with planning and facilitating future forums.

Roles and Responsibilities: The Critical Infrastructure Protection Workgroup comprises representatives from the following six sectors considered most critical to maintain in an emergency and tasked with planning the annual forum:

1. Energy
2. Water
3. Information Technology (IT)
4. Telecommunication
5. Transportation
6. Healthcare Systems

The workgroup's mission is to "determine regional critical infrastructure, establish priorities, evaluate requests, and provide appropriate resources to protect critical infrastructure in King County from terrorist attacks and all-hazard emergency events."

Workgroup members attend monthly meetings, review plans, represent their sectors in identification of interdependencies, and recommend priorities for funding to support preparedness efforts in organizing the Forum.

The King County Office of Emergency Management (OEM) provided a staff person to lead the workgroup and organize the workgroup's efforts. The OEM representative also coordinated with a larger regional interdependencies group and the Pacific Northwest Economic Region (PNWER), a bi-national, public-private partnership representing three Canadian provinces and five U.S. states.

Collaboration with Other Partners: In addition to coordinating with regional members from the priority sectors, many forum participants also participate in multi-state/bi-national table-top exercises on critical infrastructure protection. The Blue Cascades series of exercises are in support of PNWER's initiative called the Partnership for Regional Infrastructure Security, whose purpose is to develop a regional preparedness plan for dealing with large-scale emergencies in the region.

Barriers: Forum participants face a number of barriers for achieving their present and future goals including:

- Critical infrastructure sector representatives may not understand the value of the Forum to their agencies and not allocate the time to attend.
- Critical infrastructures can have different geographic boundaries, which increases the difficulty of infrastructure protection planning.
- Funding from DHS is limited, and new sources of funding will likely be needed in order to sustain efforts.

Lessons Learned: Forum participants learned valuable lessons that will help improve future efforts and serve as a model for others that want to replicate the practice, including:

- Developing relationships between interdependent sectors is critical to cooperating on joint activities.
- "Champions" need to be identified in each sector and play a leadership role.
- Interoperable communications mechanisms are essential to share threat and response/recovery information.
- Command and control issues dealing with cross-border threats and hazards need to be addressed. The principles and concepts of the National Incident Management System (NIMS) and the Incident Command Structure (ICS) need to be used.
- Understanding regional and cross-border interdependencies is important.

Success Measures: The Forum was considered a success based on the following outcomes:

- The Forum had a high participation rate; representatives from all 17 federally recognized critical infrastructures attended.
- The Forum satisfied a key requirement in the Region 6 CIPP.
- The action items identified in the Forum have been developed into a regional action plan, which will be reviewed and updated at the next Interdependencies Forum.

Benefits and Incentives: The networking opportunity afforded at the Forum provided participants with potential continued benefits, including:

- Having a voice in an organization that can represent them regionally and nationally
- Collaborating and participating in emergency training exercises
- Developing mutual aid agreements with interdependent or similar infrastructures
- Creating a more clear and current understanding of regional preparedness, and how it affects their organization
- Creating access to Homeland Security grant funding by participating in a regional emergency planning group
- Developing key relationships with infrastructure representatives, which may help to increase routine cooperation and communications

2: Utilities Helping Utilities through Mutual Aid and Assistance Agreements

Corresponding Feature Description:

Emergency Response Plan (ERP) Tested and Updated; and Partnerships

Category Type:

Collaborative; Operational

General Description: The primary objective of a mutual aid and assistance agreement is to facilitate rapid, short-term deployment of emergency support to restore critical operations at an affected utility or group of utilities in an efficient and effective manner. Mutual aid and assistance agreements accomplish this by providing the framework through which private and public utilities share resources with one another, without the need for a declared state of emergency. They also include provisions to address issues such as liability, workers' compensation, and reimbursement.

While mutual aid has been practiced by fire and law enforcement officials for hundreds of years, it is relatively new to other emergency responders, such as those responsible for securing water and wastewater critical infrastructure. Thanks to the efforts of existing Water and Wastewater Agency Response Networks (WARN) and strong support from the U.S. Environmental Protection Agency (EPA) and water sector partners such as the American Water Works Association (AWWA), mutual aid and assistance agreements are now being developed between utilities across the country.

A model mutual aid and assistance agreement and guidelines for developing a WARN, both outlined in the May 2006 "Utilities Helping Utilities" white paper authored by AWWA, can be found at www.NationalWARN.org.

Resources Required: The resources associated with developing and maintaining a mutual aid and assistance network are minimal. In-kind services are typically used to draft an agreement and generate interest amongst other utilities. Once an agreement is finalized, utilities must determine the best way to facilitate activation of the agreement during a disaster. Some utilities invest in dynamic Web sites with sophisticated resource matching databases while others opt for an on-the-fly message board where human intervention is required to match resources with needs. Specifically, the resources required to develop and maintain a mutual aid and assistance agreement include:

- In-kind contribution of time from members
- Legal fees, or in-kind legal support, associated with drafting and finalizing an agreement
- Marketing the agreement through participation in conferences and workshops
- Development and maintenance costs associated with a Web site (if applicable)
- Meeting space to hold regular meetings between members

Roles and Responsibilities: Specific roles and responsibilities are typically defined within the mutual aid and assistance agreement, and can vary from one agreement to the next. Initially, a Leadership Team is tasked with identifying the utilities, associations, and agencies that should play a major role in the implementation of the mutual aid and assistance agreement. They facilitate meetings to promote interest in the agreement, and eventually recommend representatives for a Steering Committee. The Steering Committee is responsible for identifying a Chair or Leader, determining membership criteria, and outlining the governing principles of the agreement. The Chair is responsible for ensuring an agreement is then drafted, based on

input from the group. The agreement then defines the roles and responsibilities of requesting and assisting member utilities in response to a disaster, as well as how other members help facilitate that process.

Collaboration with Other Partners: Collaboration is vital to maintaining strong mutual aid and assistance networks. On February 15, 2006, eight major water sector associations, representing water and wastewater utilities and regulatory agencies, signed a joint policy statement promoting the development of mutual aid and assistance networks as a necessary step to securing our nation's water and wastewater critical infrastructure. A strong partnership between these associations and utilities provides the framework for a better prepared and more resilient water sector.

Coordination with the state and local emergency management agencies is also essential.

Barriers: Mutual aid and assistance agreements provide many benefits to participating utilities. However, potential barriers exist and may include:

- Integrating intrastate WARN response with state emergency management agencies requires ongoing collaboration and education to avoid apparent duplication with statewide mutual aid agreements for public assets.
- Interstate WARN agreements are challenged by differences in state laws.
- Currently, the ability for private sector resources to deploy under the Emergency Management Assistance Compact (EMAC) is limited.

Lessons Learned: Evaluating response to past events is the best way to prepare for the future. Events such as 9/11 and more recently, Hurricane Katrina, have identified a need for mutual aid and assistance agreements because:

- Utilities require specialized resources to sustain operations.
- Emergency response activities and other critical infrastructure rely on water supplies.
- Utilities must provide their own support until state and federal resources are available.
- Large events impact regional areas, making response from nearby utilities impractical.
- Disasters impact utility employees and their families, creating a greater need for relief from outside sources.
- Agreements must be established prior to an event for federal reimbursement considerations.

Success Measures: One of the best ways to measure the effectiveness of an agreement is to evaluate how effectively, efficiently, and appropriately requests for assistance are met. This evaluation can take place in the form of an after-action report, summarizing both the strengths and weaknesses of response actions. The report should examine at least:

- How well requests were met and what percentage of those requests were addressed in a timely manner
- Monetary and indirect value added due to decreased service downtime (i.e., cost-avoidance for businesses and restoration of hope within the community)
- Ability of critical customers such as fire and health responders to continue their operations

Benefits and Incentives: Numerous benefits exist for mutual aid and assistance agreement members including:

- Expedited access to specialized resources
- Improved planning and coordination
- Consistency in response with National Incident Management System (NIMS) guidelines
- Voluntary and cost-free participation
- Articles addressing response issues such as member indemnification, workers' compensation, and reimbursement
- Ability to activate prior to an emergency declaration

3: Regional Contamination Response Network

Corresponding Feature Description:

Contamination Detection; and Partnerships

Category Type:

Collaborative; Operational

General Description: Through a grant from the U.S. Department of Homeland Security (DHS), a utility in the region wanted to take the lead and develop a regional response network for responding to potential drinking water contamination events. The utility hired a consultant to identify and survey potential partners for collecting data, including information on agency decision-making authorities, and sampling and communications capabilities.

Twenty-eight participants from a network of 16 agencies attended a workshop that used a drinking water contamination event to determine the region's response capabilities. During the workshop, participants drafted a statement of organizing principles, identified existing response groups, guidance documents, and systems with which the network should align. Participants developed a listing of single points of contact, agreed to implement a 24-hour phone number to activate their agency during an emergency, and developed action items for the network and region. A decision-making and communications flow exercise enabled participants to compare information about their agency's communications needs during a water contamination emergency, and resulted in the creation of a draft communications model for use during an emergency.

Following the workshop, participants formed a steering committee to further promote the network. Thirty agencies in the region participate in the response network.

Resources Required: Approximately $100,000 was spent to develop the materials, collect research information, plan and facilitate the workshop, and write up the results.

Roles and Responsibilities: Each agency representative participated in pre- and post-workshop meetings, and coordinated with their respective coworkers to identify issues of concern and raise them during the workshop. Additionally, representatives had decision-making authority so that critical decisions could be made at the workshop.

Collaboration with Other Partners:

Collaboration between local agencies included utilities, police, fire, public health, hospitals, and emergency management.

Barriers: Barriers included:

- The existence of other local response networks dilutes the purpose of a network specific to water contamination
- Lack of funding and commitment to lead the network inhibit development and growth

Lessons Learned: An important lesson learned was that creating a contamination response network was critical for providing local response capability to a contamination event. EPA provides similar emergency capabilities in the Seattle-King County area that enhances a local contamination network's ability to respond (see Practice Description #13).

Success Measures: In the absence of an actual contamination event, the success of a response network can be measured by looking at specific instances of increased cooperation between network members. This can be evidenced by:

- Instituting or increasing the number of joint contamination exercises between member agencies

- Updating response plans, contact lists, and communication procedures based on joint exercises
- Establishing mutual aid agreements between utility network members
- Adding new members to the network

Benefits and Incentives: Responding to an actual or suspected contamination event requires collaboration between the utility, the local health department, law enforcement, and emergency management. Each has a distinct responsibility to protect the health and safety of the public. Having a contamination response network provides a vehicle for engaging these partners as a group, which can lead to the pooling of resources and reduce costs. Additionally, federal security grants are increasingly being awarded with preferences towards regional and multi-agency approaches towards preparedness.

4: Conducting Disaster Exercises for Regional Preparedness

Corresponding Feature Description:

Emergency Response Plan (ERP) Tested and Updated; and Partnerships

Category Type:

Collaborative; Operational

General Description: To enhance preparedness, participants in this activity conducted three regional disaster preparedness drills, known as the Blue Cascades Series, which focused on public and private critical infrastructure interdependencies. The U.S. Department of Homeland Security has identified critical infrastructure exercises in the National Infrastructure Protection Plan (NIPP) as the model for addressing critical infrastructure security issues on a regional level.

The number of attendees at each of the three Blue Cascade exercises ranged between 100 and 200 representatives from regional public and private sector organizations. Participants included public and private infrastructure sector stakeholders from the United States and Canada, and federal, provincial, state, and local agencies. The activity also included exercise planning, as well as a workshop to follow up on the findings and recommendations of the after-action report.

Developing an exercise has been summarized into the following seven steps:

Step 1. Create a regional cooperative initiative and partnership comprising key stakeholders, including the leadership of senior local, state, and private sector leaders.

In this case, the core group of 30 to 45 organizations became the steering committee of the partnership and represents: major utilities; key local, state, regional, and federal government organizations; businesses; nonprofits; and community institutions such as hospitals and academics. Additionally, associations that represent broad organizational memberships were invited.

Step 2. Develop and conduct an interactive, educational workshop(s) to provide necessary information to key stakeholders on regional infrastructure interdependencies, disaster preparedness, and security challenges.

A primary goal of the workshop(s) was to develop an understanding of regional interdependencies and establish a framework for trust and collaboration to advance regional preparedness and response.

Step 3. Develop and conduct a regional infrastructure interdependencies exercise based on scenarios designed by members of the core stakeholder group, and other interested organizations, which reflect their interests and concerns regarding a major disaster.

The objectives of the exercise are not to test plans or procedures, but are designed to:

- Provide participants with an awareness of baseline regional interdependencies and associated physical and cyber vulnerabilities.
- Identify preparedness gaps.
- Develop action items and next steps to solve issues exposed by the exercises.

Step 4. Produce a report based on the lessons learned from the exercise with findings and recommendations that have been coordinated and validated by the key stakeholders.

Step 5. Develop and conduct an Action Planning Workshop with the exercise participants. This workshop should focus on implementing the recommended activities from the exercise reports and identify specific projects to these ends.

Step 6. In coordination with key stakeholders, prioritize the projects identified in Step 5 into an

Action Plan. The Action Plan activities should be incorporated into regional and organizational preparedness strategies, plans, and funding requests.

Step 7. Within the region, create working groups with lead government agencies and private sector organizations that will undertake development of a cross-sector approach to implementing the short-, medium-, and longer-term activities identified in the Action Plan.

Resources Required: The total cost of planning and conducting the seminar, exercise and action planning workshop was $238,000; this amount does not include the volunteer efforts by the design team or participants.

