Awwa Research Foundation
Advancing the Science of Water®

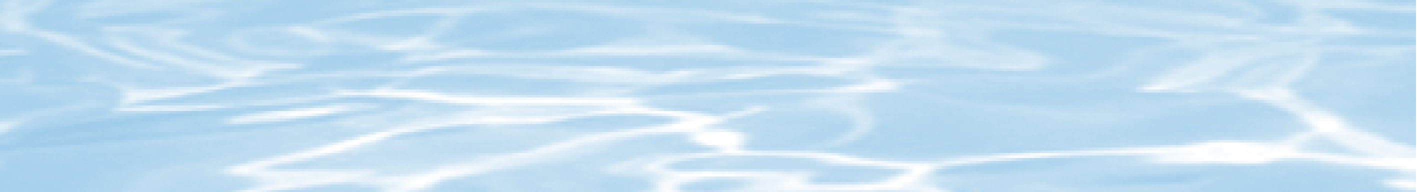
EPA

dwi

WERF

Physical Security Technologies for Water and Wastewater Utilities

Subject Area:
Efficient and Customer-Responsive Organization



Physical Security Technologies for Water and Wastewater Utilities

Awwa
Research
Foundation®

About the Awwa Research Foundation

The Awwa Research Foundation (AwwaRF) is a member-supported, international, nonprofit organization that sponsors research to enable water utilities, public health agencies, and other professionals to provide safe and affordable drinking water to consumers.

The Foundation's mission is to advance the science of water to improve the quality of life. To achieve this mission, the Foundation sponsors studies on all aspects of drinking water, including supply and resources, treatment, monitoring and analysis, distribution, management, and health effects. Funding for research is provided primarily by subscription payments from approximately 1,000 utilities, consulting firms, and manufacturers in North America and abroad. Additional funding comes from collaborative partnerships with other national and international organizations, allowing for resources to be leveraged, expertise to be shared, and broad-based knowledge to be developed and disseminated. Government funding serves as a third source of research dollars.

From its headquarters in Denver, Colorado, the Foundation's staff directs and supports the efforts of more than 800 volunteers who serve on the board of trustees and various committees. These volunteers represent many facets of the water industry, and contribute their expertise to select and monitor research studies that benefit the entire drinking water community.

The results of research are disseminated through a number of channels, including reports, the Web site, conferences, and periodicals.

For subscribers, the Foundation serves as a cooperative program in which water suppliers unite to pool their resources. By applying Foundation research findings, these water suppliers can save substantial costs and stay on the leading edge of drinking water science and technology. Since its inception, AwwaRF has supplied the water community with more than $300 million in applied research.

More information about the Foundation and how to become a subscriber is available on the Web at **www.awwarf.org.**

Physical Security Technologies for Water and Wastewater Utilities

Prepared by:
Kenneth A. Thompson, **Ralph N. Bell**, **Jane Mailand**, and **Katie Chamberlain**
CH2M HILL
9193 South Jamaica Street, Englewood, Colorado 80112
and

Barbara Heydorn
SRI Consulting Business Intelligence
333 Ravenswood Ave., Menlo Park, California 94025

Jointly sponsored by:
Awwa Research Foundation
6666 West Quincy Avenue, Denver, CO 80235-3098

United Kingdom Drinking Water Inspectorate
55 Whitehall, Room M/08, London, SW1A 2EY, England

Water Environment Research Foundation
635 Slaters Lane, Suite 300, Alexandria, VA 22314

U.S. Environmental Protection Agency
Washington, D.C 20460

Published by:

Awwa
Research
Foundation

Distributed by:

American Water Works
Association

IWA
Publishing

DISCLAIMER

This study was funded by the Awwa Research Foundation (AwwaRF), the U. S. Environmental Protection Agency (USEPA) under Cooperative Agreement No. CR-83110401, the United Kingdom Drinking Water Inspectorate (DWI), and the Water Environment Research Foundation (WERF). AwwaRF, USEPA, DWI, and WERF assume no responsibility for the content of the research study report in this publication or for the opinions or statements of fact expressed in the report. The mention of trade names for commercial products does not represent or imply the approval or endorsement of AwwaRF, USEPA, DWI or WERF. This report is presented solely for informational purposes.

ISBN 978-1-60573-034-9

Printed in the U.S.A.

Printed on recycled paper

CONTENTS

TABLES

FOREWORD

The AWWA Research Foundation is a nonprofit corporation that is dedicated to the implementation of a research effort to help utilities respond to regulatory requirements and traditional high-priority concerns of the industry. The research agenda is developed through a process of consultation with subscribers and drinking water professionals. Under the umbrella of a Strategic Research Plan, the Research Advisory Council prioritizes the suggested projects based upon current and future needs, applicability, and past work; the recommendations are forwarded to the Board of Trustees for final selection. The foundation also sponsors research projects through the unsolicited proposal process; the Collaborative Research, Research Applications, and Tailored Collaboration programs; and various joint research efforts with organizations such as the U.S. Environmental Protection Agency, the U.S. Bureau of Reclamation, and the Association of California Water Agencies.

This publication is a result of one of these sponsored studies, and it is hoped that its findings will be applied in communities throughout the world. The following report serves not only as a means of communicating the results of the water industry's centralized research program but also as a tool to enlist the further support of the nonmember utilities and individuals.

Projects are managed closely from their inception to the final report by the foundation's staff and large cadre of volunteers who willingly contribute their time and expertise. The foundation serves a planning and management function and awards contracts to other institutions such as water utilities, universities, and engineering firms. The funding for this research effort comes primarily from the Subscription Program, through which water utilities subscribe to the research program and make an annual payment proportionate to the volume of water they deliver and consultants and manufacturers subscribe based on their annual billings. The program offers a cost-effective and fair method for funding research in the public interest.

A broad spectrum of water supply issues is addressed by the foundation's research agenda: resources, treatment and operations, distribution and storage, water quality and analysis, toxicology, economics, and management. The ultimate purpose of the coordinated effort is to assist water suppliers to provide the highest possible quality of water economically and reliably. The true benefits are realized when the results are implemented at the utility level. The foundation's trustees are pleased to offer this publication as a contribution toward that end.

David E. Rager
Chair, Board of Trustees
Awwa Research Foundation

Robert C. Renner, P.E.
Executive Director
Awwa Research Foundation

ACKNOWLEDGMENTS

The authors of this report are indebted to the following water utilities and individuals for their cooperation and participation in this project:

Third-Party Contributors:
City of Phoenix Water Services Department; Danny W. Murphy
City of Glendale Utilities Department; Roger S. Bailey, P.E.
Contra Costa Water District; David J. Huey

Utility Panel:
Toronto Water; Walter Chan, CPP, CSPM, CPO
City of Glendale; Richard Levernier
Pinellas County Utilities; Alan Bollenbacher
Metro Wastewater Reclamation District; Leonard Carson
City of Phoenix Water Services Department; Madeline F. Goddard, P.E.
Contra Costa Water District; Michael D. Holley
City of Calgary Disaster Services/Water Services; Greg Solecki
Kennebec Water District; Jim Hart

Survey Participants:
The water and wastewater utilities and their representatives that participated in this portion of the project, but who are not mentioned by name in consideration of the confidentiality of the data that they provided

In addition, the advice and assistance of the Project Advisory Committee (PAC), including Dave Hook, Santa Clara Valley Water District, San Jose, California; John Balliew, El Paso Water Utilities, El Paso, Texas; John Gray and Jim Foster, U.K. Drinking Water Inspectorate, London, England; Roy Ramani, Water Environment Research Foundation (WERF), Alexandria, Virginia; Alan Roberson, American Water Works Association (AWWA), Washington, D.C.; and India Williams and Frank Blaha, AwwaRF Project Managers, are greatly appreciated.

EXECUTIVE SUMMARY

The goal of this project is to provide detailed information on commercially available security technologies to help utilities make sound buying decisions. These decisions should serve to increase physical security at these utilities while balancing risk and cost concerns. The Physical Security Technologies Decision Tool for Water and Wastewater Utilities (Decision Tool, CD in the back of the report) and the associated application guidelines developed for this project, will fill a critical information gap for both water and wastewater utilities. The application guidelines are designed to assist utilities by providing the information necessary to select and apply appropriate physical security enhancements. The primary deliverable for this project is the Decision Tool and the associated application guidelines provided on the compact disc (CD) provided with this report; the purpose of this report is to provide background on the project for the reader or future researcher.

Research was conducted in several areas: a literature search, discussions with personnel experienced in physical security at water and wastewater utilities, and a survey of 43 utilities regarding their current and future plans for physical security. Analysis of these data pointed to the physical security technologies for which application guidelines were prepared.

The Decision Tool was developed to assist the utility user in determining the types of physical security technologies that would be most appropriate for the utility's specific situation. Based on the user's input, the Decision Tool identifies appropriate technologies and links the user to the application guidelines that describe and provide specifications for the identified technologies. To assist those utilities that do not have the computer resources to run the Decision Tool, an HTML file that links a table of contents to the application guidelines alphabetically and by facility (such as a pump station or water treatment plant) is also provided on the CD containing the Decision Tool.

The research also resulted in the following conclusions and recommendations:

- Many utilities were hesitant or declined to provide security-related information despite assurances that the information would be confidential, not attributed to any specific utility, and combined with the information from all other participating utilities. The utilities that did respond, however, cited information sharing between utilities as an important element in the successful implementation of physical security. Methods to increase utilities' comfort and ability to share information in a trusting, yet confidential, manner would benefit the water and wastewater industries overall.
- The majority of utilities apply traditional physical security measures, such as fences, locks and manual keys, and lighting, and many have added more sophisticated technologies, such as closed circuit television (CCTV) systems and electronic sensors. Very few have added ultra-sophisticated technologies such as biometrics, and smoke and foam obscurement. As physical security technologies continue to improve and expand, it will be necessary for utilities to be informed both about improvements to traditional technologies and the development of new, more advanced technologies. Without this knowledge, utility decision makers will be unable to determine whether the new or improved technologies are appropriate and beneficial to their specific utility circumstances.
- In the eyes of utilities, physical security does not stand alone. Utilities see the operational and procedural aspects of security as integral to the use of technologies

and equipment. Integrating operational and procedural information with physical security technology information will help utilities to effectively integrate physical security into their facilities.

- The information contained in the Decision Tool is most applicable to non-physical security experts, most likely to be working in small- to medium-sized utilities that do not employ a security expert and rely on utility managers to make security decisions. However, the information contained in the Decision Tool will be useful to all.

Suggested future research includes the following:

- Determine the statistical validity of the data collected from the interview surveys.
- Increasing the amount and availability of independent sources of information for physical security technologies.
- Continuously improving the Decision Tool with more information and data.

CHAPTER 1
BACKGROUND

The goal of this project is to provide detailed information on commercially available security technologies to help utilities make sound buying decisions that will serve to increase the physical security of their facilities. Guidelines for the application of various physical security technologies that could provide utilities with information related to effectiveness and risk reduction potential of these technologies do not exist. The result can be that an inappropriate application is purchased and implemented that does not adequately reduce risk or is not applicable to the intended purpose.

Improving the physical security of water systems in the United States has become a priority for utility managers and governing bodies since the events of September 11, 2001. Protection of water systems from malevolent acts is also a very high priority for federal agencies such as the Department of Homeland Security (DHS) and the U.S. Environmental Protection Agency (EPA). The EPA is responsible for working with the water sector (including water and wastewater utilities) to protect of the nation's critical water infrastructure, including the systems used to collect, treat, and distribute potable water. The EPA has a similar responsibility for wastewater operations. These critical infrastructures are fundamental to public health and welfare and are subject to both natural disasters such as floods and earthquakes, and man-made hazards such as terrorist attacks. Such disasters could place surrounding areas and populations at significant risk.

There are many definitions of "best practices" in regard to security implementation at utilities, but they all hinge on the availability of knowledge acquired through experience and/or research on the topic. Water utility managers are dedicated to serving the public's needs and, in that context, may see potential value in establishing rigorous security systems. To establish a successful security system, information on available and applicable security technologies must be accessible. This need for information creates a demand for specific guidance that allows water professionals to make informed decisions. The major result of this project (the Physical Security Technologies Decision Tool for Water and Wastewater Utilities [Decision Tool]) should provide the information necessary for these professionals to make the decisions necessary to protect their water systems from accidental or unauthorized access. In addition, utility implementation of physical security systems and technologies can result in improvements and multiple-use mitigation measures that support utility security and operational life-cycle benefits.

The Decision Tool and its associated application guidelines will fill a critical information gap for both water and wastewater utilities. The guidelines will provide utilities with the tools to implement the physical security enhancements identified in vulnerability assessments or through other means by assisting them in selecting the appropriate applications to reduce risk to an specified level. The primary deliverable for this project is the Decision Tool and the associated application guidelines provided on the compact disc (CD) provided with this report; the purpose of this report is to provide background and supporting information for the user.

CHAPTER 2
APPROACH

The project consisted of the following activities:
Task 0: Conduct Chartering Session
Task 1: Define Risk-Based Goals and Objectives
Task 2: Perform Database Definition and Design
Task 3: Conduct Background Research
Task 4: Conduct Interviews
Task 5: Compile and Analyze Data
Task 6: Develop Proposed Application Guidelines

TASK 0: CONDUCT CHARTERING SESSION

A chartering session was conducted on February 10, 2006 and was attended by those listed in Table 2.1.

The purpose of the chartering session was to finalize the Scope of Work that would be the roadmap for project execution. Prior to the session, a draft Scope of Work was provided for review. The chartering session included the following activities:

- Finalize the Scope of Work
- Establish project priorities and goals
- Define expectations and critical success factors
- Finalize project team roles, responsibilities, and methods for communication
- Discuss logistics of the project development process
- Finalize the project schedule, including meetings and conference calls
- Finalize procedures for receiving and incorporating comments on drafts

Table 2.1
Attendees at the project chartering session

India Williams, AwwaRF	Susan Turnquist, AwwaRF
Alan Roberson, American Water Works Association (AWWA)	John Gray, Drinking Water Inspectorate (United Kingdom)
Dave Hook, Santa Clara Valley Water District	Roy Ramani, Water Environment Research Foundation (WERF)
Ken Thompson, CH2M HILL	Forrest Gist, CH2M HILL
Rex Hesner, CH2M HILL	Wesley Go, CH2M HILL
Jane Mailand, CH2M HILL	

TASK 1: DEFINE RISK-BASED GOALS AND OBJECTIVES

The goal of Task 1 was to develop a comprehensive understanding of the risk-based goals and objectives that can be achieved by incorporating a wide range of physical security systems and technologies into water and wastewater systems. The combination of physical security recommendations resulting from vulnerability assessments (VAs) and experience obtained from conducting VAs was identified as an effective way to provide this information.

Recommendations from previously conducted VAs were reviewed, and discussions held with personnel responsible for conducting VAs in response to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. It was also the intent to draw from the experience of those who conducted a review of VAs for EPA. However, this approach could not be used due to the extremely confidential nature of that work. To replace this source of information, information from a recently hired employee, who in a previous position with a nationwide water utility company developed physical security systems for over one hundred facilities in 17 states, was included in the development of the risk-based goals and objectives, and the interview results included in the description of the activities in Task 4.

Physical security recommendations resulting from water utility VAs were compiled and categorized by the general type of critical facility or asset. Each utility assessed had unique infrastructure with a unique set of environmental conditions and existing physical security equipment. This compilation presented a general sense of the current state of physical security at water utilities of various sizes. However, because the information was facility- or asset-specific, it could not alone point to specific physical security elements that are or should be used by a particular facility or asset type.

Discussions with personnel familiar with water utility VAs helped to focus the types of physical security equipment most frequently used, as well as common facilities and assets. These personnel were certified in Sandia National Laboratories' Risk Assessment Methodology for Water (RAM-W^{TM}), an approach that focuses on the effectiveness of the security system for individual drinking water system components. The group identified 14 common facilities that are part of most water and wastewater utilities and 19 types of physical security equipment used at these facilities. One facility and six technologies were added based on the review of *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA/WEF 2006b) and *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006a), and through discussions with security technology experts. The common facilities and complete list of physical security technologies are listed in Tables 2.2 and 2.3.

Table 2.2
Common facilities in water and wastewater utilities

Source water reservoirs and intakes	Water distribution system
Groundwater wells	Turnouts/interconnects with other utilities
Source water transmission pipelines	Support facilities
Water treatment plants	Collection systems
Pump stations (raw or treated water)	Lift stations
Finished water storage	Wastewater treatment plants
Valves, hydrants, vaults, and meters	Outfall pipes

Table 2.3
Physical security equipment types

Access Control Systems (Software and Control Units)	Ladder Cages
Electric and Mechanical Locks	Special Locks (manhole, hydrants, valve)
Key code pads (electronic or manual)	Operator Duress Devices
Card Readers	Perimeter Walls and Toppings
Biometrics	Sally Port Entrances
Door Sensors/Switches	Security Doors
Closed Circuit Television Systems (cameras, storage devices, video software)	Security Grilles
Chemical Fill-Line Locking Devices	Security Lighting
Building Entrance Security	Sensors (buried line, microwave, linear beam, infrared, dual technology, glass-break, fence-mounted, pipeline)
Equipment Enclosures	Signage
Exterior Surfaces (special coatings, etc.)	Vent Security
Fences and Gates	Wiring Protection
Fence/Gate Enhancements	

In addition to utility infrastructure and physical security equipment, the group also discussed the risks to water and wastewater utilities. While risks to utilities can come from natural sources, such as weather, or from accidents, such as a spill resulting from a traffic incident, the groups focused on risks from manmade sources. Man-made risks are purposefully created by vandals, criminals, terrorists, rioters, and even employees of a utility. The risks faced by a utility range from damage to or theft of equipment and supplies to contamination of the raw water supplies (surface water or groundwater), treatment system (water or recycled water), distribution system (water or recycled water), collection system, wastewater treatment system, and outfall. The intent of physical security against man-made risks is to stop a malevolent action before it can affect the target (prevention); interrupt the action against the target (delay); or identify, respond, and stop/capture the perpetrators before or after a target is reached (detection and response).