Roles and Responsibilities: The key roles and responsibilities for this practice are as follows:

- The regional organization leading the preparation of the exercises should obtain funding, identify the scope of the exercise, and identify a scenario design team. It should then periodically meet with the design team to review and refine the scenario.
- In parallel with overseeing the scenario design work, the organization should arrange all planning workshop and exercise logistics, including notifying and scheduling participants, securing the facilities to be used in the exercise, and developing materials for the exercise.
- After the exercise, the regional organization collects all exercise feedback and materials and prepares an after-action report with recommendations. This report is then reviewed in a full-day meeting with the design team, the evaluation team, and in some cases the participants, to comment on the report and to prioritize the actions. The report is then finalized and a meeting is conducted to refine the resulting action plan.
- The design team is responsible for designing the scenario within the scope dictated by the regional organization, participating in a pre-exercise walk-through, and helping with the review of materials for the after-action reports.
- The evaluation team also participates in the pre-exercise walk-through; documents the successes, failures, and lessons learned from the exercise; presents their findings; and participates in drafting the after-action report.

Collaboration with Other Partners: This entire practice is a collaborative process between sectors and public and private agencies. The focus is to identify interdependencies and further regional preparedness through collaboration. Additional collaboration can occur among regional organizations by sharing information on planning and implementing exercises as well as the after-action reports and other outcomes of the exercises.

Barriers: The most significant barrier is balancing the need for comprehensive representation among participants with the inherent difficulties that emerge from trying to coordinate too large a group. This group has varied backgrounds, knowledge, experience, constraints, and capabilities that should be considered in the exercise design and conduct, as well as follow-up planning to prepare the region, but it is feared that the group cannot sustain many more members.

Lessons Learned: The overall practice includes a process for identifying and applying lessons learned to constantly adapt and improve the practice. Lessons learned specific to this case include the following:

- The core partnership is located in the Puget Sound region; however, several smaller metropolitan partnerships exist in Anchorage, Alaska; Vancouver, British Columbia; Edmonton/Calgary, Alberta; and Portland, Oregon. Engaging potential participants through smaller regional groups may allow the organizing agency to recruit a greater diversity of participants without significantly increasing effort.
- The participants tend to be more from the core location of the organization than from outlying geographical areas.
- The growth has occurred organically, based on word of mouth. Thus, providing successful exercises and good follow-up planning attracts new participants from the region and across sectors.

Success Measures: For regional organizations seeking to undertake a similar activity, the success of the exercises themselves will be determined based on the specific objectives of the exercise and the after-action report and evaluation. For evaluating the success of the process, the organizers can look at several factors, including:

- Evaluation forms filled out by participants
- Projected costs vs. actual costs, and the success in securing supplementary funding, like homeland security grants
- Deadlines met for meetings and developing materials
- Repeat and expanding participation (although, as mentioned, the size of the group should remain manageable)

Benefits and Incentives: This activity presents many benefits and incentives to participating agencies, including:

- Participants in the practice build relationships that can improve cooperation and response to many other types of events.
- Interdependencies and gaps in a response are identified before an incident occurs, allowing participating agencies to develop plans and activities to deal with these.
- Documentation of preparedness needs such as these can then support applications for homeland security grants.
- In addition to homeland security grants, participating agencies can pool resources and funding, lowering the overall cost to individual agencies.

5: Educating Public Officials

Corresponding Feature Description:

Promote Communication; and Establish Partnerships

Category Type:

Collaborative

General Description: This utility established, and is maintaining, an ongoing relationship with local public officials to educate them on the importance of a safe and reliable water supply. The utility held one-on-one meetings with top public officials and water utility leaders to communicate the preparedness issues faced by the utility and how they impacted the community. Prior to the meetings, utility staff held discussions among themselves to decide the most critical information to provide the public officials, and provided this information to the public officials' staffers in pre-meeting briefings. Discussion topics included utility security program features, funding issues, outcomes from emergency response exercises, and interactions with other city departments.

This strategy allowed the utility to effectively communicate the true value of a safe water supply to the community, and enabled public officials to better understand that the water utility is a key component of the municipal infrastructure for promoting public safety and health.

These discussions have been extended to an annual basis and now include the entire group of elected public officials at the city and county level.

Resources Required: The most significant investments involved activities related to the meetings utility staff attended. The main cost included staff time to develop briefing and presentation content, present that content to the public officials, and conduct follow-up activities as a result of the meetings. There were also additional minor expenditures for producing briefing materials.

Roles and Responsibilities: Utility managers and supervisors from the major departments (such as customer service, operations, treatment, and distribution) needed to determine their respective issues, concerns, resources, and funding requirements for preparing and responding to a water emergency. The utility security lead acted as the utility's representative to the public officials by presenting the utility department's information and facilitating the subsequent discussion. The utility security lead required the support of a public official's liaison to provide preliminary review of utility proposals and activities; and to coordinate with the public officials on the utility program and agenda items. The public officials liaison also needed to convey to the utility security lead the interests and needs of the public officials and their constituents to better prepare the utility security lead for the meetings and discussions.

Collaboration with Other Partners: Key partners included law enforcement, fire, and information technology (IT) department officials. These partners often share budgets and should coordinate with each other regularly. A water emergency would directly affect a fire departments' ability to provide adequate fire protection. Law enforcement may serve many roles, including site security and crowd control, or assist with door-to-door notification of water-use restrictions in the event of a water emergency. The IT department may need to be accessed to coordinate communication between these partners and the utility. Obtaining their support for utility security proposals and requests serves to bolster the utility's case to the public officials.

Barriers: The primary barriers encountered during this activity included gaining access to public officials and conveying that utility concerns are, in

fact, public safety concerns and should be of concern to public officials. In addition:

- Elected officials have a limited amount of time to allocate to the many, often competing, interests and constituents they serve. Utility proposals should be clear and supportable without overloading the officials with unnecessary information.
- Many public officials have not viewed water utility security as a vital community security concern. Changing this mindset will take time and a regular flow of information to the officials.
- Just as utility representatives should present their concerns in the best interest of the public and the public officials, they should also consider the impacts of their proposal from the perspective of the public officials.

Lessons Learned: Among the lessons learned during this activity, a common theme involved cultivating professional relationships between agency representatives. In addition:

- The credibility of the top utility officials among public officials and other first responder officials is invaluable in winning support for adequate budgets for security and preparedness.
- The role of elected officials as policy advocates for utility security and emergency management activities is critical to winning requested funding.
- An open and stable relationship between the utility and its elected officials, and first responder partner agencies, is essential to a successful utility preparedness program.

Success Measures: The most evident success measure was increased and/or continued funding of the security and emergency management activities. This reflects recognition by public officials of the challenges faced by a utility in maintaining an active and effective protective program, as well as the success of utility representatives in presenting their concerns as overall community concerns.

Benefits and Incentives: Maintaining regular meetings and communications with public officials can result in ongoing funding of the utility's security and preparedness efforts. Additionally, in an emergency, public officials will serve as representatives both to, and of, the public. Cultivating a strong relationship with them will help maintain public confidence in the utility during times of crisis.

6: Water Sector Collaboration with Law Enforcement to Enhance Local Emergency Response

Corresponding Feature Description:

Promote Communication; and Establish Partnerships

Category Type:

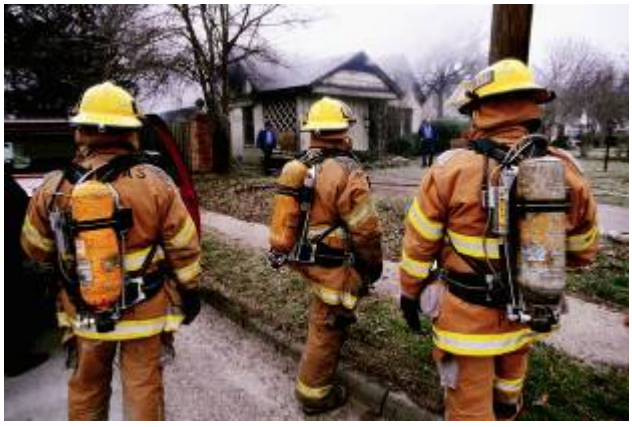
Collaborative

General Description: This utility developed a working relationship with law enforcement to enhance their emergency response capabilities. The utility and law enforcement agencies employed a number of methods to open communication channels and improve cooperation, summarized below:

- The utility and area law enforcement instituted regular monthly meetings to improve inter-agency familiarity and communication.
- Daily electronic incident reports were sent to utility, law enforcement, and crime analysis staff to increase awareness of potential threats and vulnerabilities.
- The utility became involved in the regional intelligence fusion center, allowing it to both contribute and receive threat information.
- The utility and law enforcement collaborated to create a utility-specific video for law enforcement personnel to familiarize them with water security issues.
- The utility included law enforcement personnel in reviewing and improving utility incident response procedures and facility security measures.
- The utility and law enforcement agencies involved agree that the improved communication and cooperation realized through these actions has increased the security and safety of the community.

Resources Required: The main resource associated with this activity was man-hours to perform the listed activities. These costs for staff time varied depending on the number of meetings the utility attended and the number of representatives they sent. The costs for staff attendance came out of the utility's operations budget. Additionally, the utility had to procure software and training for staff on the electronic incident reporting tool. Law enforcement agencies incurred similar labor costs to attend monthly meetings, contribute to the development of the utility video for law enforcement, and review utility security procedures and measures.

Roles and Responsibilities: The utility's Director of Security and Emergency Management and other utility security specialists met regularly with local law



enforcement agency representatives to discuss and maintain their partnership, to review patterns and trends in crime, and to develop plans to coordinate overall response. Additionally, utility security and watershed protection staff met regularly with the law enforcement officers assigned to their respective areas to discuss site-specific issues and response coordination.

Collaboration with Other Partners: The utility collaborated with their local law enforcement partners at many levels, from highly placed officials to patrol personnel. Additionally, their participation in the regional fusion center allowed them to engage emergency response and law enforcement partners beyond the utility's geographical coverage area and at the state and federal level.

Barriers: Barriers encountered while building this practice include:

- Changes in staff, which can set back communications while new relationships are built
- Additional burdens on staff time, which limited their ability to promptly and carefully review the large amounts of intelligence and incident data that were received

Lessons Learned: This practice revealed lessons learned that ranged from selecting appropriate technologies to better methods of fostering inter-agency relationships. Specifically:

- A stronger relationship with law enforcement can be developed if both entities focus on common interests, like physical security and intelligence sharing.
- The utility should be able to employ a number of different communication technologies. Text pagers and telephones may be best for relaying immediate security threat information, while emails may be the best vehicle for providing periodic reports. These should not replace face-to-face meetings and presentations, which reinforce existing relationships.
- A main focus of inter-agency contacts should be to develop teamwork and trust between agencies in order to foster a positive working relationship over time.
- Employing professionally trained patrol staff with law enforcement experience at the utility improves communication between agencies.

Success Measures: The success of this practice can be measured by monitoring regular contacts between the utility and law enforcement. Specifically, evaluating the quality and consistency of:

- Regular monthly meetings between utility and law enforcement managers and supervisors
- Daily transmission of incident reports and summaries
- Regular security reviews and patrols in conjunction with law enforcement personnel

Benefits and Incentives: Partnering with law enforcement can help the utility win federal grants through the Urban Area Security Initiative (UASI). UASI is the U.S. Department of Homeland Security's grant program, passed through to states to administer at the local level. UASI sets a strategic direction for the enhancement of regional response capability and capacity. UASI's mission is to reduce area vulnerability and prevent terrorism and/or weapons of mass destruction (WMD) incidents by strengthening the cycle of response, and ensuring that potential targets are identified, assessed, and protected.

The UASI funding board also includes law enforcement representatives. Developing strong relationships with local law enforcement agencies can improve the utility's chance of securing UASI funding as those agencies can act as advocates for the utility.

7: Drinking Water and Wastewater Agency Collaboration with Other Sectors in Regional Emergency Planning

Corresponding Feature Description:

Emergency Response Plan (ERP) Tested and Updated; and Partnerships

Category Type:

Collaborative; Operational

General Description: Water sector agencies in the area recognized the need to be involved with regional security committees in order to have a voice in grant allocation and regional planning decisions. Several utility directors from across the county divided their efforts, so each of the regional homeland security committees would have a drinking water or wastewater utility representative.

Water sector representatives attended regional meetings, promoted and received first responder recognition, and became accepted members of the regional emergency management groups. Representatives were able to participate in developing regional plans, including implementing requirements under the U.S. Department of Homeland Security's Strategic Plan.

Resources Required: The resources for this activity include time and expenses for drinking water and wastewater utility representatives to travel and attend their respective regional security committee meetings and perform associated duties. Meetings are typically held annually.

Roles and Responsibilities: It is the responsibility of each drinking water and wastewater utility representative to attend regional security committee meetings (or send an informed designee), to present the water sector's concerns and issues, and to report back to other drinking water/wastewater security committee representatives on any regional developments and opportunities reported in committee meetings.

Collaboration with Other Partners: This practice allows for regional collaboration of drinking water and wastewater utilities with fire and police departments, port authorities, local government, and citizen groups.

Barriers: No significant barriers were encountered during this activity.

Lessons Learned: Balancing the additional responsibilities of being a regional security committee representative with normal duties can prove challenging, as can securing funding for travel to the various meetings.

Success Measures: Increasing drinking water/wastewater sector representation on regional security committees, which includes:

- Increasing attendance at regional security committee meetings
- Increasing representation of water sector in regional trainings and exercises
- Increasing representation of water sector in more localized response committees and organizations, for example local fire and police chief associations

Benefits and Incentives: In addition to giving utilities a voice in the security arena, utilities have been awarded grants that typically are provided to traditional first responders such as police and fire.