Prevention is not easily measured because it would require suspected threats to be interviewed to determine why they had not yet attempted to attack a particular facility. Information such as this is difficult to obtain. Response is not directly related to the physical security in place at water and wastewater utility infrastructure. As such, it was determined that the risk-based goals and objectives related to man-made risks that a utility could apply in regard to physical security are delay and detection (Table 2.4).

Table 2.4
Goals and objectives of physical security in response to man-made risks

Objective	Methods	General considerations
Delay	Signs, advertisements, fences, walls, warning lights, solid covers and doors, limitations on the size of door and window openings, bars on windows/openings, locks, hidden hinges, multiple barriers, loss of vision or movement capability	• Consideration should be given to what is being protected and why. • Delay is accomplished by one or more physical barriers between the attacker and the critical assets of the operation that make the target more difficult and more time-consuming to reach. • Delay methods, beginning with the facility perimeter and moving closer to the critical assets, can be integrated into layers of security that begin at the facility perimeter and proceed inward. • Visible security must be functional and not a decoy. • Critical assets must be out of sight and hard to reach.
Detection	Visual detection or cameras, motion sensors, heat or pressure sensors, torsion sensors on fences, on-line water quality monitoring, lighting, digital recording, transmission equipment	• Detection is accomplished when a potential threat is noticed, identified, and assessed. • Visual verification is needed of who, when, and where intruders enter controlled areas. • Detection monitoring systems must be reliable and have low false alarm rates. • Detection is not valuable if no response measures are in place, or if no one is monitoring detection information.

The final aspect of physical security discussed by the group was the prioritization of the various types of physical security equipment that a utility would implement as part of a comprehensive security system. The consensus was that a layered approach to security, beginning at the outside of a site and working inward with a focus on critical assets, was most effective for external threats such as vandals, criminal, and saboteurs. Critical assets were described as meeting at least one of the following characteristics: (1) a single point of failure that would cause the entire facility or system to fail, (2) something without which the facility or system could not exist (for example, a water system could not operate without source water; if the system had source water available, then it could not operate without treatment), and (3) a primary concern of the utility (for example, meeting its mission and vision or protecting against a specific threat, such as the theft of copper). A more detailed description of the ways in which a utility would prioritize the implementation of physical security equipment using the layered approach from the outside in is provided in Appendix A.

During this time, the project team interfaced with the American Society of Civil Engineers (ASCE), American Water Works Association (AWWA), and the Water Environment Federation (WEF) to develop voluntary consensus standards in accordance with ASCE Rules for Standards Committees. These standards, titled "Guidelines for the Physical Security of Water Utilities" (ASCE/AWWA/WEF 2006b) and "Guidelines for the Physical Security of Wastewater/Stormwater Utilities" (ASCE/AWWA/WEF 2006a), were based on earlier guidance documents (developed by CH2M HILL for AWWA and WEF) and underwent balloting by a balanced standards committee. A summary of the site-specific physical security recommendations drawn from the documents are included as Appendix B to this report based on the usefulness of the information and the agreement between the documents and the experience of the project team.

TASK 2: PERFORM DATABASE DEFINITION AND DESIGN

The goal of Task 2 was to create a database to store and categorize the information gathered in Tasks 1, 3, and 4 and ultimately be used as a part of a tool to assist utilities in identifying, purchasing, and installing physical security equipment. While the data were compiled with the specific purpose of developing the physical security application guidelines, future audiences and purposes for this information were also considered. Database development comprised the following components:

- Database Design and Development
- Queries Development
- Forms and Reports Development
- Testing
- Documentation

This effort continued throughout the project as the data and the database were updated and refined to include additional information as it became available.

To begin the process, the desired outputs of the database application were identified: applicable technologies for utility security systems and the format of the application guidelines that would be used to deliver this information to utilities. The security equipment and technologies compiled during Task 1 (and listed in Table 2.3) were identified as applicable and appropriate for the purposes of this project. The best format of the application guidelines was determined to be electronic files provided in portable document format (pdf) that could be viewed on-screen, saved to the user's personal computer (PC), or printed for future use.

The next step was to determine the functional requirements of the database. Two primary requirements were identified. The first was to provide the user with a list of applicable technologies based on user-specified facility or asset characteristics. The relevant characteristics were determined to be threat type, facility type, function, environment, climate, and power and communication capability. The second was to provide the user with ability to select specific application guidelines without regard to their appropriateness to a specific facility or asset. It was also important that the database be easy to use and maintain. In parallel, the system requirements for the database application were determined. The preferred delivery of the system was via compact disc (CD), so the database application was designed to be loaded onto a PC.

Once a draft version of the database was complete, the application underwent testing by a Utility Panel. Eleven utilities throughout the United States and Canada initially agreed to review the database application; eight provided input in time for preparation of this report. The comments received were incorporated into the database application as appropriate

TASK 3: CONDUCT BACKGROUND RESEARCH

The purpose of Task 3 was to compile security-related information from both inside and outside the water and wastewater industries and develop a list of contacts that could provide additional information and feedback on physical protection systems that have been tested in everyday use.

The information sources initially identified for review and a brief annotation of the contents of each source are provided in Table 2.5. Information contained in these documents supported the continuing development of the list of physical security technologies currently in use by the water and wastewater communities. As the project continued, additional sources, some specific to a particular technology, were added and are included in the References found at the end of this document. Relevant information from each of these sources was added to the physical security technology application guidelines.

Eighty-one utilities were contacted via e-mail or telephone to ask whether the utility would be interested in participating in a survey regarding physical security. Fifty-three of those contacted agreed to participate in the survey. (The interview survey and process are discussed in Task 4.) The reasons that utilities declined to provide information was not specifically tracked. However, anecdotally, the utilities that did not provide information cited two primary reasons: (1) the feeling that the utility was not a good candidate for this research because they did not have enough security data to provide and (2) reluctance to share security information.

To further supplement the information about physical security, a CH2M HILL employee who had developed physical security systems for over one hundred utilities in 17 states for a previous employer was asked to complete a single survey that comprised relevant data from all of those systems. To preserve the security of those facilities, the employee's name and former employer are not provided in this report.

An attempt to gather security information from other industries was also made. A list of ten contacts was provided by a CH2M HILL employee who had performed security-related work for industrial clients, and a survey was e-mailed to these clients.

Table 2.5
Information sources for literature review

Reference	Annotation
American Society of Industrial Security (ASIS). 2004. Protection of Assets. Alexandria, VA.	ASIS works across multiple business sectors for developing security applications. Many of these applications are easily transferable over to the water and wastewater industry. This document is a compilation of practical treatments of a broad range of protection subjects, strategies, and solutions.
American Water Works Association (AWWA). 2004. Interim Voluntary Security Guidance for Water Utilities. Denver, CO. www.awwa.org/science/wise/	This document provides an approach for identifying areas of required security protection based on a water utility's design basis threat. USEPA Water Infrastructure Security Enhancements (WISE) ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at the ASCE, AWWA, WEF, and USEPA web sites.
Department of Defense (DoD). 2002. Minimum Antiterrorism Standards for Buildings. Unified Facilities Criteria UFC 4-010-01. www.tisp.org/files/pdf/dodstandards.pdf	The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria for buildings.
Naval Facilities Engineering Service Center (NFESC). 1999. Selection and Application of Vehicle Barriers (MIL-HDBK-1013/14). Washington Navy Yard, DC. www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_14.pdf	This handbook provides guidance to ensure that appropriate design, operational, environmental, cost, security, and safety considerations are included in the selection process for vehicle barrier systems. Topics covered in the handbook include: vehicle barrier requirements, vehicle barrier installation and design, and descriptions and data on commercially available vehicle barriers and passive barriers that can be constructed on site. Also included is a list of manufacturers for both active and passive vehicle barriers, examples on how to use the selection process delineated in the handbook, and cost data for the various vehicle barriers discussed.

(continued)

Table 2.5 (continued)

Naval Facilities Engineering Service Center (NFESC). 1993a. Design Guidelines for Physical Security of Facilities (MIL-HDBK-1013/1A). Washington Navy Yard, DC. www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_1a.pdf	This manual provides guidance to ensure that appropriate physical security considerations are included in the design of general facilities. Aspects considered in this manual include the pre-design phase, the assessment of physical security threats, and an overview of the design phase. Specific technical sections in the manual also describe exterior site physical security, building physical security, ballistic attack hardening, standoff weapon hardening, and bomb blast hardening.
Naval Facilities Engineering Service Center (NFESC). 1993b. Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities (MIL-HDBK-1013/10). Washington Navy Yard, DC. www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_10.pdf	This military handbook provides guidance and detailed criteria for the design, selection, and installation of new security fencing, gates, barriers, and guard facilities for perimeter boundaries of Navy and Marine Corps installations or separate activities, and designated restricted areas.
U.S. General Services Administration (GSA). 2005. Facilities Standards for the Public Buildings Service. Washington, DC. http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8195&channelPage=%2Fep%2Fchannel%2FgsaOverview.jsp&channelId=-17304	These design standards and criteria are to be used in the programming, design, and documentation of GSA buildings. These standards and criteria include the physical security aspects that can be integrated into the functional design of a building and augmented by follow-on physical security enhancements.
Water Environment Federation (WEF). 2004. Interim Voluntary Security Guidance for Wastewater/Stormwater Utilities, Alexandria, VA. www.wef.org/ConferencesTraining/TrainingProfessionalDevelopment/WaterSecurity/	This document provides an approach for identifying areas of required security protection based on a wastewater or stormwater utility's design basis threat. USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at the ASCE, AWWA, WEF, and USEPA web sites.
Water Environment Federation (WEF). 1998. Design of Municipal Wastewater Treatment Plants, Manual of Practice No. 8, 4th Edition. Alexandria, VA.	This industry standard for wastewater design describes the critical process for a wastewater treatment plant that should be evaluated for redundancy and additional protection. This document is also known as ASCE Manual of Practice No. 76.

TASK 4: CONDUCT INTERVIEWS

An iterative process was used to ensure the survey questions were worded in such a way that they would elicit the intended type of information for this project. (The final survey is provided as Appendix C.)

Professional interviewers conducted the survey. Three organizations were selected to serve as a pilot test for the survey document prior to the survey being conducted on a wider basis. Based on results of the pilot, the survey was slightly modified to meet interviewees' time constraints and to further refine the questions. Responses were received from 40 of the 53 utilities that agreed to participate in the survey (of the remaining 13, four declined to participate and nine did not respond to repeated telephone and e-mail requests). Three additional also completed surveys.

Random numbers were assigned to the completed surveys (for anonymity purposes) and the completed surveys were reviewed to ensure that no identifying information was contained within. At the completion of this project, the original surveys and all other identifying information will be destroyed to ensure anonymity of the respondents.

A second, limited version of the survey was being prepared for use in interviewing industrial organizations about the physical security technologies that they have used. The intent of this version was to determine whether organizations outside of the water and wastewater utility community have a different perspective on the selection and implementation of physical security technologies. Of the ten organizations solicited for information, four provided responses.

TASK 5: COMPILE AND ANALYZE DATA

The data collected during Tasks 1, 3, and 4 were reviewed and analyzed to identify trends, disparities, lessons learned, and other requirements and recommendations that apply to physical security technologies. Overall, the data were used to review the selection of physical security technologies for which application guidelines were created and to identify the topic areas in the application guidelines. Some data were ultimately incorporated into the appropriate application guidelines.

TASK 6: DEVELOP PROPOSED APPLICATION GUIDELINES

The purpose of Task 6 was to incorporate the information developed in Tasks 1 through 5 into a comprehensive set of application guidelines. The application guidelines are the output of the Decision Tool; they are intended to assist utilities in selecting appropriate security technologies for their given applications. Application guidelines were created for all physical security technologies identified in Table 2.3.

The application guidelines were provided as PDF files to the database development team for inclusion into the Decision Tool. For proper integration of the application guidelines into the database, the following criteria based on the functional requirements identified in the description of Task 2 were identified, applied to each technology, and entered into the database application:

- Function of the technology (detect, delay)
- Applicable facilities at which the technology may be used
- Threats the technology can protect against (insider, criminal, vandal, saboteur)
- The environment (indoors, outdoors) in which the technology may be used

- The climates (extreme heat, extreme cold, wet, dry, poor visibility) in which the technology may be used
- Power availability
- Data communication availability

This criteria information identified for each technology serves to connect the technology to the threat type, facility type, function, environment, climate, and power and communication capability that the user selects for a particular facility or asset. For example, if a user identifies (selects) that he would like information about a technology that can detect a criminal at a maintenance storage yard where both power and data communication are available, the database application would identify, among other technologies, a CCTV system.

Because legal liability varies from state to state, no liability issues were addressed as part of the application guidelines. Users of this information should verify that security measures are implemented within the confines of state and local regulations.

CHAPTER 3
OBSERVATIONS

From the data-gathering portion of this project, some observations have been drawn regarding the following areas:

- The willingness of utilities to share security-related data for the purposes of research and the education of other utilities
- The types of physical security technologies currently in use by water and wastewater utilities and the direction in which it seems utilities are heading
- The beliefs utilities have about the use of security at their facilities
- The audience for the Decision Tool

Each of these areas is discussed more fully below.

THE WILLINGNESS TO SHARE SECURITY-RELATED DATA

Utilities consider it important to benefit from the experience of other utilities. When utilities were asked for suggestions that they would make to utilities that are selecting/installing/operating security equipment (question 6 in the survey), seven responses included references to obtaining information from other utilities:

- "Talk to other Utilities to determine which systems really work." (Entry no. 4)
- "…visit existing utilities that have successful systems." (Entry no. 5)
- "Talk with utilities that have gone through the process and have learned or are learning the hard way how to transition from the water business to the security business." (Entry no. 15)
- "Go visit similar installation and determine for yourself if they will work in your application." (Entry no. 16)
- "Look at what other utilities have done and see how effective it is." (Entry no. 23)
- "You need to spend the time to research different options, whether it is by visiting other locations, talking to other facilities, or meeting with the vendors." (Entry no. 35)
- "Visit sites and talk with end users of the equipment to be purchased." (Entry no. 41)

One drawback to the consideration of these utilities' opinions is that, like any voluntary survey, the opinions and other data provided are those of respondents who are willing to share data. It is possible that utilities that do not wish to share opinions and data would not be interested in the opinions and data of other utilities.

To support the effort to obtain physical security-related data from water and wastewater utilities, great care was taken to assure the utilities that their highly sensitive data would be handled confidentially, that the data provided would be used collectively, and that no data would be attributed to the utility specifically.

Confidentiality and security of data were also addressed in the cover letter to the recipients of the interview surveys (which can be found on the last page of Appendix D):

> Your answers will be incorporated into a summary document designed to provide the utility industry with useful information on real-world security experiences. In the summary document, no information will be attributed to your organization directly; instead, your information will be summarized with the information from

> all of the other participating utilities. We understand the importance of maintaining your organization's confidentiality and respecting your security concerns. Access to the individual surveys will be limited to project team members at SRIC-BI and CH2M HILL.

Despite these assurances, only 53 facilities agreed to provide security-related data. While realizing that the reluctance to share security-related data was not the only reason for declining, it was one of the primary reasons. This is unfortunate because it appears that, for at least the utilities completing the survey, the experience of others like themselves is considered valuable.

An ongoing AwwaRF project, *Critical Information Policies for Water Utilities* by Stratus Consulting 2007, is finding that utilities are very concerned about negative consequences that could result from the sharing of security data, so they tend not to share that data. This concern clearly had an impact on the data collection associated with this physical security technologies project survey, and subsequent conclusions and recommendations. Those conducting security-oriented projects should be aware of and understand this reluctance to share security information, and build this consideration into their project plans.

The Critical Information Policies project suggests that utilities identify levels of information sensitivity and specific policies applicable to each level. Practices such as this and established standards and requirements for information and data sharing may partly overcome utilities' reluctance to share security information for the benefit of all.

THE TYPES OF PHYSICAL SECURITY TECHNOLOGIES IN USE NOW AND IN THE FUTURE

Most of the utilities that responded to the survey use traditional security technologies, such as fences, locks and manual keys, and lighting, and many have added more sophisticated technologies, such as CCTV systems and sensors (which were rated as the most effective types of equipment; as such, the application guidelines in the database are the most robust for these technologies). Very few have added ultra-sophisticated technologies such as biometrics and smoke or foam obscurement. The most common types of security equipment used by the responding utilities at each of the facilities types listed in the survey are provided in Table 3.1.

Most utilities (75 percent) use both internal and contracted support personnel to maintain and monitor their security equipment.