8: Supplying Emergency Water via Temporary Piping

Corresponding Feature Description:
Design and Construction

Category Type:
Infrastructure

General Description: This utility's vulnerability assessment indicated that seismic activity or a malevolent act could result in significant consequences to critical customers—areas served by a sole water main or service areas isolated by bodies of water. The utility evaluated multiple scenarios and the impacts of a serious water service interruption following an emergency event or equipment malfunction, and identified those situations with the highest probability and consequence.

As a result of the evaluation, this utility purchased flexible temporary transmission and distribution lines, along with multiple associated fittings to mitigate the risk of a service interruption. Lines in several diameters (up to 12 inches) are stored on reels and staged in three locations where they can be rapidly deployed. The water pipes are flexible plastic and can be installed on the ground or under water to provide temporary water service.

Resources Required: The cost for 12-inch diameter flexible transmission and distribution lines is around $150 per foot, including associated fittings. Additional resources include annual exercises for field staff to maintain familiarity in the deployment of the temporary water mains and pipes, and inspection time to ensure the lines and related supplies are well-maintained and free of contamination.

Roles and Responsibilities: The utility staff is trained by the supplier for effective use of the flexible transmission and distribution lines. Utility staff is responsible for installation, maintenance, disinfection, sampling, and testing of the piping and fittings according to approved procedures.

Collaboration with Other Partners: The military and other utilities with experience using flexible transmission and distribution lines provided information on lessons learned and installation techniques for the pipes and fittings. Additionally, the utility incorporated the temporary transmission and distribution lines into their mutual aid agreements with other utilities, making them available in times of need.

Barriers: The primary barrier encountered for implementing this activity was overcoming staff concerns that the temporary transmission and distribution lines might compromise disinfection and water quality. The utility previously employed rigid, less versatile piping to supply emergency water, which did not pose the same concerns.

Lessons Learned: Multiple lessons learned from implementation and consultation included:

- Positioning storage locations for the lines is important for ready deployment. Key considerations include storing equipment in multiple areas and focusing on sections of the water system that are only served by a single water main.
- Proper maintenance, storage, cleaning, and disinfection are critical to effective deployment as a temporary potable water system.
- Staff gains training and experience by implementing procedures and using the equipment during routine outages due to maintenance, water main breaks, or construction activity.
- Assessing the correct sizes and amount of temporary lines needed is critical, and should be

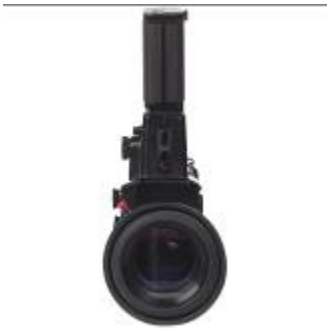
based on the utility size, geography, and single points of failure.

Success Measures: Success measures for this activity include staff accepting use of the temporary lines as standard operating procedure, regular use during routine operations, and successful deployment of the lines during training and actual events.

Benefits and Incentives: Implementing this practice provides multiple benefits for the utility and the community it serves, including:

- The temporary lines can be used for both emergencies and routine operations.
- The lines are sufficient for providing water for fire suppression, if necessary.
- The equipment can be made available as a regional resource to other water utilities.
- Customer confidence and satisfaction is increased by enhancing the utility's ability to provide safe water to its customers during emergency events, routine system failures, and service interruptions due to construction activities.

9: Enhancing Law Enforcement Response with Video Assessment



Corresponding Feature Description:

Physical and Procedural Controls on Facility Access; and Establish Local Partnerships

Category Type:

Infrastructure; Collaborative

General Description: This utility's vulnerability assessment identified priority facilities and critical assets vital to fulfilling the utility's mission. They determined the loss of one or more of these critical assets were of high consequence. The utility installed a video assessment system to increase its ability to assess alarm events that occur at, or near, critical assets. This equipment uses a Digital Video Recording (DVR) system, along with a communications system to transmit the video to a central location for viewing and assessment.

An actual security event occurred during the trial period, where the utility discovered evidence of a break-in and called local law enforcement. Law enforcement viewed the related video footage, and the individual was apprehended. After the incident, the utility and law enforcement determined that security could be further enhanced by the installation of alarms at locations where security cameras were installed. The utility then installed detection and alarm monitoring equipment. The system now alerts utility staff of the immediate need to assess video surveillance images and to contact law enforcement for an investigation, instead of waiting until an intrusion is detected during routine patrols.

Resources Required: Resources required for this practice are divided into three components:

- Purchase and installation of cameras and DVR equipment
- Building a wireless communications system to transfer images
- Installing facility alarms

Roles and Responsibilities: Roles and responsibilities include:

- Utility control center staff receives alarms, monitors the video assessment equipment, assesses unusual activity, contacts law enforcement, and prepares incident reports.
- Utility maintenance staff inspects and maintains equipment and the communications systems to assure reliable operation of the alarm and video system.
- Law enforcement officers assess field conditions at the site and take appropriate action to prevent and/or mitigate consequences, including interactions, as necessary.
- Utility management develops protocols for utility staff assessment and response, provides training, and provides supervision at critical events.

Collaboration with Other Partners:

Collaboration occurs between utility staff and law enforcement to maintain common understanding of the threats as well as the communication techniques employed during an event.

Barriers: The barriers encountered were technical, which affect the operations of the equipment. For example, difficulty with using and adjusting the monitoring equipment resulted in poor video images due to improper camera focus, panning range, and changes in light and weather conditions. The quality of the images directly affected the assessment of those images, which impacted the utility's ability to gauge the particular threat.

Lessons Learned: The lessons learned involved both technological issues related to the new equipment implementation and inter-agency relationships to ensure an efficient response. Specifically:

- Utilities need to include the use of video cameras in daily operations to keep employees trained and comfortable with the technology. This will also alert staff early to problems with the equipment from malfunctions and improper adjustments that impact the quality of the images recorded.
- Detection is an important feature of the video assessment system to indicate an immediate need to monitor the event. Installing facility alarm systems in conjunction with video assessment systems greatly enhances facility security.
- Creating relationships with local law enforcement before an incident is essential for coordinating response procedures. It is also important for law enforcement to know the reliability of information the utility is providing (a facility alarm with video of an intruder is more significant that just a facility alarm).

Success Measures: The equipment has already proven successful at identifying an intruder. In addition, the equipment has the potential to decrease the number of false alarms in cases where an employee accidentally trips the alarm and fails to report it.

Benefits and Incentives: This practice increases the utility's ability to protect its customers' drinking water supply and provide faster assessment and response to possible intrusion and malevolent acts. The enhanced relationship with law enforcement also helped to improve security and response to other facilities without equipment upgrades. This practice is an integral part of the utility's comprehensive all-hazards preparedness program.

10: On-site Sodium Hypochlorite Generation for Wastewater Disinfection

Corresponding Feature Description:

Incorporate Security Considerations into Design and Construction

Category Type:

Infrastructure

General Description: Many utilities use chlorine for drinking water and wastewater treatment. The practice of using chlorine has included both gaseous and liquid forms based on factors of convenience, reliability, and safety. As concerns increased about risks associated with malevolent acts after September 11, 2001, utilities began finding new ways to reduce this risk. Concerns for personal and environmental safety resulted in adoption of risk management practices that caused many utilities to switch from using gaseous chlorine to liquid chlorine and other alternatives. *Please note: EPA does not have an official position on chlorine use; the practice described here is utility specific.*

This practice was implemented at a small utility with less than 30 employees. The utility determined that using liquid sodium hypochlorite for one of its routine applications in wastewater treatment had been a preferred practice prior to September 11, 2001. The utility chose the process of on-site generation of sodium hypochlorite over deliveries of liquid chlorine. This process converts ordinary salt to a usable chlorine product via an electrolytic process. The utility continued to use gaseous chlorine for the remainder of its treatment processes, but changed this practice when the risk management processes required conducting emergency drills in the neighborhoods where the chlorine gas was used. This new requirement meant creating an ongoing program to prepare the local residences in the event of a release of chlorine gas. The utility chose the conversion process based on a cost-benefit analysis that considered security and public health concerns. The new practice at this utility is to use on-site chlorine generation for all wastewater treatment practices.

Resources Required: The cost of this practice is approximately $6,000 every 2 to 3 years for maintaining the on-site equipment. Additional resources are needed to pay for power, labor, and salt costs related to producing sodium hypochlorite. The utility offset some of these costs by eliminating the expense and risk of transporting and storing one-ton gaseous chlorine cylinders. Instead, the utility stores a small amount of liquid sodium hypochlorite at a concentration that is at, or below, the concentration of household bleach.

Roles and Responsibilities: There are no distinct roles and responsibilities for implementing this practice outside of the normal utility processes for operational safety.

Collaboration with Other Partners: This practice does not involve collaboration with other partners.

Barriers: There are potential financial barriers to this practice. Individual utilities will need to weigh the expense of implementing an on-site sodium hypochlorite generation system with their current system. This analysis should include other considerations such as reduced security requirements from removing the likelihood of being a target.

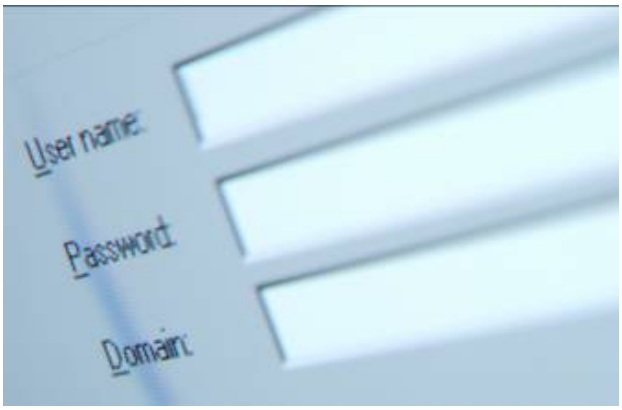
Lessons Learned: The primary lesson learned was improved safety for utility staff and the community.

Success Measures: The main measure of success for this practice is that the utility found the practice sustainable for partial conversion to on-site generation before the heightened security concerns sparked by September 11, 2001, and found the changing security environment post-September 11,

2001, justified conversion to complete on-site generation.

Benefits and Incentives: The primary benefit of this practice is reduced risk to the community due to an accidental or purposeful release of gaseous chlorine.

11: Securing Utility Information



Corresponding Feature Description:

Security Sensitive Information Access Control

Category Type:

Infrastructure

General Description: This utility developed a set of practices for identifying security sensitive information, determining the value of the information (based on the consequences from improper use, disclosure or loss), and developed practices and procedures to mitigate those risks, as follows:

- Inventorying and controlling information to which employees need access (e.g., maps and records) by instituting employee access classifications, identifying procedures and facilities to protect restricted records, and assigning access based upon need and classification.
- Using of a security consultant to assist the utility in controlling access to critical data in electronic format.
- Restricting consultant/contractor access to data and preventing removal of data from a utility site.
- Changing the traditional process of security consultant selection within the utility to reduce distribution of sensitive information. This included choosing a security consultant based on qualifications rather than bid.
- Securing critical data from the public record by removing it from Web sites, and other public documents and records. Information provided to other government agencies may be subject to the Freedom of Information Act (FOIA) and state or local government requirements. However, FOIA, and many state and local ordinances, contain exemptions for sensitive and security related data.
- Re-keying critical facilities on a scheduled basis to make sure access is restricted to authorized personnel. Assignment of keys to employees is done based on need. All assigned keys are tracked.
- Securing vouchers and pay requests from contracts for physical security enhancements. When payment vouchers are routed through a primary government agency, purchase information becomes part of the public record, resulting in publicly accessible information about security enhancements. This knowledge can increase the risk of individuals or groups learning the nature, design, capabilities, and limitations of the utility security system. By allowing one category of vouchers to remain accessible only to the auditor, sensitive information regarding the nature of a utility's security system is protected. This approach to designating one type of voucher or pay request can be justified based on being diligent when protecting the safety and security of the utility, the utility's employees, and the public.

Resources Required: The resources needed to protect and secure information vary widely depending on how much of the work is done internally and how much is contracted out to consultants. Accurate accounting for this practice was unavailable.

Roles and Responsibilities: The utility designated an internal information security team, comprising members of all of the major departments. The team was responsible for identifying sensitive information and handling procedures, which include storage, handling when not in storage, and other considerations. Individual team members were responsible for identifying security sensitive information within their respective departments and

for assessing the level of security needed for each piece of information. In addition, utility and local government councils were consulted to determine the legal issues associated with protecting information.

Collaboration with Other Partners: This utility conducted their information security program internally, with the assistance of an outside security consultant. Utilities engaging in a similar practice may consider consulting other drinking water and wastewater utilities (and other utilities in general, such as electric or gas utilities), and local agencies to determine how they protect their information.

Barriers: This utility did not face any significant barriers. However, some utilities may face barriers getting their employees to take a new, security minded attitude towards protecting information.

Lessons Learned: Implementing a program to assess and protect sensitive information reduced the risk of malevolent acts. Additionally, it helped to educate staff about the types of information they handle on a daily basis and the importance of safeguarding that information.

Success Measures: One measure of success is that the utility can demonstrate they have fully catalogued, and appropriately protected, sensitive security information. In addition, periodic audits of the program determine if employees have embraced it and ultimately determine the program's success.

Benefits and Incentives: Instituting an effective information security program has many benefits. Protecting sensitive information related to physical security measures improves the effectiveness of those measures by making them harder to identify and defeat. Measures for securing electronic information include general improvements to the utility's information technology (IT) systems, which provide additional benefits in preventing electronic attacks on the utility (for instance, more secure firewalls for preventing access to sensitive data also helps prevent hacking of command and control systems). By identifying and eliminating information the utility does not truly need (or by implementing stronger security measures for protecting it), the utility increases customer confidence and decreases its legal liability in the event the data is stolen.

12: Enhanced Security of the Distribution System through Bulk Water Metering Stations

Corresponding Feature Description:

Intrusion Detection and Access Control; and Resiliency in Design and Construction

Category Type:

Infrastructure

General Description: To reduce the risk of contamination from backflow or siphoning into the water distribution system, this utility installed water metering stations for its bulk water purchasers, such as builders and landscapers. All commercial bulk water purchasers should use the stations and are prohibited from using fire hydrants for bulk water filling. Additionally, the utility began a rewards program for citizens who report unauthorized use of fire hydrants. The use of the metering stations allows the utility to better track the number of gallons used. It also simplifies the monitoring of hydrants because unofficial vehicles should never use them.

Resources Required: For this utility, a metering station cost approximately $25,000 to install, including appropriate backflow protection devices. Costs may vary depending on local conditions. No significant maintenance costs were incurred during the first 2 years of use. This utility also partnered with a neighboring utility, which decreased costs on design and construction.

Roles and Responsibilities: The system requires minimal staff training and only routine equipment maintenance and billing administration. The utility provides orientation sessions to bulk water purchasers on the use of the metering stations. Citizens within the district take an active role in the program by reporting unauthorized vehicles and persons accessing the metering stations, which helps prevent theft and possible contamination.

Collaboration with Other Partners:

Implementation and design of the system involved collaboration with bulk water purchasers, fire department, law enforcement, and water utility customers. The utility shared its design with a neighboring water utility, and both utilities installed the water metering stations concurrently.

Barriers: There was initial resistance from some of the bulk water purchasers who objected to the cost incurred for them to provide licensed vehicles and drivers to travel to the metering stations. This was resolved through a series of meetings with the utility manager who explained the importance of the stations to the security of the distribution system, and further explained that the utility incurred costs as well.

Lessons Learned: Some lessons learned during this activity include:

- A utility should site metering stations where access is visible to, and does not negatively impact, the existing community. This will increase the effectiveness of citizens as station monitors.
- A utility should also site the metering stations where access is easy, and make metering system instructions as clear and simple as possible. This will help decrease resistance from bulk purchasers.

Success Measures: This activity was highly successful for the utility in cost savings and community support. Some notable successes include:

- The utility estimated that prior to the water metering stations, only one in ten water loads was reported. Revenue from the accurate accounting of the metering stations paid for the

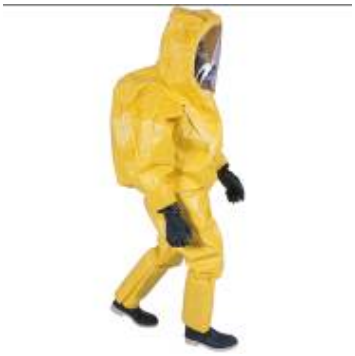
metering stations in 17 months and has provided a more accurate accounting of system efficiency and water loss figures.

- Customer complaints of low pressure and cloudy water have decreased now that hydrants are not used for bulk water filling.

Benefits and Incentives: This practice helps mitigate the risk of distribution system contamination identified in the vulnerability assessment. Although the implementation of the system was driven by a desire to decrease water contamination vulnerability, implementing water metering stations has provided other benefits, including:

- Backflow protection.
- Increased revenue through more accurate metering.
- Decreased maintenance costs from hydrant abuse and damage to water mains caused by sudden surges (water hammers) within the distribution system.
- Decreased customer water quality complaints.
- Increased security awareness and personal responsibility of citizens to care for their water system.

13: EPA Assistance for Water Contamination Incidents



Corresponding Feature Descriptions:

Contamination Detection; and Partnerships

Category Type:

Operational; Collaborative

General Description: EPA's Region 10 Emergency Response Unit (Response Team) has developed a water sampling and analysis practice, and uses On-Scene Coordinators to support the water sector in responding to emergency contamination incidents. The practice was developed after several contamination events overwhelmed the local utilities' response capabilities. EPA Region 10, which serves several Northwest states, including Seattle-King County, recognized the need for their role in this area and established this practice.

The Response Team members, including On-Scene Coordinators, were trained to assist water systems with emergency preparedness, response, and recovery. The Response Team developed specific procedures for water related incidents including utilizing the practices contained in EPA's Response Protocol Toolbox (RPTB).

The Response Team's capabilities include:

- Readiness to respond 24 hours-a-day to a contamination incident
- Response with technical resources required to address immediate dangers to the public and environment
- Community relations skills that can be called upon to assist with informing the public about a contamination event, response activities, and the contaminant involved

The four main practice areas where the Response Team provides emergency assistance are:

1. Collecting multiple samples from different sampling points.
2. Rapid analytical field testing, including deploying a portable gas chromatograph and mass spectrophotometer (GCMS).
3. Coordinating analytical data, including access to the EPA National Homeland Security Research Center and certified commercial environmental labs. In addition, the Response Team coordinates directly with state labs, other federal agencies such as the U.S. Department of Homeland Security (DHS) and Department of Defense (DoD), depending on the complexity of the situation.
4. Data management of samples, methods, and field and lab results.

Members of the Response Team undergo more than one month of training and education annually, including:

- Hazardous Worker Training
- Advanced Emergency Response
- Incident Command System (ICS)
- Specialized training for sampling and analysis equipment and instrumentation

Additional information on the Response Team is available at http://www.rrt10nwac.com/.

Resources Required: There is no monetary cost to the utility to access the Response Team. The Response Team staff and equipment are maintained by the federal budget to support this practice.

Roles and Responsibilities: On-Scene Coordinators lead the field sampling and response effort, and work as part of a Unified Command at an incident. EPA staff and their contractors are trained to respond as field support, part of the initial sampling team, and part of the analysis team. Administrative staff is provided by EPA to maintain accurate information on resources, contractors, and laboratories. The utility contributes to the response by

providing staff who can supply utility-specific input and advice to EPA and contractor staff.

Collaboration with Other Partners: This EPA practice supports public and private water sector agencies that request assistance from EPA. To support this effort, the Response Team uses the resources of other government and private agencies to provide a rapid and comprehensive response. The response capabilities include a variety of public and private labs, along with federal equipment and resources.

Barriers: To avoid encountering barriers during a response, the following recommendations are for all utilities and drinking water and wastewater agencies and organizations:

- Be familiar with the Response Team and its capabilities, as described above.
- Utilities should be able to activate their own resources and personnel on short notice to provide support for an incident.
- Understand that the Response Team's first priority is to protect human health and assist in stabilization of an incident.

Lessons Learned: EPA realized many lessons learned, including:

- Outreach to local utilities through in-person networking has been a key to the ongoing success of the program.
- Utilities need to know how to make a request for technical assistance if resources are needed.
- The Response Team's first concern is public health and the environment.

Capabilities: The EPA Region 10 Emergency Response Unit has been successful in enhancing the resources and expertise that can quickly be brought to bear on a contamination incident. Some of these capabilities include:

- Providing on-scene support in a water sector contamination incident
- Ability to provide and utilize rapid response field testing kits for water contaminants
- Ability to provide and utilize water contamination incident sampling kits
- Successful implementation of emergency response drills and exercises with water utilities

Benefits and Incentives: The EPA Response Team provides a number of benefits when activated to respond to an incident, including the following:

- Resources for federal support to a contamination response can be activated without a disaster declaration.
- Utilities gain access to experienced support staff that is well-trained in water sector emergency response and ICS.
- Response Team can be a part of the Unified Command or work under the operations section of the ICS.
- Response Team's access to specialized equipment and analytical resources provides rapid and efficient results for samples taken for testing.

Utilities that access the Response Team are accessing not only technical assistance, but also resources and coordination on preparedness, planning, response, and recovery activities. The Response Team will assist in incidents involving hazardous substances, biological agents, pollutants and contaminants, oil, and weapons of mass destruction in malevolent, natural, or accidental disasters or other incidents of national significance.

14: Emergency Preparedness Survey of Critical Customers

Corresponding Feature Description:

Partnerships

Category Type:

Operational; Collaborative

General Description: This utility developed a survey to collect information on critical customers' water needs in order to help prepare for an emergency that could result in a temporary or extended loss of service. Critical customers can include hospitals and other medical facilities, elderly populations, or other entities where water is a critical component to their operations, such as power generation and other industrial uses. Critical customers have special needs from water utilities, especially during emergencies. Periodically identifying and cataloguing the special needs for each critical customer provides for an understanding between the utility and the customer of what to expect if an emergency strikes.

The utility's annual survey is typically a two-page instrument with questions related to customer storage capacity, connectivity to the water system, and identification of the customer's disaster plan. Customers respond with information on specific procedures for water needs (including backup water supply), an assessment of the customer's level of independence (the length of time the customer can be self-sustaining), and emergency 24/7 contact information. These data are then provided to field crews responsible for routine and emergency shutoffs and outages, as well as emergency management staff responsible for event planning and response.

Resources Required: The level of effort for developing the survey, administering it, and cataloguing responses represent a small increase in the annual operations budget. Implementing the system, developing surveys, and maintaining the data required staff time; however, actual hours were not tracked.

Roles and Responsibilities: The utility Customer Service Key Account Representative (or equivalent) has responsibility to collect and maintain the data. The utility Field Operations and Control Center staffs maintain and review the data so they remain prepared for a loss of water in the portions of the system serving these customers. The lead for field response is the Water Quality Inspector, who assumes the role of Incident Commander and makes decisions on shutdowns, communications with critical customers, and providing temporary water. The utility should maintain access to each critical customer's data and conduct regular, preferably joint training on action plans to maintain water service or provide adequate water in the case of a loss of service.

Collaboration with Other Partners: Developing and maintaining critical customer data requires collaboration with local hospital associations, dialysis centers, nursing home associations, critical industries, and other service providers. Working with these groups enables improved communications and identification of additional critical customers, as well as identification of potential areas for improvement between the utility and customers.

Barriers: Many of the barriers encountered relate to securing participation from critical customers, and include:

- Difficulty obtaining responses from all or a high percentage of customers. Critical customers' staffs may already be stretched thin answering other surveys. It is important to impress upon them the importance of the information to the utility and how it impacts their operations.
- Challenges finding correct customer contacts within the surveyed entity (e.g., building

engineer) who has the needed information and/or authority to provide it.

- Hesitancy on the part of customers and utilities to make changes that incur costs if the survey indicates inadequate measures in place to deal with a loss of service to the customer.
- Difficulty maintaining a regular schedule for updating the information. This is extremely important because outdated information can mask the severity of a situation and worsen an emergency.

Lessons Learned: Lessons learned during this activity revealed gaps in the customers' ability to continue operating during a loss of service from the utility. Some of the lessons learned include:

- Critical customers need to ensure they have reliable backup supplies of water. Many customers mistakenly believed they did have supplies, but found through this effort they did not.
- Utilities need to conduct surveys and work directly with critical customers to clarify specific customer vulnerabilities that would otherwise not be known until an emergency happens.
- Once a vulnerability or inadequacy is identified, it is important to follow up with a contingency plan between the utility and the customer to address concerns.
- Data and procedures related to water security apply to a multitude of events linking critical customers with the utility, including routine utility operation and maintenance.
- After-action reports created following contamination events show that critical customers who cooperate with their utilities on their specific needs prior to an event are better prepared for a loss of service.

Success Measures: Success measures for building a comprehensive critical customer database include:

- Creating up-to-date information on critical customers, including having surveys available for collecting information
- Increasing the number of customer or sector-specific contingency plans and agreements (e.g., with hospitals and medical facilities, fire departments, manufacturing facilities)

Benefits and Incentives: Creating data on critical customers helps the utility meet their mission to provide safe and reliable water to their customers. The impact of a loss of service to a critical customer is likely to have greater consequences, and generate greater public attention, than a similar loss to the regular customer base. Avoiding a loss of services can help improve and maintain public confidence.

15: Funding Security Enhancements

Corresponding Features Description:

Emergency Response Plan (ERP) Tested and Updated; Security Resources and Implementation Priorities; and Intrusion Detection and Access Control

Category Type:

Operational

General Description: The U.S. Department of Homeland Security (DHS) makes grants available that are administered through state committees for security enhancements. In this case, the utility applied for funding for security upgrades via the county emergency planning committee. The utility procured the equipment upgrades up front and then applied for reimbursement. The upgrades included:

- Vault alarms installed around the wellheads
- A metering station for bulk water sales
- Chlorine residual and pH sensors to provide baseline contaminant protection

All requests for funding should contain detailed cost information. For example, a utility applying for fencing should include the type of fence and cost per foot of installed fence. However, the application for DHS funding does not need to be elaborate; this successful application was three pages long.

If a utility applies for grant funds prior to implementing the upgrades, the grant allows for a 10 percent cost variance from the estimate on the application. Any expenditure beyond that requires pre-approval.

The utility started the application process in September 2003 and received the grant approximately 18 months later.

Resources Required: In this case, total cost of the equipment installed was approximately $383,000. Consultant services for developing the cost estimate were $2,000. Approximately $75,000 covered outside labor costs for installing the equipment, and approximately $50,000 paid for additional equipment to complete installation.