Table 3.1
Most common types of security equipment
used by responding utilities at specified facilities

Facility type	Security equipment in use (percentage of utilities using this equipment type*)
Source water reservoirs and intakes	Mechanical keys (85%) Security lighting (74%) Security locks (70%) Surveillance cameras (63%)
Groundwater wells	Mechanical keys (86%) Security lighting (68%) Security locks (55%)
Source water transmission pipelines	Mechanical keys (36%) Security locks (30%) Security lighting (21%)
Water treatment plants	Security lighting (97%) Mechanical keys (86%) Surveillance cameras (81%) Window/door sensors/alarms (75%) Security locks (69%) Card readers (69%) Security doors (61%) Fence/gate sensors/alarms (50%)
Pump stations (raw or treated water)	Mechanical keys (86%) Security lighting (86%) Security locks (64%) Security doors (58%) Window/door sensors/alarms (58%) Surveillance cameras (53%)
Finished water storage	Mechanical keys (78%) Security lighting (76%) Security locks (73%) Ladder cage (70%) Surveillance cameras (54%)
Valves, hydrants, vaults, and meters	Mechanical keys (54%) Security locks (33%) Security lighting (13%)
Turnouts/interconnects with other agencies	Mechanical keys (50%) Security locks (43%) Hatch sensors/alarms (13%) Guards or other monitoring personnel (13%)

(continued)

Table 3.1 (continued)

Facility type	Security equipment in use (percentage of utilities using this equipment type*)
Support facilities (offices, maintenance facilities, labs, etc.)	Security lighting (90%) Mechanical keys (77%) Card readers (69%) Window/door sensors/alarms (64%) Security locks (59%) Surveillance cameras (54%)
Collection systems	Mechanical keys (35%) Security locks (17%) Security doors (13%) Security lighting (13%) Water monitor for contaminants (13%)
Lift stations	Mechanical keys (78%) Security lighting (70%) Security locks (57%)
Wastewater treatment plants	Security lighting (95%) Mechanical keys (74%) Security locks (63%) Card readers (47%)
Outfall pipes	Mechanical keys (35%) Security locks (18%) Security lighting (12%) Other types of physical security equipment (12%)

*The criterion for "most common equipment types" was considered to be equipment types used by more than 50 percent of the responding utilities that own or operate the specific type of facility. If no equipment type was used more than 50 percent of the time, the top three equipment types (by percentage) are listed.

Few utilities (19 percent) have had to deal with public concerns about security equipment on their sites. Often contact with the public is simply providing responses to inquiries. Those utilities that did report public concerns listed the following:

- Cameras: suspicions about the use of cameras
- Fencing: dislikes about fencing, including dislike of "razor" wire, denial of access, and dislike of appearance
- Lighting: dislike of stray light and too much light

Sixty-five percent of utilities used at least some encryption of their security-related communications systems. Those who had concerns about the security of their communication systems listed the following:

- Hacking
- Reliability, especially of newer technologies, both in performance and security
- Cost

UTILITIES' BELIEFS ABOUT THEIR SECURITY SYSTEMS

When utilities were asked for suggestions on what other utilities should consider when selecting/installing/operating security equipment, the suggestions primarily referred to planning, operation, and implementation of the technology. The following items were most often:

- Design: Twenty-two of the 41 respondents to this survey question (no. 6) provided a response that related to the design of the security system. Identifying what should be accomplished before investing in a system, designing facilities with security in mind, using security experts to create the design instead of civil engineers, and applying industry guidelines were cited most frequently
- Equipment purchasing: Relating to the process used to purchase equipment and not to either specific equipment types or vendors, the largest number of respondents suggested talking to or visiting other utilities to see what works. An overall comment included the purchase and use of quality, compatible, and, preferably, non-proprietary equipment.
- Staff: Numerous comments related to staffing, but there was not one type of comment that outweighed the others. Overall, the comments discussed educating and training the staff on security issues and the use and management of internal and external security personnel.

Ninety-five percent of utilities consider their security systems to be somewhat to quite effective; 86 percent intend to improve/change their system. These statistics indicate that utilities consider security important enough to engage in a continuous improvement methodology for their security systems.

Seventy-eight percent of utilities have spent between $100,000 and $10,000,000 on security since 2001. Approximately half (46 percent) have a separate annual budgets for security. The amount spent on security most often ranges from less than one percent to five percent of a utility's total annual operating budget.

AUDIENCE FOR THE DECISION TOOL

Additional conclusions can be drawn from Utility Panel feedback provided in its review of the Decision Tool.

The Utility Panel generally found the database application easy to use, but stated that its content is most applicable to water or wastewater employees who are responsible for security, but who are not physical security experts. Representatives from larger utilities indicated that they already had this type of information and were looking for even more advanced security information, such as "unclassified controlled nuclear information" that would be obtained from the Department of Energy, Office of Security and Safety Performance Assurance. Smaller utilities that do not employ a security professional, but that instead rely on their utility managers for security planning and implementation, were recommended as the target audience for the type and level of information provided in the database application.

The Utility Panel also believed that systems integration information should be added to the database. Security equipment must not only work with other types of security equipment, but must also complement that equipment, as well as operational and procedural policies and activities. Some relationship between security equipment types can be intuited by the list of application guidelines provided for a specific type of facility with specific security characteristics, but the overall relationships between, for example, cameras and fencing, are not clearly defined.

CHAPTER 4
RECOMMENDATIONS

Based on the conclusions provided in the previous chapter, the following recommendations are made using the categories from the previous chapter.

THE WILLINGNESS TO SHARE SECURITY-RELATED DATA

Experiential data seem to be an important consideration by the utility respondents to the interview survey. Information provided by an experienced user of security products is more desirable than is information provided by vendors. Security information-sharing networks, such as WaterISAC and other state-sponsored organizations, currently exist; however, the scope of this project did not include whether and how frequently these venues for information sharing are used. Perhaps the distribution of the Decision Tool could be integrated with some type of an information-sharing technique.

In addition, other security-related projects should consider the reluctance of utilities to share security information and build this consideration into their project plans. If general standards and requirements for information and data sharing are developed and accepted prior to initiating a security-related project, utilities may be less reluctant to share security data.

THE TYPES OF PHYSICAL SECURITY TECHNOLOGIES IN USE NOW AND IN THE FUTURE

As physical security technologies continue to improve and expand, it will be necessary to continue to inform utilities both about improvements to traditional technologies and the development of new, more advanced technologies. Utility decision-makers must be knowledgeable about existing technologies to be able to evaluate a new or improved technology and determine whether it is appropriate and beneficial. It is also important that any security technology be used properly and consistently, which is unlikely if those using it are not provided with adequate information.

Because most utilities use both internal and contracted support personnel to maintain and monitor their security equipment, training these groups to work with one another effectively and efficiently is essential. Cross-training and tabletop exercises may be an effective way for each group to understand the roles, needs, and resources of the other. Without an understanding of how these two groups should work together, security measures may be ignored or used in an inefficient or unacceptable manner. An enhanced relationship between the two groups could only bring greater cooperation and, thus, improved security to a utility.

Fortunately, few utilities reported public concerns about security equipment on their sites. Continuing a positive relationship with the community is important, and good communication strategies can often allay concerns about security. In addition, sincere consideration for the public surrounding utility facilities can likely lower the percentage of those having difficulty with the public in regard to security-related equipment.

As utilities continue to implement security measures that rely on electronic communication, the need for knowledge about cyber security and its relationship to overall utility security will continue to grow. Focused information and education on cyber security provided in an easy-to-understand manner (for those whose skill set and responsibilities are not centered on information technology [IT]) may result in better cyber security for the utility.

UTILITIES' BELIEFS ABOUT THEIR SECURITY SYSTEMS

Many utilities responding to the interview survey made suggestions that primarily referred to planning, operation, and implementation of security technologies. Thus, it is clear utilities see the operational and procedural aspects of security as integral to the use of the technologies and equipment. When providing physical security technology information to utilities, a comprehensive discussion of the operational and procedural aspects related to a specific security technology may help the utility more effectively use that technology. With technology changing so quickly, it is necessary to review and update current security systems on a regular basis to ensure the desired level of security at a facility is adequately maintained in the most effective and efficient manner.

AUDIENCE FOR THE DECISION TOOL

Utility Panel participants indicated that the Decision Tool is easy-to-use, but is most applicable to water or wastewater employees who are responsible for security, but who are not physical security experts. The distribution of this information should focus on small- and medium-sized utilities that typically do not employ a security expert and who rely on utility managers for security decision-making.

The Utility Panel also recommended that systems integration information be added to the database. This is a valid suggestion, and a way to incorporate this information into the database should be considered.

CHAPTER 5
FUTURE RESEARCH

Suggested future research can be categorized into three areas:

- Determining the statistical validity of collected data
- Increasing the availability and amount of independent sources of information for certain technologies
- Continuously improving the Decision Tool

DETERMINING THE STATISTICAL VALIDITY OF THE COLLECTED DATA

Due to the limited time that security improvements have been implemented in the water and wastewater industry, the data collected include more subjective and anecdotal information rather than validated statistical data. As the industry matures, a statistical approach to data collection could be useful in gaining a more complete understanding of the technologies being used. Future research on this topic should include interviewing a larger group of utilities that can provide statistically valid data. With a larger group of participants, it will be easier to identify overall trends in the application of physical security technologies.

INCREASING THE AVAILABILITY AND AMOUNT OF INDEPENDENT SOURCES OF INFORMATION FOR CERTAIN TECHNOLOGIES

Future research efforts should include focusing on technologies that have little information currently available to the public. While performing Tasks 3 and 6, the lack of information available for certain technologies, such as pipeline sensors, CCTV video analytics, and biometrics, hindered the ability to provide a complete, useful application guideline to the end users of the Decision Tool. While there is adequate brand-specific information provided by vendors on these topics, there are few independent sources of information.