The amount of time internal staff spent on preparing the grant was significant, but not closely tracked. A large part of this cost went to paying overtime to meet deadlines. These costs can be reduced through pre-planning, particularly if the utility has a dedicated grant-writer.

Roles and Responsibilities: The utility staff performed most of the work required within the framework of the assistance agreement. This included managing the contractors performing the upgrades, or performing the upgrades themselves. The utility used a consultant to perform a detailed costs analysis for DHS.

Collaboration with Other Partners: This activity did not involve collaboration with other partners beyond DHS. However, applying for grants in collaboration with, or with the support of, other local agencies (e.g., law enforcement and health) or utilities can help increase the chances of receiving a grant.

Barriers: The barriers encountered relate to difficulties negotiating the process of applying for the grant, and included:

- The committee in charge of funds had no formal system for allocating the money.
- Some utility staff changed during the grant process and new staff had to be brought up to speed on the security enhancement program and grant application process, slowing the process.
- Changes to the application required additional reviews by county, state, and sometimes federal government personnel.
- Each step of the grant process required written approval of the state committee.
- Communications between the county and state were cumbersome.

Lessons Learned: The upgrades implemented for this activity were identified as necessary in the

utility's vulnerability assessment (VA). Relating funding requests to a VA, or similar risk assessment, demonstrates an ongoing commitment by the utility to improve the safety and security of its system, and lends additional legitimacy to funding requests.

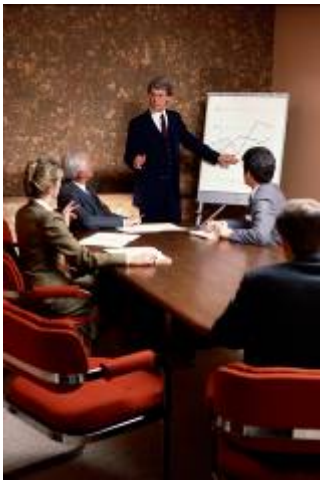
Success Measures: The new equipment and upgrades helped address gaps identified in the VA, allowing the utility to move on to other areas of concern. The utility's success with obtaining grant funds has encouraged them to consider applying for additional grant funds to implement more security-related improvements.

Benefits and Incentives:

The wellhead protection upgrades and metering station for bulk water sales has lessened the risk that contaminants can be introduced to the system by limiting unauthorized access. As noted in Practice Description #12, metering stations also help the utility more accurately monitor bulk water sales, increasing revenue.

The positive experience this utility had with obtaining grant funding has encouraged staff to complete a more comprehensive assessment of the water system beyond the VA, and look to grants for funding the assessment and any needed improvements.

16: Using a Clear Message for Risk Communications



Corresponding Feature Description:

Communications

Category Type:

Operational; Collaborative

General Description: To prepare for critical communications with the public during an emergency incident, this utility developed pre-scripted communications materials, or "message maps" to deliver key messages to the public about specific emergency scenarios. Message mapping is a science-based communications methodology that enables people who are required to communicate with the public to quickly and concisely deliver the most important information about an emergency. Scientific studies regarding the way in which people absorb information during high-stress situations have been reviewed extensively. Guidelines have been developed for the most effective means for delivering critical information to the public in such a way as to increase their retention of important information and to ease public fears and stress. Guidelines include recommended length of messages and the order in which information is provided.

Message mapping provides Public Information Officers (PIOs) and other public officials with key messages, graphics, maps, background information, a guidelines manual, and sample press releases (the message mapping "kit") that can be quickly modified to the specifics of the event. Message mapping has been successfully employed during major crises such as the September 11, 2001 attacks, the London underground bombings, and the Severe Acute Respiratory Syndrome (SARS) scare, as well as during many less publicized events. In this utility, message maps were developed for four emergency scenarios: the bypass of radiological contaminated wastewater from a combined sewer system; radiological contamination of a wastewater treatment plant; toxic and flammable material in a combined sewer; and chlorine gas release from a treatment plant.

Resources Required: The time it takes to develop message maps is dependent on the number of scenarios to be mapped and the number of people needing to be involved. In this case, an external consultant was employed to facilitate message mapping sessions and develop the initial message maps. Additionally, message maps should be reviewed and updated periodically and new staff should be familiarized not just with the maps, but with the concepts behind them.

Roles and Responsibilities: The utility PIO should understand the contents of the message mapping kit and coordinate with utility staff and other PIOs to update and maintain the kits. Utility staff is responsible for providing specific data on an emergency event to the PIO. Types of data may include the nature of the incident, extent of the affected area, anticipated length of any service disruptions, water use and health advisories, etc.

Collaboration with Other Partners: The message mapping kit was created in collaboration with personnel from the City of Seattle, U.S. Coast Guard, EPA Region 10, Washington State Department of Health, King County Public Health, King County Department of Natural Resources and Parks, and King County Office of Emergency Management. A key to the success of this practice is including all PIOs that would have involvement in the regional Joint Information Center. Another effective method is the practice of performing joint public briefings, with PIOs from different agencies addressing questions in their respective agencies' area of expertise. For instance, law enforcement PIOs may address questions regarding criminal aspects of an

event, while the utility PIO and health department PIO address questions regarding the safety of the water.

Barriers: The concepts and techniques of using message maps were new to the participants developing the manual, which created some resistance to the process. Additionally, maintaining the kits is time consuming and can be neglected.

Lessons Learned: Message mapping helps PIOs prepare for the expected and unexpected for communicating with the public. Following an emergency event, providing background information to PIOs can be time consuming and disruptive to the Incident Commander. Establishing a procedure before an event occurs that guides how and when a PIO should obtain information to plug into the message maps speeds and improves communications and reduces disruption. It is important that the PIOs of all responding agencies cooperate on developing the maps and related procedures prior to an event so the Incident Commander and his/her staff do not have to provide duplicate information to different PIOs.

Success Measures: Success is measured by the presence of having readily available messages and reducing public stress and anxiety. Evidence of success includes:

- Having readily available message maps that address a wide variety of crisis emergencies, as well as routine events that represent the input of multiple responding agencies
- Increasing PIO usage of message maps in emergency training exercises, and the resultant after-action reports that allow emergency planners to gauge the effectiveness of the practice at the particular utility and locality

Benefits and Incentives: This specific activity was initially developed for a radiological event, but participants learned that message maps are easily expanded to other types of events, including chemical releases. Additionally, a well developed message mapping kit should ease transition for new PIOs by organizing key utility messages (such as their mission statement) and presentation materials in advance, and familiarizing the PIO staff with the utility structure, assets, and systems.

17: Security and Emergency Response Metrics

Corresponding Feature Description:

Utility-Specific Measures

Category Type:

Operational

General Description: The term "security metrics" is the application of quantifiable or statistical analysis to measure security functions and workload. If implemented effectively, it allows the agency to track staff level of effort, costs, and productivity. This practice is an ongoing activity to identify and revise metrics and communicate appropriate levels of detail, frequency, and format of the data with the intent of measuring processes, program activity, and achievements.

A key objective for this practice is to identify those metrics by which real change can be measured. Metrics and data sources used in this practice include:

- The number of assets patrolled and events detected or reported (e.g., graffiti, break-ins, vandalism or unlocked doors, alarms)
- Type of background check for each category of critical personnel, different employees (vendors, contractors, etc.), and the percentage of those personnel who have received checks
- Employee training (skills assessment/inventory and completion of scheduled trainings)
- Time of response to incidents and resolution of events
- Incident reporting tools (incident report forms, after-action reports, closure reports, executive reports, and daily operational reports)
- Costs of security program (investments, resources, time spent)

Resources Required: After an initial investment of staff time to identify relevant metrics and reporting format, an estimated 15 percent of security staff time is spent annually on reporting and analyzing the data.

Roles and Responsibilities: The Director of Security and Emergency Management was the lead for identifying and reporting on metrics. However, staff from many different utility departments participated in collecting and submitting the data, and preparing reports.

Collaboration with Other Partners: Law enforcement, other utilities, and other agencies (i.e., state drinking water primacy agency, EPA, state and local emergency management agencies, etc.) may provide useful advice in identifying metrics. Additionally, the utility may share specific incident or observation data with these partners to ensure the practice's currency and relevance.

Barriers: Potential barriers that were identified during this practice were:

- Dedicating and maintaining sufficient staff time for identifying the metrics and subsequently implementing the data collection and analysis.
- Identifying a high-level utility staff person to oversee the process and push for necessary changes identified by the practice.

Additionally, this activity involved mainly risk-based measures that do not necessarily fit the traditional cost/benefit analysis process, and therefore may be difficult to communicate to decision makers.

Lessons Learned: The lessons learned that were identified relate to developing and implementing the activity, including:

- To ensure data is properly collected, management should ensure staff understands the reason for collecting the data.
- The utility should periodically review the metrics and the data associated with them. Over time, the utility will likely eliminate or alter existing metrics and develop new metrics as users become more familiar with the program data and quality improves.
- Measures can be borrowed from other sectors; however, terminology may not necessarily translate from one sector to another (particularly from private to public). One reference used by this utility was Security Metrics Management by Gerald L. Kovacich.
- Planning for collection of data requires sophistication and multiple systems to report out the data with an understanding of the form and frequency needs of each person (e.g., pagers, displays on computers for various key staff, automated paper reports). Users may not know what they want to see and will need education and experience to refine information.
- Metrics and measurable data can be used to build a business case for increasing and providing ongoing support of utility security programs.

Success Measures: Some of the success measures that can be used to gauge the effectiveness of this activity include:

- Data analysis outputs (like reports) are used in supporting the case for improving and maintaining the security program; their use was determined to be a factor in winning support.
- Expanding the group of data users can support increased procurement of important equipment (for instance, data used by the department in charge of distribution may procure more secure or tamperproof hydrants). The data may also be used by entities outside the utility such as public funding agencies to support security enhancements.

Benefits and Incentives: The output of this activity is a method for evaluating the effectiveness and efficiency of a utility's security program in different ways. This information can be used to improve specific protocols and procedures to improve security practices, to better allocate resources to where they are needed most, and to demonstrate and justify a utility's security needs to decision makers.

18: Radiological Contamination Event Procedure for a Combined Sewer System

Corresponding Feature Description:

Security Resources and Implementation Priorities; and Partnerships

Category Type:

Operational

General Description: This practice is based on a risk assessment of the effects of a "dirty bomb" explosion in an urban area serviced by a combined sewer system. The risk assessment was the first of its kind to address the dangers to wastewater workers, treatment plant and conveyance system, biological treatment processes, and the solid waste stream (e.g., biosolids, grit, screenings).

The tools and processes used in this practice included:

***Detection and Notification*:** There were no detection instruments deployed in the system itself. Emergency responders in the area notified emergency officials, who in turn notified the wastewater utility.

***Determining Extent of Contamination*:** To determine the presence and extent of contamination in the conveyance and treatment system, sampling points were identified upstream of the plant (including lift stations), in the influent barscreen room, at grit collection points, and at biosolids collection and transport points. Personnel used electronic personnel dosimeters, portable survey dosimeters, and other field laboratory instrumentation.

***A Radiological Emergency Response Plan*:** The plan included procedures for protecting the workers and the plant itself in the event of radiological material entering the waste stream. The plan also included a decision process flow diagram (also known as a decision tree) presenting the decision points and subsequent actions to take.

An Emergency Communications Guidance Manual: The manual included pre-scripted messages, also known as message maps, aimed at targeted audiences. The messages assisted the utility in answering common questions concerning the actions of the utility. This manual also included guidance on communication channels (for instance, using radio, television, print, and online resources), sample statements, and graphics to support the messaging.

Cleanup, Decontamination and Contaminated Waste Disposal Considerations: It is acknowledged that an event of this type will likely tax local, state, and federal response experts and resources, so a private consultant well-versed in radiological contamination and terrorism has been contracted to assist the utility in post-"dirty bomb" operations.

Training: Training is under development. The training will consider when and how to use the guidance as well as message mapping skills.

Resources Required: This activity required conducting a risk assessment and procurement of detection equipment. Additionally, training on detection equipment and response procedures should be conducted. This utility obtained a Homeland Security grant to help fund this activity. In this case the risk assessment was designed and performed in such a way that its findings could be used by other wastewater utilities with similar combined systems to conduct a risk assessment if the parties agree to sharing the information and safeguarding the contents.

Roles and Responsibilities: The overall lead for a radiological event is the municipal Emergency Operations Center (EOC). At the treatment plant, emergency actions were directed by the on-duty Operations Supervisor, who acted as the plant Incident Commander (IC).

Staff was trained on sampling protocols and detection equipment calibration and maintenance for use immediately following an event; response protocols for the protection of workers, the public, and infrastructure; and cleanup and decontamination procedures.

Collaboration with Other Partners: The utility collaborated with response agencies at the local, state,

and federal level as part of this activity, and established notification protocols with local and regional emergency response agencies based on which agency first discovers the contamination.

Barriers: Preparing for an event of this magnitude and impact can present many barriers; however, barriers can be greatly reduced through early and active cooperation between response partners. Some barriers include:

- Inconsistent and improvised public communication protocols have the potential for causing mass panic.
- Response personnel may be concerned for their personal safety while responding. Worker protection guidelines should be developed, communicated, and training conducted with personnel beforehand.
- State and federal regulatory considerations regarding the collection, transport, and disposal of radiological contaminated waste may complicate efforts to restore normal utility service.