The American National Standards Institute (ANSI) established the Homeland Security Standards Panel to coordinate the development of homeland security and emergency preparedness standards. Hundreds of security-related standards are available for purchase from ANSI’s eStandards Store (ANSI 2007). The American Society for Industrial Security (ASIS) International, has developed the Security Industry Buyer’s Guide database. While this database lists sources for numerous types of security physical technologies and services, the information is provided solely by vendors. ASIS is in the process of developing physical security measure guidelines that may provide additional standards for specific physical security technologies.

For utilities to consider using a specific technology, especially more sophisticated technology, general background and technical information needs to be available on the topic. The availability of this information is necessary for a utility to understand not only how the technology can benefit their facility, but also to allow a utility to confidently contact vendors and inquire about integrating these technologies into their security system. For the more sophisticated technologies, it will be important to have independent analyses of these technologies.

CONTINUOUSLY IMPROVING THE DECISION TOOL

To continue improving the database in the future, more in-depth information may be added to the technology application guidelines. This would require ongoing research on the technologies available to the water and wastewater industries and informational updates to the database. It is suggested that the technologies be reviewed on a yearly basis to ensure information is up to date and that the possibility of adding new technologies to the Physical Security Technologies Database also be considered on a yearly basis. These yearly revisions would require redistribution of the most recent database version on CD-ROM to those utilities using the application.

APPENDIX A

PRIORITIZATION OF PHYSICAL SECURITY

PRIORITIZATION OF PHYSICAL SECURITY IMPROVEMENTS

The suggested prioritization of physical security improvements is based on the following concepts:

- **Protect critical assets first.** Critical assets are those facilities or systems that present a single point of failure (causing the entire facility or system to fail), a facility or system without which the facility or system could not exist (for example, a water system could not operate without source water; if the system had source water available, then it could not operate without treatment), or a primary concern of the utility (for example, meeting its mission and vision or protecting against a specific threat, such as the theft of copper).
- **Create layers of security, beginning from the outside of the site and moving in.** Once critical assets have been considered, continue by evaluating the perimeter of the site, the area between the perimeter and facility structures, the facility structures themselves, and then individual assets within the facility structures (ASCE/AWWA/WEF 2006).
- **Physically harden the site in each successive layer.** Physical hardening increases the levels of deterrence and delay faced by an adversary.

If needed physical security improvements have not been identified, an initial site evaluation is required. The evaluation should consider each of the following items in light of the concepts listed above:

1. Does the site have full perimeter fencing? Does the fencing have gaps under the fence line making it easy for an adversary to breach the perimeter?
2. Is the current site lighting adequate?
3. How is vehicle and pedestrian (employees, contractors, and visitors) access to the site controlled?
4. Is there a central critical asset at the site, or is it a combination of critical assets? Are the critical assets located within a building or outboard on the site?
5. If the critical asset(s) are located within a building or other structure, are the doors and windows adequate to secure the building or will additional hardening of windows, doors, hatches, etc. be required?
6. Is the site remote, or typically unmanned?
7. Is the site in an urban environment where the rights of neighbors must be respected?
8. Is there existing security infrastructure, such as a card access panel, CCTV head end equipment, or other components that can be expanded upon to enhance the existing security system?
9. What physical security measures (if any) have already been implemented?
10. What will be the response to an intrusion? Is there a guard at the site, or will response be by local law enforcement?

APPENDIX B

SITE-SPECIFIC PHYSICAL SECURITY RECOMMENDATIONS

Site-specific physical security recommendations*

Facility and critical assets	Recommendations to reduce risk
General recommendations that can be applied to most sites	
Perimeter	Fencing or walls surrounding the site. Enhanced perimeter fencing could include climb/cut-resistant fencing and a fence foundation that prevents tunneling.
	Gates with security features that correspond to the security level provided by the fence or wall.
	Access control technology used at the gate. This technology could range from key locks and card readers to intercoms and remotely operated gates to a guardhouse.
	Bollards or other vehicle barrier to limit vehicle access.
	Intrusion detection installed on fencing or wall.
	Lighting along perimeter fencing and gate.
	Hardened site openings when the opening is ≥ 96 square inches in area.
	“No Trespassing” signage every 50 feet that includes adequate language to delineate a legal boundary.
Area between perimeter and facility structures	An adequate clear zone between the perimeter and the facilities.
	Landscaping that does not obscure building or other assets, or provide a means to traverse a fence or wall.
	Basic perimeter fencing can be enhanced with a second layer of fencing or walls. The second layer can also be enhanced, if necessary, with climb/cut-resistant fencing, concrete fencing foundation, and intrusion detection.
	Gates with security features that correspond to the security level provided by the second layer of fence or wall.
	Access control technology used at the secondary gate could range from card readers to intercoms and remotely operated gates to a guardhouse.
	Motion-activated lighting.
	Bollards or other vehicle barrier around critical exterior equipment.
	Bollards or other vehicle barrier to limit vehicle access to areas within second layer of fencing.
	Locked protective barrier or cage around outdoor transformers, generators, and switchgears/motors.
	Security locks or other fasteners and intrusion detection on manholes.
	Locked access to outdoor chemical storage and feed equipment. To enhance security, include intrusion detection.

(continued)

Site-specific physical security recommendations* (continued)

Facility and critical assets	Recommendations to reduce risk
	"No Trespassing" signage every 50 feet on secondary fence or wall that includes adequate language to delineate a legal boundary.
	Minimizing signage that identifies the location of specific assets.
Facility structures	Valve operator covers – locking caps.
	Valve vault hatches – mechanically fastened or locked with shrouded lock; for enhanced protection, include double hatch doors, and intrusion detection.
	Door hinges – industrial, tamper-resistant hinges.
	Doors – key locks; enhanced security equipment can include automatic locks, status switch contacts, electronic access controls, or blast-resistant capabilities; double entry system (mantrap).
	Windows – break-resistant glass; for enhanced security, include blast-resistant glass or glass-break sensors.
	Skylights and louvers – grilles or barriers with intrusion sensors as enhanced security.
	Roofs – locked roof hatches with intrusion sensor as applicable; roof access ladder with locked shroud or intrusion alarm.
	Indoor transformers, generators, and switchgears/motors – locked protective barrier or cage.
	Interior spaces – motion detection devices.
	Chemical fill lines, storage, and feed equipment – interior, locked access; exterior, locked access with intrusion detection.
Closed circuit television (CCTV)	Facility exterior doors, hatches, and vaults – fixed cameras for alarm assessment.
	Overall site, main gates, interior – pan-tilt-zoom (PTZ) cameras for surveillance.
Power and wiring systems	Uninterruptible power supply.
	Electrical panels – locked.
	Electrical wiring – run in conduit; security wiring electronically supervised.
	Incoming site utilities – harden power, gas, water, waste, and their facility entry points.
SCADA	PLC/RTU – enclosed and locked with tamper switch on enclosure.
	Instrumentation wiring – run in conduit.

(continued)

Site-specific physical security recommendations (continued)

Facility and critical assets	Recommendations to reduce risk
Facility structures	Open basins – protective grating or screens as a shield from objects thrown from outside perimeter fence.
Wells and pumping stations (site-specific recommendations in addition to general recommendations)	
Facility structures	Aboveground well casing and airlines extending through well casing – locking cap; for enhanced security, include protective cage or enclosure around casing and air lines.
	Monitoring wells – locking cap; for enhanced security, include protective cage around well.
Water treatment plants (site-specific recommendations in addition to general recommendations)	
Perimeter	Vehicle sally port gate entrance for delivery vehicles. For enhanced security, include guardhouse and manned entrance gate.
	Provide separate visitor vehicular sign-in checkpoint.
Area between perimeter and facility structures	Public or visitor parking located as far away from the facility as practical, but at least 30 feet away.
Facility structures	Clearwell hatch/manway – hardened lock with shroud or mechanically fastened. Include double layer doors and/or intrusion detection for enhanced security.
	Gooseneck pipe clearwell vent –double screen.
	Rectangular or circular clearwell vent – double layer with shrouded lock; include intrusion alarm for enhanced security.
	Overflow outlet for clearwell – screen and/or flap valve with cage; include intrusion detection for enhanced security.
	Clearwell – intrusion detection; include remote clearwell isolation by means of an automated valve for enhanced security.
	Access ladder for clearwell – locked shroud; include intrusion detection for enhanced security.
	Visitor waiting area.
Finished water storage facilities (site-specific recommendations in addition to general recommendations)	
Area between perimeter and facility structures	Public or visitor parking located as far away from the facility as practical, but at least 30 feet away.