Lessons Learned: Lessons learned from the assessment include:

- The radiological risk assessment revealed that the plant and its workers are at risk.
- The plant would immediately go from a permitted Publicly Owned Treatment Works (POTWs) under traditional regulations, to a low-level radiological facility, drastically changing requirements.
- The 140–170 tons of biosolids produced at the plant every day would go from being marketable fertilizer to low-level radiological waste.

In trying to address the consequences, the utility and its partners also determined the following:

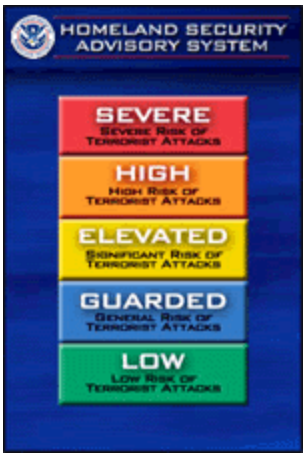
- Worker protection standards at the state and federal level would have to be changed to allow for the continued operation of the plant.
- The wastewater utility would largely be on its own during the first days of a radiological event.
- The utility and its partners identified the types of radiological monitoring equipment necessary to protect the workers and determine that the equipment should be stockpiled before an event to increase utility readiness and decrease response times.

Success Measures: Success measures for this activity come from after-action reports following exercises and trainings. Additionally, the creation of the emergency response plan, the message maps and risk communication guidance, and regulation-compliant cleanup and disposal plans will be indicative of success.

Benefits and Incentives: This activity provides many benefits to the utility. For example:

- Risk assessments conducted as a precursor to this activity may reveal other, more probable, sources of potential radiological contamination than a dirty bomb scenario.
- The concepts and principles for developing message maps to a radiological event can be applied to developing message maps for other scenarios.
- The partners the utility engages for this practice will likely be partners for other types of responses; therefore this activity will set the stage for future cooperation on other, more probable scenarios.

19: Utility Response to Changing Threat Levels



Corresponding Feature Description:

Threat-level Based Protocols

Category Type:

Operational

General Description: Utilities cannot operate efficiently in a constant state of high level alert; therefore, this utility developed a dynamic system of changing operational conditions, or alert levels, to correspond to the current level of threat to the utility. Threat levels can change due to national alerts, local events, or intelligence provided through a variety of resources. The practice that the utility developed uses a communication network with the water sector, and other agencies in the region, to share ongoing threat intelligence. This sharing of intelligence allows for quick adaptation to changes in threat levels by increasing surveillance at critical assets.

This practice mandates that management monitor the threat level at the national, state, and local level to determine the appropriate alert level for the utility and decide whether an elevation or relaxation is necessary. Daily threat level monitoring and a credible communications network with local emergency managers, police, and federal agencies, helps assure that this information sharing process is timely and seamless.

At times of elevated alert, operations staff increase site visits to critical facilities, and conduct more intensive inspections at each facility. On-call employees are also required to expand their weekend surveillance of utility facilities in response to increased alert levels.

Resources Required: This practice requires an initial investment of staff time, mainly at the managerial level, to establish the communications network with regional partners, and to develop the protocols associated with different threat levels. The level of ongoing staff commitment will depend on the specific alert protocols and the frequency of alert level changes. For this utility, the practice did not cut into productive work hours or increase costs.

Role and Responsibilities: Threats are monitored by utility managers through daily reports and email from Homeland Security Information Network (HSIN) and Water Information Sharing and Analysis Center (WaterISAC) at a national level. These same networks are also used to provide information on local incidents. The utility's general manager is the contact for all communications between each network and the utility staff responsible to respond and prepare for changes in threats.

Collaboration with other Partners: This practice involves collaboration with sector partners through the HSIN and WaterISAC. Additional partners for threat information sharing can include local Terrorism Early Warning Groups (TEWG) (which usually include local law enforcement), and EPA Criminal Investigation Division (CID) and regional offices. Local partners can also contribute locally; for instance, local law enforcement may agree to assist in more frequent patrols.

Barriers: There were no specific barriers identified for this practice; however, one barrier may include a utility not having electronic access to security information networks such as HSIN and WaterISAC. Water sector information sharing networks, such as HSIN and WaterISAC, are readily available to the water sector. Alert level protocols should not fundamentally involve new practices, and typically focus on more frequent and thorough patrols and inspections. Training on new protocols should be easily folded into existing security training programs.

Lessons Learned: The main lesson learned during this practice is that implementing a system of threat-based security protocols is a low-cost and effective

way to improve utility security, which can be applied to utilities of all types and sizes.

Success Measures: The success of this practice can be measured by the establishment of threat-based protocols for increasing utility security (particularly if law enforcement, security, and/or utility experts review and agree with the protocols), as well as by maintaining daily interaction with the different threat intelligence networks and law enforcement.

Benefits and Incentives: This practice is part of a broad strategy applied in many practices; establishing and maintaining a network of people in the region who have invested in building relationships with each other to prepare for and respond to emergencies. Many of the contacts and communications networks employed in this practice, particularly at the local level, will be applicable to other emergency situations.

20: Procedure for Contractor and Vendor Access

Corresponding Feature Description:

Access Control

Category Type:

Operational; Infrastructure

General Description: This utility's vulnerability assessment recognized that vendors and contractors have both knowledge of, and access to, critical utility assets. In response, the utility developed protocols and procedures for contractor and vendor access to sensitive utility information and facilities. This represents a major change in the historical practices used in the water sector. Utilities often have had a long-standing relationship with their vendors and contractors and have relied on them to safeguard the most important assets with little oversight.

The process began with the identification of each vendor and contractor and their need for specific knowledge of, and access to, critical assets. If access was justified, procedures were developed to restrict or provide oversight for each access event. The following are examples of this utility's procedures:

Contractor companies verify personnel employment and assignment to the utility. When work is to be performed, each contractor staff person registers on site as they enter facilities and when they leave, and are escorted to sites by utility employees. Identification badges are issued to contractors while they work at utility facilities. Contractor equipment or materials cannot be left on site without approval of the utility.

Vendors are usually chemical supply companies but can include other types of vendors. Chemical delivery agents are prescreened for entry to the facility by having their driver's license verification issued by facsimile from the chemical supply company. Chemicals are then tested on site with portable test equipment. Drivers are accompanied on site and utility employees observe the unloading to the utility storage areas. Finally, field water-quality monitors are observed for unusual changes that may relate to the delivery and use of new chemicals. In some cases, chemicals are picked up by employees directly from the supply company. For other vendors, drop-off points are provided outside critical areas.

Cell phone company installations are located on this utility's property. Cell phone company personnel who maintain these sites should be accompanied by utility staff. Utilities are compensated for the use of facilities, such as water storage tanks, and terms are agreed to in the contract for the lease of the utility property.

Utility services, specifically the electric power utility staff, no longer enter utility sites to read meters. Instead, the electric utility uses remote meter-reading technology.

Resources Required: This practice does not require any resources beyond staff time to review and revise contractor and vendor access protocols.

Roles and Responsibilities: The specific roles and responsibilities for this practice may differ by utility, depending on their existing internal processes for contracting and procuring supplies and services. The utility security officer should lead the effort to revise access protocols, and should coordinate with different departmental managers to ensure that the revised protocols are not overly burdensome. Utility departmental managers are responsible for identifying vendor and contractor functions that require access to sensitive sites, for providing recommendations to the security officers, for instructing their personnel on the new access protocols, and for relaying the new protocols to vendor and contractor staff.

Collaboration with Other Partners: This practice does involve collaboration with affected contractors, vendors, and other entities.

Barriers: This utility did not encounter any barriers in implementing this practice. However, staff and contractor/vendor acceptance of, and adherence to, a change in the status quo could prove difficult for other utilities.

Lessons Learned: The primary lesson learned was to have active outreach to vendors and contractors to ensure compliance with defined protocols and procedures.

Success Measures: The success of this practice can be measured by the existence of defined processes and protocols. Another success measure is mitigating or reducing risks identified in the vulnerability assessment.

Benefits and Incentives: The main benefit to this practice is that it is a low cost, low effort way to improve security, in both implementation and maintenance. Developing new protocols means better controls of who has access to the utility. Another benefit is the opportunity to gather feedback through surveys and other means from both their own staff and contractor and vendor staff on the new procedures. Additionally, utility security records concerning unauthorized access by non-utility staff may also be a data source for determining whether the program is being accepted by the staff responsible for implementing it.

21: Updating a Vulnerability Assessment

Corresponding Feature Description:

Vulnerability Assessment Up to Date

Category Type:

Operational

General Description: This utility established a vulnerability assessment (VA) cycle for each function of their operation, including drinking water and wastewater. The initial VA was completed before the deadline set by the Bioterrorism Act of 2002 for water utilities, and was performed with the Risk Assessment Methodology for Water (RAM-W™) and the Risk Assessment Methodology for Dams (RAM-D^{SM}). The utility has planned for the VA update by establishing a VA committee composed of eight members, which meets monthly.

Timing for an update of the utility's VA is driven by the cycle for implementation of improvements. This utility defined that cycle to be every 5 years, and it is composed of the following:

- Conduct the VA, which takes approximately three months and covers about 150 assets.
- Develop security improvement proposals based on the results of the VA.
- Present proposals to elected officials to secure funding.
- Implement the improvements in a phased approach.
- Review progress and initiate the cycle again.

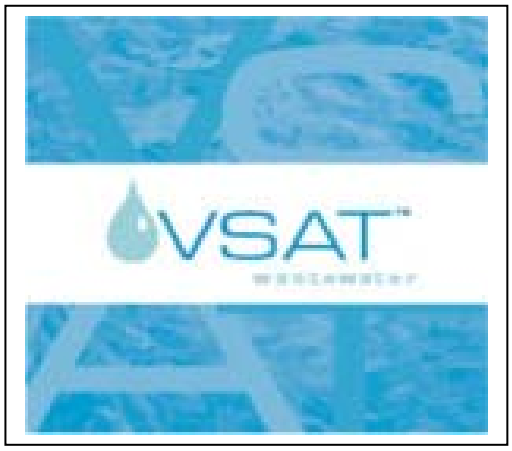
Resources Required: Updating the VA cost the utility approximately $85,000, which does not account for costs associated with staff time for maintaining a VA committee to review and discuss findings. Developing proposals for utility improvements and implementing them are already accounted for in the utility's budget and staff responsibilities.

Roles and Responsibilities: Utility operations and security staff compile hazard trend information for review by the VA committee. The VA committee comprises seven members representing critical assets (including Information Technology [IT] and Supervisory Control and Data Acquisition [SCADA] system components), and the eighth is a security specialist. In addition to the responsibilities of hazard trend review, the committee also advises on budget expenditures and presents budget proposals for security improvements to elected officials. They also oversee improvement implementation and progress.

Collaboration with Other Partners: This practice did not involve collaboration with other partners outside the utility.

Barriers: The main barrier encountered for this practice was dedicating staff time to gather the data necessary to perform the VA update, in addition to their regular duties.

Lesson Learned: The utility learned two main lessons through updating its VA. First, the utility has switched to the Vulnerability Self Assessment Tool (VSAT™) to replace the RAM method for the update. Utility staff found that VSAT's ease of use (specifically the data displays with color codes) makes for simple revisions for future VA updates, and only one primary data collector needed VSAT training. VSAT also allows for documentation of specific risk reduction measures and also measures how much they helped reduce risk. Second, the committee found that Design Basis Threat (DBT) conditions documented during the first VA had not changed; therefore, the rigorous assessment of all assets done for the initial VA was not necessary for the update.



Success Measures: The success of this practice can be measured every cycle by comparing previous

VAs and noting the reduction and/or elimination of vulnerabilities. Additional measures include funding secured for improvements based on the recommendations of the VA, and implementation of those improvements.

Benefits and Incentives: The results of the updated VA provide documented security needs for the utility, which can serve as a basis for the utility's funding requests to budgeting officials, and for changes in utility security protocols and programs.

22: Creating and Maintaining a Security Culture

Corresponding Feature Description:

Explicit Commitment to Security; Promote Security Awareness; and Defined Security Roles and Employee Expectations

Category Type:

Organizational

General Description: This utility adopted a plan to foster a security culture using a variety of methods to increase awareness of security and preparedness among its employees. The process began with the formation of an executive committee representing all branches of the utility. The committee defined a single plan and message to create the security culture. This message provided a framework for the other components of the plan, which were:

- Linking safety and security by incorporating a security message into every safety training session
- Developing a security and emergency management Web site that provides employee access to security information, policies, and procedures
- Providing preparedness training for all employees
- Monthly newsletter articles

Resources Required: This practice potentially requires significant staff time, particularly in the development stages. Additionally, resources such as a Web site, newsletter, and poster publishing, need to be developed to spread the messages created by the committee throughout the utility.

Roles and Responsibilities: Creating a security culture requires the cooperation and participation of staff from all levels of the utility, but should start at the highest levels. In particular, the Security and Emergency Management Director and staff are responsible for developing a plan to implement the culture within the utility. Senior management and supervisors are responsible for presenting a consistent message to the employees that security is important, and to reinforce that message by example. All levels of staff are responsible for participating in training and events pertaining to security, and utilizing this knowledge during daily operations.

Staff providing employee training should maintain knowledge of current threats to the utility as well as current security practices as this information is provided to policy and decision makers during discussions that shape the security culture training program.

Collaboration with Other Partners: The utility worked closely with other departments, including human resources, citizen groups, and the Mayor's office to develop and present a cohesive message. The utility also sought to improve communication and interaction at all levels with responders like police, fire, public health, and labs to further reinforce the security culture.