(continued)

Site-specific physical security recommendations (continued)

Facility and critical assets	Recommendations to reduce risk
Facility Structures	Tank hatch/manway – mechanically fastened or shrouded lock; include double layer doors and/or intrusion detection for enhanced security.
	Gooseneck pipe clearwell vent –double screen.
	Rectangular or circular clearwell vent – single layer with shrouded lock; include double layer and an intrusion alarm for enhanced security.
	Overflow outlet – screen and/or flap valve with cage; include intrusion detection for enhanced security.
	Intrusion detection on top of tank.
	Access ladder – locked shroud with intrusion alarm for enhanced security.
	Reservoir – remote isolation using an automated valve.
Distribution systems (site-specific recommendations in addition to general recommendations)	
System structures	Exposed pipelines - fencing with intrusion detection for enhanced security.
	Control, pressure-reducing, air-relief, and other valves – locking covers with intrusion detection for enhanced security.
	Sampling stations - locking covers with intrusion detection for enhanced security.
	Hydrants – locking mechanisms.
	Contractors' temporary connections – locking devices.
	Residential customers - uni-directional meters (to reduce backflow potential).
	Multi-family residential connections and commercial facilities (such as motels) – backflow prevention valves or tamper switches.
	Interconnections to neighboring water systems, wholesale customers, or industrial facilities – backflow prevention valves.
Water system support facilities (site-specific recommendations in addition to general recommendations)	
Perimeter	Number of vehicle access points and entrance gates minimized.
	Vehicle sally port gate for delivery vehicles; guardhouse and manned entrance gate for enhanced security.
	Separate visitor vehicular sign-in checkpoint.

(continued)

Site-specific physical security recommendations (continued)

Facility and critical assets	Recommendations to reduce risk
Area between perimeter and facility structures	Public or visitor parking located as far away from the facility as practical, but at least 30 feet away.
	No parking underneath facilities.
	Fuel storage tanks located at least 100 feet from all buildings and away from perimeter fence lines.
Facility structures	Visitor waiting area.
	Dedicated meeting room outside secured building interior for meetings with visitors and vendors.
	Unobstructed views of people approaching controlled areas or critical assets.
	Windows located away from doors to prevent intruders from unlocking doors through the windows.
Wastewater treatment plants (site-specific recommendations in addition to general recommendations)	
Perimeter	Vehicle sally port gate entrance for delivery vehicles. For enhanced security, include guardhouse and manned entrance gate.
	Provide separate visitor vehicular sign-in checkpoint.
Area between perimeter and facility structures	Public or visitor parking located as far away from the facility as practical, but at least 30 feet away.
Facility structures	Visitor waiting area.
Collection Systems (site-specific recommendations in addition to general recommendations)	
System structures	Exposed pipelines and forcemains – fencing; for enhanced security, buried or installed in hardened carrier pipes with vibration/motion detection as indicated by threat.
	Control, pressure-reducing, air-relief, and other valves – locking covers with intrusion detection for enhanced security.
	Manhole covers – pan-type locks; for enhanced security, bolt-type locks or tack-welds and motion detection.
	Existing catch basins, curb inlets, and pipe inlets and outlets – bar screens or horizontal bars.

(continued)

Site-specific physical security recommendations (continued)

Facility and critical assets	Recommendations to reduce risk
	New catch basins, curb inlets, and pipe inlets and outlets – bolt-type locking devices; welded screens and horizontal bars with motion detection. Deep tunnels – hardened key-locked accessways; for enhanced security, electronic access controls, motion detection, intrusion alarms and/or thermal imaging devices.
Wastewater/stormwater system support facilities (site-specific recommendations in addition to general recommendations)	
Perimeter	Number of vehicle access points and entrance gates minimized. Vehicle sally port gate for delivery vehicles; guardhouse and manned entrance gate for enhanced security. Separate visitor vehicular sign-in checkpoint.
Area between perimeter and facility structures	Public or visitor parking located as far away from the facility as practical, but at least 30 feet away. No parking underneath facilities. Fuel storage tanks located at least 100 feet from all buildings and away from perimeter fence lines.
Facility structures	Visitor waiting area. Dedicated meeting room outside secured building interior for meetings with visitors and vendors. Unobstructed views of people approaching controlled areas or critical assets. Windows located away from doors to prevent intruders from unlocking doors through the windows.

[*] The contents of this table have been drawn from the American Society of Civil Engineers (ASCE)/American Water Works Association (AWWA)/Water Environment Federation (WEF). 2006. Guidelines for the Physical Security of Water Utilities. Reston, VA. December.

APPENDIX C

INTERVIEW SURVEY FORM

ID # _________

CH2M HILL Physical Security Technologies Questionnaire

FACILITIES REVIEW

1. Which of the following kinds of facilities/sites/systems does your utility own or operate? (Please "X" all that apply)

Source water reservoirs and intakes .... ___
Groundwater wells .... ___
Source water transmission pipelines.. ___
Water treatment plants.. ___
Pump stations (raw or treated water).. ___
Finished water storage.. ___
Valves, hydrants, vaults, and meters .... ___
Turnouts/interconnects with other agencies .... ___
Support facilities (offices, maintenance facilities, labs, etc.)................................... ___
Collection systems.. ___
Lift stations... ___
Wastewater treatment plants... ___
Outfall pipes .... ___

PHYSICAL SECURITY EQUIPMENT

2. Please indicate below the kinds of security equipment that your utility uses. *(Please "X" all that apply)*

	Source-water reservoirs and intakes	Ground-water wells	Source-water trans-mission pipelines	Water treatment plants	Pump stations (raw or treated water)	Finished water storage	Valves, hydrants, vaults, and meters	Turnouts/ inter-connects with other agencies	Support Facilities	Collec-tion systems	Lift stations	Waste-water treatment plants	Outfall pipes
Card readers													
Biometric devices													
Key-code pads (electronic or manual)													
Mechanical keys													
Security lighting													
Surveillance cameras													
Fence or gate sensors/alarms													
Window or door sensors/alarms													
Hatch sensors/alarms													

(continued)

2. (continued) Please indicate below the kinds of security equipment that your utility uses. *(Please "X" all that apply)*

	Source-water reser-voirs and intakes	Ground-water wells	Source-water trans-mission pipelines	Water treatment plants	Pump stations (raw or treated water)	Finished water storage	Valves, hydrants, vaults, and meters	Turnouts/ inter-connects with other agencies	Support Facilities	Collec-tion systems	Lift stations	Waste-water treatment plants	Outfall pipes
Buried cable systems													
Water monitoring systems for contaminants													
Vehicle barriers (jersey barriers, cables, bollards, etc.)													
Security doors													
Equipment cages													
Security locks (mechanical and others)													
Ladder cages													
Smoke or foam obscurement systems													
Hardening or partitioning areas within areas (layering)													
Guards or other security monitoring personnel													
Other types of physical security equipment (to restrict gate access, control visitors, detect intruders, etc.) *(please describe below*)*													

*Description of other types of physical security equipment:

Please feel free to use as much space as necessary to answer the following questions:

3. If you have had problems or difficulties with any of your security equipment, please describe the type(s) of facilities at which the problem occurred, the nature of the problem, and what (if anything) has been or will be done to address the problem.

4. If you were selecting and installing security equipment in your facilities now, how would it be different from what you currently use, in terms of the type of equipment you would use, the amount you would spend, placement of devices, the support hardware and software you would use, and so on? Please provide as much detail as possible.

5. Of your installed security equipment, which is particularly effective and where, if relevant, is it installed? Please describe.

6. What suggestions, if any, would you make to utilities that are selecting/installing/operating security equipment?

7. Taken together, how effective would you say your utility's physical security equipment is currently? *(Please "X" one response)*

Not at all Effective	Somewhat Effective	Quite Effective	Extremely Effective
___	___	___	___

8. Do you have any improvements or changes planned in your physical security equipment? If yes, please describe the improvements and the types of facilities at which the improvements will be made.

9. Do you maintain and monitor your security equipment with internal personnel, with contracted support personnel, or with both internal and contracted personnel? (Please "X" one response)

Internal personnel only.. ___

Contracted personnel only.. ___

Both internal and contracted personnel .... ___

10. Has the public expressed any concerns regarding your utility's physical security equipment? If so, please describe.

COMMUNICATION SYSTEMS

11. Which of the following kinds of communication systems do you use to support your security equipment? *(Please "X" all that apply)*

Hard-wire	Fiber optics	Microwave (wireless)	Radio (wireless)	Dial-up telephone modem	DSL, T1, or other network broadband connection	SCADA
___	___	___	___	___	___	

12. Are the security-systems communications encrypted to protect the signals from outsiders? *(Please "X" one response)*

Yes, all are ___   Yes, some are ___   No, none are ___   Have no idea ___

13. Do you have any concerns regarding the security of the communication systems your utility currently uses? If yes, please describe.

SECURITY EQUIPMENT COSTS AND BUDGETS

14. About how much has your utility spent since 2001 on physical security equipment?

15. Does your utility have a separate annual budget for physical security equipment?

16. What percentage of your utility's total annual operating budget is devoted to security equipment? (If uncertain, is it less than 1%? Between 1% and 5%? Between 6 and 10%? Between 11 and 15%? More than 15%?)