Barriers: When creating a security culture, the utility encountered employees who were resistant to the idea that the utility would ever be subject to any sort of illegal activity or disaster, which hindered efforts to implement this practice. Additionally, the deployment of monitoring equipment, such as cameras, caused privacy concerns for both employees and the general public.

Lessons Learned: This utility learned a number of lessons that may help others better implement a security culture at their utilities. First, the utility found that creating a team early on to implement the program helped to maintain a consistent message.

However, adoption and acceptance of the security culture by employees takes persistent effort. To ease this, communication to employees should occur often and in a variety of settings and forms. Also, in some instances, messages should be tailored to specific audiences inside and outside the utility. Because of increased awareness and reporting of security incidents, additional security staff was added.

Success Measures: In this case, after implementing the program the utility noted an increase in the reporting of security incidents each year. The increase in reported incidents demonstrates that staff are more aware of and reacting to possible problems that would otherwise result in more severe measures needed such as public notifications.

Benefits and Incentives: Fostering a security culture has shown external as well as internal benefits to the utility. Utility security concerns have increased credibility in the eyes of law enforcement and the local Federal Bureau of Investigation office. This has improved the utility's ability to win funding for further security and preparedness upgrades by acquiring external partners who will support the utility's security concerns to decision makers. This in turn results in staff that are well trained in disaster response and recovery, which can be applied to many more common events, such as weather related disasters or civil unrest, that threaten utility assets.

23: Training on Security and Emergency Response

Corresponding Feature Description:

Promote Security Awareness; and Defined Security Roles and Employee Expectations

Category Type:

Organizational; Operational

General Description: This utility developed a National Incident Management System (NIMS)-compliant Emergency Response Plan (ERP). The utility then created an internal training program based on its ERP.

The training program is exercised at all staff levels to improve the utility's capability to respond to all-hazard events. It consists of an annual tabletop exercise based on a different emergency scenario each year. The utility has also conducted a full-scale exercise that involved an earthquake scenario. As part of the exercise, the staff trained on performing visual inspections of sites and reporting the assessments to the Emergency Operations Center (EOC).

Additionally, the utility maintains a library that has copies of the ERP that can be easily accessed during an emergency, or if staff feel the need to review the plan between exercises and training. Another copy of the ERP is kept at a remote site in case the library is destroyed or inaccessible. Also, the utility has placed placards in key locations where response resources are located.

Resources Required: This practice requires an initial investment of staff time to revise the ERP for NIMS compliance, to conduct staff training on NIMS concepts and processes, and then to train staff on the new ERP. However, after this initial investment, this practice should not represent a significant increase in the normal emergency response training budget of the utility. Additionally, there are many local, state, and federal grants available for emergency preparedness and training, particularly to bring response entities into NIMS compliance.

Roles and Responsibilities: The utility formed a Safety and Emergency Management Committee that meets once a month. Departmental staff members are periodically rotated through the team to provide the utility with a broad emergency response knowledge base. The district engineer and a few other key personnel are the only permanent members of the team. This committee advises management regarding how to use the training funds and other available resources. The group also decides who will be sent to external training events, like regional exercises.

The average staff member participates in approximately 16 hours of training each year, as well as biweekly safety and security meetings. Senior staff and members of the Safety and Emergency Management Committee have additional training requirements.

Collaboration with Other Partners: In this case, the utility collaborated with the state Office of Domestic Preparedness Programs, state Department of Health, the County government, and an outside consultant to develop its training program. However, NIMS trainings and exercises can be designed to incorporate a wide range of partners, ranging from the local to federal level.

Barriers: In revising its ERP and NIMS structure, this utility encountered difficulty in defining the roles and responsibilities of certain staff if an emergency occurs after normal business hours.

Lessons Learned: The utility was not awarded preparedness grant money in 2006. This underscored the need for dedicating regular annual funds for security and preparedness, so that the utility is not caught short if supplemental funding sources do not come through.

Success Measures: Success is measured by the existence of an ERP that has been reviewed and accepted by the local, county, or state NIMS compliance officer. In addition, having personnel that have received the appropriate NIMS training is a requirement for receiving Homeland Security grant funding, and many states and tribes have more stringent requirements. The current federal NIMS training requirements can be found at http://www.fema.gov/emergency/nims/nims_training.shtm.

Additional success can be measured by reviewing the results of training after-action reports. In this case, successive trainings and exercises have shown staff and management are better prepared and more capable to respond to an emergency than prior to the implementation of the practice. This was demonstrated by improved communications across groups both internal and external to the utility and in awareness of interdependencies among different agencies when various scenarios were applied.

Benefits and Incentives: NIMS compliance is a requirement for receiving federal preparedness funding, and individual states and tribes have more stringent requirements. This practice is a necessary step towards opening future supplemental funding pathways for utilities. Additionally, NIMS is a proven emergency response framework; federal program administrators have developed specific NIMS trainings targeted at public works departments. Finally, the response partners with which a utility will team during a response will likely be well versed in NIMS; being NIMS compliant is therefore necessary to ensure that the utility is capable of a coordinated, effective response effort.

SECTION 6: EXAMPLE OF SECURITY AT A SMALL UTILITY

Even small utilities can use the practices described in this report to develop an active and effective protective program. The description below shows how one small utility in the Seattle-King County area implemented such a program. The program provides them with benefits through collaboration with other utilities and agencies, reduces costs for the utility and its customers, improves its infrastructure, and enhances its protective posture. For security reasons, the utility is not identified.

Utility Background

The utility profiled here is a small combined drinking water and wastewater system serving approximately 10,000. Before the attacks of September 11, 2001, the utility made security and preparedness a high priority. After September 11, 2001, the utility increased its efforts in response to federal mandates and management's awareness that more could be done—especially to address terror-related threats. Historically, the focus was on natural disasters and vandalism.

Operational Practices

The utility added or changed several practices to increase security and preparedness of its facilities and its control and communication systems. One step it took after September 11, 2001, was increasing system component inspection from once weekly to twice weekly.

Remote access to computer and SCADA systems is proven to be valuable to operations, yet the potential for hacking is a credible threat. The utility addressed the risk by switching connections to "dial-up," which provides protection by having the ability to monitor who is connecting to the system. In addition, any user will be locked out after three failed attempts to connect. This feature diminishes the likelihood that code-breaking programs can access the system.

The utility took simple effective steps to protect communications equipment. The utility keeps a variety of equipment available such as non-electronic phones capable of maintaining dial tone during power outages, 800 MHz radios, two-way walkie-talkies in vehicles for general maintenance work, and access to a ham radio. The utility also has access to daily threat information through Northwest Warning, Alert, and Response Network (NW-WARN). The utility also communicates security information to customers through a newsletter that advises them to dial 911 if they see suspicious activity, such as persons attempting to connect to a fire hydrant.

The utility secured public access to information by removing pump station location information from its Web site. The utility also requires those who request information to identify themselves and the purpose of their information request. Both drinking water and wastewater systems are secured at the same level because the utility included the entire system in its security and preparedness program.

Organizational Practices

Before September 11, 2001, the utility had policies and procedures in place to prevent and mitigate acts of vandalism. Each of the utility's staff also had his/her own written emergency response procedures for disasters. The staff used these emergency procedures during an earthquake in 1989, when a quick visual assessment of the entire system was necessary. The staff's familiarity with procedures enabled them to confidently assess the system and report information back to administrators. Because of the procedures, staff was able to complete the assessment within 40 minutes.

Utility managers provide staff with security and emergency training to foster a culture of safety and security. Staff members are trained continuously with basic protective practices during weekly staff meetings and participate in regional emergency exercises.

Continued on next page

Infrastructure Practices

The utility implemented several practices to better protect its infrastructure. First, the utility installed water metering stations at secure points in the distribution system for contractors to safely withdraw bulk water for their trucks. This protects against contamination and eliminates wear and tear on hydrants, which used to occur when contractors hooked their hoses directly to a hydrant. Now the hydrants have a non-standard lock to prevent unauthorized hook-ups. Second, after an incident in which a hatch was left ajar and the utility incurred a $3,000 charge to isolate a tank and sample water, staff modified the hatch so it cannot be left open or ajar; now it can only be totally removed. Third, all entrances and exits at the utility's headquarters have been secured using a combination of locks, alarms, and cameras. The details of the protective components at the remote sites are kept secret from all outside entities.

Collaborative Practices

Historically, utility personnel were not considered first responders. Homeland Security Presidential Directive 8 (HSPD-8) redefined public works department staff, including those within the water sector, as first responders. Utility managers encouraged staff to participate on regional security and emergency management committees in response to the shifting culture.

The utility manager provided local police with a list of critical sites and contact information of system operators and managers to help familiarize local responders with the utility system. A much stronger local network has emerged in which utility operators are fully integrated into the local emergency response community. In addition, a better understanding exists among local emergency responders about one another's needs, and utility vulnerabilities.

The utility worked to expand relations with other drinking water and wastewater utilities in the county. According to the utility manager, although there was a mutual aid response program for water and sewer districts for many years, after September 11, 2001, agencies and municipalities began to work even more closely together through the county's regional disaster planning group.

Conclusion

The practices at this utility demonstrate that even a small utility can make meaningful gains in security and preparedness. Part of this utility's success is due to its commitment towards making security and preparedness a high priority. As a result, it has been able to make significant progress despite a limited budget. Implementing security and preparedness priorities through the use of in-house staff, rather than hired consultants, is one way that it keeps costs low. This is critical, because the utility found obtaining federal, state or county funding is difficult.

While the utility is unable to define cost savings resulting from its safety and protective programs, management is confident that in the event of an emergency, they "will be able to respond quickly so that [their] customers are protected." Moreover, the utility's security and preparedness programs help to educate utility staff and the community about the importance of security and preparedness issues. "This opened people's eyes to some of the potential problems that can arise," said the utility's general manager. "It has been a good education."

APPENDIX A: CASE STUDY GUIDANCE TEAM MEMBERS

Person	Affiliation
Allen Alston	King County Wastewater Treatment Division
Ben Budka	King County Wastewater Treatment Division
Gene Taylor	Water Security Lead: U.S. EPA Region 10
Mike Boykin	On-Scene Coordinator: U.S. EPA Region 10
Shad Burcham	King County Office of Emergency Management; King County Critical Infrastructure Protection Group
Scott Decker	Washington State Department of Health
Robin Friedman	Seattle Public Utilities Director for Security and Emergency Management
Brandon Hardenbrook	Pacific Northwest Economic Region (PNWER)
Jim Henriksen	Seattle-King County Department of Public Health
Randy Holmes	City of Bellevue Utilities
Mike Jackman	City of Bellevue Utilities
Mitzi Johanknecht	King County Sheriff's Office
Bob Lomax	Seattle Fire Department
Fred Savaglio	Region 6 Hospital Emergency Preparation Committee
Hal Schlomann	Washington State Association of Sewer and Water Districts; King County Critical Infrastructure Protection Group
Ron Speer	Soos Creek Water and Sewer District
Ted Stencilin	King County Sheriff's Office

APPENDIX B: ADDITIONAL PRACTICES

The Area Workshop and individual discussions provided opportunities to gather information on practices that are in use or are needed by the Seattle-King County community. Although the Case Study effort could not document all of these practices in detail, the following additional practices were captured for future consideration.

Organizational Practices

Conduct management training and briefings about the water sector and interdependent services.

Conduct training and tabletop exercises for water sector management and staff on security, emergency preparedness, and response.

Provide technical assistance and capacity development for small systems on planning, response and recovery, and Rural Community Assistance Partnership (RCAP).

Conduct regular tabletop exercises to practice response plans and facilitate collaboration and networking between water sector utilities.

Dedicate funding resources for security and preparedness activities.

Identify specific staff with security and preparedness as a primary job function.

Train staff on Incident Command System (ICS) and Emergency Operations Center (EOC) functions.

Participate in EOC training and planning.

Identify and document who has primacy over utilities in each jurisdiction (e.g., local health department, state health department, Department of Environmental Quality [DEQ], Department of Environmental Protection [DEP], and U.S. Department of Energy [DOE]).

Develop response and recovery plans with the idea that all response activities begin at the local level.

Use water sector needs assessments conducted by local and state agencies to develop response and recovery plans.

Learn to use home rule/jurisdictional agreements (e.g., Memoranda of Understanding [MOUs] to facilitate mutual aid, collaboration, and resource sharing).

Conduct cross-training with Hazardous Materials (HAZMAT) units.

Operational Practices

Establish an ability to connect with Supervisory Control and Data Acquisition (SCADA) and other Information Technology (IT) systems remotely.

Ensure a method for continued communications of customer service/communications during an emergency event.

Conduct cyber security and preparedness training.

Provide technical assistance and capacity development for small systems.

Establish cross-sector liaisons within interdependent agencies (e.g., electric customer service representative dedicated to water sector).

Update local and regional Emergency Medical Services (EMS) contact information.

Identify organizations and residences exempt from service shutoff for all utilities and share information between sectors.

Update emergency response plans regularly.

Identify and prioritize equipment needs that facilitate continuity of service.

Plan and develop system redundancies for continuity of service (e.g., personnel, equipment, and fuel).

Use established tools, such as the EPA Response Protocol Toolbox to validate potential contamination events.

Ensure occupational safety and security is integrated.

Establish the ability to track field staff.

Identify essential personnel and cross-train staff to ensure coverage during an emergency; put emergency roles and expectations into job descriptions.

Create a response plan for radiological contamination events.

Work collaboratively to create specific agreements with hospitals (who are large drinking water and wastewater users).

Conduct IT/data systems cross-training within the water sector and with other sectors, to support continuity of business and service outside the disaster area.

Develop water sector response and recovery teams.

Develop lists of laboratories (e.g., public health, environmental, or both), and create agreements on capabilities during an emergency.

Provide continuing education opportunities on security and emergency response.

Establish rules for disclosing information to the public.

Develop a manual of operations that addresses cross-sector issues.

Prioritize restoration of service for water sector utilities and other critical infrastructures.

Establish emergency permitting protocols and a tiered permit approval process to respond to increasing levels of urgency.

Conduct assessment of information needs and develop communication plans.

Train field personnel within all sectors to recognize and report issues of concern.

Train operator and field staff on contaminant detection and other security surveillance.

Establish protocols for distributing emergency drinking water.

Routinely re-key assets so that people with old keys cannot open locks.

Use a testing procedure to verify chemical delivery truck contents.

Infrastructure Practices

Develop an ability to isolate portions of the system in a contamination event (e.g., diversion valves).

Develop intra-/inter-agency communications systems (e.g., radios, phones).

Create off-site data centers.

Develop maps and overlay water, electric, and transportation pipes and conduits.

Catalog equipment within mutual aid areas, including with other critical infrastructures.

Develop plans for accessing resources such as fuel, energy, staging, etc.

Install water hydrant access control.

Install raw water intake protection.

Designate wells as emergency water supply.

Develop multiple source water intake locations.

Secure wellheads for protection.

Install intrusion alarms on assets such as reservoir hatches and remote site doors.

Collaborative Practices

Conduct joint emergency response planning among neighboring water sector utilities.

Conduct joint emergency response planning among critical infrastructures (e.g., energy, dams, and hospitals).

Create cross-sector advisory committees.

Use Northwest Warning, Alert, Response Network (NW-WARN) for information sharing.

Conduct regular meetings in water sector and across sectors to facilitate networking and relationship building.

Conduct outreach and education with public officials.

Submit multi-sector and cross-jurisdictional applications for U.S. Department of Homeland Security (DHS) grants and other funding.

Conduct water sector-specific and cross-sector tabletop exercises.

Establish contact with other sectors for collaboration and networking (e.g., invite to tabletop exercises).

Advocate for water sector inclusion as a first responder in activities.

Identify interdependencies and impacts between water sector and other critical infrastructures.

Conduct and participate in multi-sector conferences, trainings, and workshops.

Develop and coordinate Public Information Officer (PIO) functions, especially for organizations without PIO capacity.

Identify audiences and target messages for communication (e.g., who do we need to reach, what do they want to know, when do they need to know it, what is the best way to communicate each message to each targeted audience).

Share surveillance data, customer calls, and water quality data with public health departments.

Share information through established security channels (e.g., Water Information Sharing and Analysis Center [WaterISAC]).

Learn surveillance methods and capacities of state and local health departments, and integrate syndromic surveillance when possible.

Engage the public on security and preparedness issues.

Establish better relations between the local EOC and water sector utilities.

Establish a policy that allows water sector utility leaders to use the county EOC if their own EOC is not available.

Improve collaboration between public organizations and private entities.

Establish protocols for communication channels between local, state, and federal agencies.

Establish multi-sector planning for prioritizing equipment sharing and restoration of service.

Create and implement a risk communication strategy for the water sector.

Develop cross-sector information sharing through Homeland Security Information Network (HSIN).

APPENDIX C: KEY FEATURES OF AN ACTIVE AND EFFECTIVE PROTECTIVE PROGRAM

The water sector has developed the Features of an Active and Effective Protective Program to assist owners and operators of drinking water and wastewater utilities (water sector) in preventing, detecting, responding to, and recovering from all-hazards, including terrorist attacks or natural disasters. The features are based on the National Drinking Water Advisory Council's recommendation: *14 Features of an Active and Effective Security Program*. The features contained in this version update the original 14 to:

- Capture the water sector's post Hurricane Katrina emphasis on "all hazards" preparedness; and
- Establish explicit alignment with the Water Sector-Specific Plan for Critical Infrastructure Protection (Water Sector SSP) prepared under the framework of the National Infrastructure Protection Plan (NIPP).

The features describe the basic elements for establishing a "protective program" for owners/operators of utilities to consider as they develop utility-specific approaches.

Note: Throughout this document, the terms "protective program," "protection," or "protective" are used to describe activities that enhance resiliency and promote continuity of service regardless of the hazard a utility might experience. These activities address the physical, cyber, and human elements of prevention, detection, response, and recovery.

Features of an Active and Effective Protective Program

1. **Encourage awareness and integration of a comprehensive protective posture into daily business operations to foster a protective culture throughout the organization and ensure continuity of utility services. (Most strongly aligned with SSP Goal 1, Objective 1.)**
   - Senior leadership makes an explicit, easily communicated commitment to a program that incorporates the full spectrum of protection activities.
   - Incorporate protection concepts into organizational culture.
   - Foster attentiveness to protection among front line workers and encourage them to bring potential issues and concerns to the attention of others; establish a process for employees to make suggestions for protection improvements.
   - Identify employees responsible for implementation of protection priorities and establish expectations in job descriptions and annual performance reviews.
   - Designate a single manager (even if it is not a full time duty) responsible for protective programs. Establish this responsibility at a level to ensure protection is given management attention and made a priority for line supervisors and staff.
   - Keep current on improvements and good protective practices adopted by other utilities.
   - Monitor incidents and available threat-level information; escalate procedures in response to relevant threats and incidents.

2. **Annually identify protective program priorities and resources needed; support priorities with utility-specific measures and self-assess using these measures to understand and document program progress. (Most strongly aligned with Goal 1, Objective 1.)**

   - Annually identify and dedicate resources to protective programs in capital, operations, and maintenance budgets; and/or staff resource plans.
   - Tailor protective approaches and tactics to utility-specific circumstances and operating conditions; balance resource allocations and other organizational priorities.
   - Annually review protection commitments and improvement priorities with top executives.
   - Develop measures appropriate to utility-specific circumstances and operating conditions.
   - Self-assess against the measures developed to understand and document program progress.

3. **Employ protocols for detection of contamination while recognizing limitations in current contaminant detection, monitoring, and public health surveillance methods. (Most strongly aligned with Goal 1, Objectives 2 and 3.)**

   - Recognize that water quality monitoring, consumer complaint surveillance, sampling and analysis, enhanced security monitoring, and public health syndromic surveillance are different, but related, elements of an overall contamination warning system. The effectiveness of these components may vary from system to system.
   - Establish sampling and testing protocols for events (and suspected events) and understand availability of, and be prepared to access, specialized laboratory capabilities that can handle both typical and atypical contaminants.
   - Track, characterize, and consider customer complaints to identify potential contamination events.
   - Use security monitoring methods (e.g., intrusion detection devices such as alarms or closed circuit television) to aid in determining whether a suspected contamination event is the result of an intentional act. (Also see feature 5)
   - Establish working relationship with local, state, and public health communities to detect public health anomalies and evaluate them for contamination implications.

4. **Assess risks and periodically review (and update) vulnerability assessments to reflect changes in potential threats, vulnerabilities, and consequences. (Most strongly aligned with Goal 2, Objectives 1 – 3, although is a critical contributor to Goal 1, Objective 1.)**

   - Maintain current understanding and assessment of threats, vulnerabilities, and consequences.
   - Utilities will need to adjust continually to respond to changes in threats, vulnerabilities, and consequences.
   - Establish and implement a schedule for review of threats, vulnerabilities, and consequences and their impact on the vulnerability assessment at least every three to five years to account for factors such as, but not limited to, facility expansion/upgrades, community growth, etc.
   - Reassess threats, vulnerabilities, and consequences after incidents and incorporate lessons into protective practices.
   - Individuals who are knowledgeable about utility operations should conduct the reviews. Include an executive in the review process to provide an ongoing conduit of information to/from management.

- Use a methodology that best suits utility-specific circumstances and operating conditions; however, ensure the selected method supports the criteria outlined in the National Infrastructure Protection Plan (NIPP).

5. Establish physical and procedural controls to restrict access only to authorized individuals and to detect unauthorized physical and cyber intrusions. (Most strongly aligned with Goal 2, All Objectives.)

- Identify critical facilities, operations, components, and cyber systems (such as SCADA).
- Develop and implement physical and cyber intrusion detection and access control tactics that enable timely and effective detection and response.
- Utilize both physical and procedural means to restrict access to sensitive facilities, operations, and components; including treatment facilities and supply/distribution/collection networks.
- Define, identify, and restrict access to security-sensitive information (both electronic and hard copy) on utility operations and technical details.
- Establish means to readily identify all employees (e.g. ID badges).
- Verify identity of all employees, contractors and temporary workers, with access to facilities, through background checks as appropriate per local/state law and/or labor contract and other agreements.
- Test physical and procedural access controls to ensure performance.

6. Incorporate protective program considerations into procurement, repair, maintenance, and replacement of physical infrastructure decisions. (Most strongly aligned with Goal 2, All Objectives)

- Bring forward protective program considerations early in the design, planning, and budgeting processes to mitigate vulnerability and/or potential consequences and improve resiliency over time.
- Design and construction specifications should address both physical hardening of sensitive infrastructure; and adoption of inherently lower risk technologies and approaches where feasible.
- Design choices should consider ability to rapidly recover and continue services following an incident.

7. Prepare emergency response, recovery, and business continuity plan(s); test and review plan(s) regularly, update plan(s) as necessary to ensure NIMS compliance and to reflect changes in potential threats, vulnerabilities, consequences, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations. (Most strongly aligned with Goal 3, Objectives 1 and 3.)

- Understand the National Incident Management System (NIMS) guidelines established by DHS (as well as community and state response plans and FEMA Public Assistance procedures); and incident command systems (ICS). At a minimum, utility response and recovery planning should be NIMS compliant.
- Coordinate emergency plan(s) with community emergency management partners:
  - Establish interoperable communications systems where feasible to maintain contact with police, fire, and other first responder entities.

  - Establish internal protocols to maintain communications with employees to ensure safety and to coordinate response activities.

- Implement backup plans and strategies for critical operations, including water supply and treatment (to mitigate the potential public health, environmental, and economic consequences of events), power, and other key components.
- Maintain plan(s) that are exercised at least annually, identify circumstances that prompt implementation, and identify individuals responsible for implementation.
  - Provide employees with appropriate security and preparedness training and education opportunities.
  - At least annually review plan(s) and conduct exercises that address the full range of threats relevant to the utility.
  - Update plan(s), as necessary, to incorporate lessons from training, exercises, and incident responses.
- Ensure plan(s) identify critical and time sensitive applications, vital records, processes, and functions that need to be maintained; and the personnel and procedures necessary to do so until utility has recovered. At a minimum, plan(s) should include a business impact analysis and address need for power, communication (internal and external), logistics support, facilities, information technology, and finance and administration-related functions; including necessary redundancy and/or timely access to backup systems and cash reserves.

8. Forge reliable and collaborative partnerships with first responders, managers of critical interdependent infrastructure, other utilities, and response organizations to maintain a resilient infrastructure. (Most strongly aligned with Goal 3, Objectives 2 and 4.)

- Partnerships should be forged in advance of an emergency, ensuring utilities and key partners are better prepared to work together if an emergency should occur.
- Partnerships with other local utilities, peers, and associations should emphasize formation of, and participation in, mutual aid and assistance agreements such as a Water and Wastewater Agency Response Network (WARNs).
- Maintain awareness of industry best practices and available protective program-related tools and training.
- Establish relationship with critical customers (hospitals, manufacturing, etc.) to identify interdependency issues that may impact business continuity.
- Participate in joint exercises with identified partners as appropriate.

9. Develop and implement strategies for regular, ongoing communication about protective programs with employees, customers, and the general public to increase overall awareness and preparedness for response to an incident. (Most strongly aligned with Goal 4, Objective 1, although is critically supportive of Goal 1, Objectives 1 and 2.)

- Establish public communications protocol, including pre-prepared public announcement templates, to share critical information; and implement mechanisms for receiving community feedback.
- Public communication strategies should:
  - Identify means to reach customers and the general public with incident information;

  - Provide a mechanism for customers and the public to communicate with appropriate personnel about unusual or suspicious events;
  - Inform customers about appropriate actions to enhance their preparedness for potential incidents that may impact services; and
- Internal communication strategies should:
  - Increase and/or maintain employee awareness of protective program;
  - Motivate staff to support protective program strategies and goals;
  - Provide ways for staff to notify appropriate personnel about unusual or suspicious activities;
  - Ensure employees understand nature of, and restrictions on, access to security sensitive information and/or facilities; and
  - Ensure employee safety during an event or incident and enable effective employee participation during response and recovery efforts.
- Evaluate effectiveness of communication mechanisms over time.

10. Monitor incidents and available threat-level information; escalate procedures in response to relevant threats and incidents. (Most strongly aligned with Goal 4, Objective 2, although a critical contributor to Goal 1, Objective 1 and Goal 3, Objective 3.)

- Develop standard operating procedures to identify and report incidents in a timely way and establish incident reporting expectations.
  - In the specific context of intentional threats and acts, ensure staff can distinguish between normal and unusual activity (both on/off site) and know how to notify management of suspicious activity.
- Develop systems to access threat information, identify threat levels, and determine the specific responses to take.
  - Investigate available information sources locally, and at the state or regional level (e.g., FBI Infraguard and Water ISAC).
  - Where barriers to accessing information exist, make attempts to align with those who can, and will, provide effective information to the utility.
- Make monitoring threat information a regular part of the protective program designee's job and share utility-, facility- and region-specific threat levels and information with key staff and those responsible for protection.