THANK YOU VERY MUCH FOR YOUR PARTICIPATION IN THIS SURVEY.

Please return this completed questionnaire to
Barbara Heydorn
SRI Consulting Business Intelligence, 333 Ravenswood Avenue, Menlo Park, CA 94025
Phone: 650-859-5717

APPENDIX D

INTERVIEW SURVEY

SUMMARY OF RAW DATA

CH2M HILL
PHYSICAL SECURITY TECHNOLOGIES QUESTIONNAIRE

Number of respondents (n) = 43
Unless otherwise indicated, the number of respondents to each question is 43.
Information is provided in the following format: number of respondents/% of total respondents

FACILITIES REVIEW (Facilities as % of Total Respondents)

1. **Which of the following kinds of facilities/sites/systems does your utility own or operate?** ***(Please "X" all that apply)***

Source water reservoirs and intakes	27/63%
Groundwater wells	24/56%
Source water transmission pipelines	34/79%
Water treatment plants	37/86%
Pump stations (raw or treated water)	39/91%
Finished water storage	40/93%
Valves, hydrants, vaults, and meters	43/100%
Turnouts/interconnects with other agencies	32/74%
Support facilities (offices, maintenance facilities, labs, etc.)	43/100%
Collection systems	25/58%
Lift stations	26/60%
Wastewater treatment plants	21/49%
Outfall pipes	18/42%

PHYSICAL SECURITY EQUIPMENT

2. **Please indicate below the kinds of security equipment that your utility uses.** ***(Please "X" all that apply)***

	Sourcewater reservoirs and intakes		Groundwater wells		Sourcewater transmission pipelines		Water treatment plants		Pump stations (raw or treated water)		Finished water storage		Valves, hydrants, vaults, and meters		Turnouts/ inter-connects with other agencies		Support Facilities		Collection systems		Lift stations		Waste-water treatment plants		Outfall pipes	
PHYSICAL SECURITY TECHNOLOGY	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities	total # of facilities	% of facilities
Card readers	8	30%	3	14%	0	0%	25	69%	10	28%	12	32%	2	5%	2	7%	27	69%	1	4%	1	4%	9	47%	1	6%
Biometric devices	0	0%	0	0%	0	0%	1	3%	0	0%	0	0%	0	0%	0	0%	1	3%	0	0%	0	0%	0	0%	0	0%
Key-code pads	2	7%	2	9%	0	0%	16	44%	9	25%	7	19%	0	0%	1	3%	13	33%	0	0%	0	0%	4	21%	0	0%
Mechanical keys	23	85%	19	86%	12	36%	31	86%	31	86%	29	78%	21	54%	15	50%	30	77%	8	35%	18	78%	14	74%	6	35%
Security Lighting	20	74%	15	68%	7	21%	35	97%	31	86%	28	76%	5	13%	5	17%	35	90%	3	13%	16	70%	18	95%	2	12%
Surveil Cameras	17	63%	7	32%	4	12%	29	81%	19	53%	20	54%	0	0%	2	7%	21	54%	1	4%	1	4%	8	42%	0	0%
Fence/Gate S/A	6	22%	5	23%	3	9%	18	50%	12	33%	9	24%	1	3%	2	7%	11	28%	2	9%	3	13%	3	16%	0	0%
Window/ Door S/A	11	41%	7	32%	1	3%	27	75%	21	58%	12	32%	0	0%	3	10%	25	64%	1	4%	4	17%	5	26%	0	0%
Hatch S/A	9	33%	3	14%	3	9%	13	36%	10	28%	16	43%	4	10%	4	13%	3	8%	0	0%	5	22%	3	16%	0	0%
Burried Cable Sys	2	7%	2	9%	2	6%	8	22%	3	8%	5	14%	1	3%	3	10%	5	13%	0	0%	4	17%	4	21%	0	0%
Water Monitor for Contaminants	5	19%	1	5%	3	9%	15	42%	12	33%	10	27%	3	8%	3	10%	2	5%	3	13%	2	9%	3	16%	1	6%
Vehicle Barriers	8	30%	1	5%	3	9%	14	39%	6	17%	6	16%	2	5%	1	3%	7	18%	1	4%	3	13%	5	26%	0	0%
Security Doors	10	37%	9	41%	4	12%	22	61%	21	58%	15	41%	2	5%	1	3%	18	46%	3	13%	9	39%	9	47%	1	6%
Equipment Cages	3	11%	2	9%	1	3%	11	31%	5	14%	5	14%	1	3%	2	7%	10	26%	1	4%	2	9%	3	16%	1	6%
Security Locks (Mech & Other)	19	70%	12	55%	10	30%	25	69%	23	64%	27	73%	13	33%	13	43%	23	59%	4	17%	13	57%	12	63%	3	18%
Ladder Cage	4	15%	1	5%	2	6%	7	19%	8	22%	26	70%	2	5%	2	7%	2	5%	1	4%	1	4%	4	21%	1	6%
Smoke/ Foam Obscurement Sys	1	4%	1	5%	1	3%	2	6%	2	6%	1	3%	1	3%	1	3%	3	8%	1	4%	2	9%	2	11%	1	6%
Hardening Partitioning Areas w/in Areas (Layers)	5	19%	2	9%	1	3%	13	36%	8	22%	7	19%	1	3%	0	0%	4	10%	1	4%	2	9%	5	26%	0	0%
Guards or Other Monitoring Personnel	8	30%	5	23%	3	9%	16	44%	9	25%	7	19%	3	8%	4	13%	11	28%	2	9%	3	13%	8	42%	1	6%
Other Types of Physical Security Equip	5	19%	2	9%	2	6%	10	28%	5	14%	5	14%	1	3%	1	3%	2	5%	2	9%	3	13%	7	37%	2	12%

Other types of security equipment are described in the Summary spreadsheet. The following list reflects a broad classification of the types of responses and the number of times each type of equipment was mentioned (in parentheses).

- Burying manhole covers or tack welding covers closed (1)
- Buzzers to gain entrance at unspecified locations (1)
- Cameras: thermal imaging (1), IR (1)
- Concrete dig – under barrier walls with fencing <concrete barrier directly beneath the fence> (1)
- Digital Motion Tracking (1)
- Electronic key (Cyberlock) to create audit of use and permission levels (1)
- Fence perimeter detection system (1)
- Fencing (2)
- Gates and/or gate entrance procedures, including buzzing and intercom systems (6)
- Intercom systems to gain entrance at unspecified locations (1)
- Intelligent Video Motion Detection System (1)
- Key fobs (similar to a card reader, but in the form of a key fob) at the pump stations and turnouts/interconnects (1)
- Landscaping (rock) that is decorative and prevents vehicle access (1)
- Radio communication (1)
- Sensors: Glass breakage and infrared motion sensors integrated into the interior surveillance camera system in the water treatment plant (1), Microwave Area Motion Sensors (1), motion sensors on water storage tanks and raw water intakes (1), pavement sensors at the water and wastewater treatment plants to detect when someone is there (1), sensor phone/motion detection system at a remote pumping station (1)
- “Vista Scape” intelligent video management system (1)
- Visitor procedures, including escorting contractors and badging (2)

3. **If you have had problems or difficulties with any of your security equipment, please describe the type(s) of facilities at which the problem occurred, the nature of the problem, and what (if anything) has been or will be done to address the problem.**

The Summary spreadsheet contains a complete description of each respondent’s answer. The following lists reflect SRIC-BI’s broad classification of the types of responses and the number of times each type of problem was mentioned (in parentheses). Each item appears on only one list.

Most problems reported by the respondents were associated with false alarms associated with intrusion detection systems and CCTV systems, including the cameras, recording devices, and software.

Total number that did not report problems: 9/21% (4 blank, 4 no problems, 1 “not many” problems)

Total number that described problems: 34/79% (most respondents reported multiple problems)

Typical equipment failures and solutions cited, organized by type of equipment (number of utilities citing similar problems):

- Access cards: chip on access card failed, reissued access card (1)
- Alarms: unreliable alarm/alert system, corrected by vendor with updated software (1)
- Badges: badge failed, reissued badge (1)
- Bollards: hydraulic bollards that are part of electronic gate access system failed in inclement weather, fixed (1)
- Cameras: various bugs, corrected by vendors (2), does not perform as promised by vendor (2), frequent failure (1), cameras not actively monitored (2), images take up too much bandwidth, one utility will solve with data compression (2), inconvenient to retrieve images at remote site, solved with web-enabled camera that sends data by phone line (1), tape back-up doesn't store enough information and needs to be turned over manually, will go to DVD system (1), regular cameras require appropriate lighting but still may not work in bad weather, IR cameras may work under more conditions but are expensive (1), cameras require lighting but the neighborhood doesn't like the lights (1), thermal imaging cameras expensive to maintain, will go to infra-red cameras with <emitters> (1), lens is fogged easily by humidity, insects, or freezing and requires regular maintenance, may replace camera and specify anti-fog lens (1), spiders attracted to light spin webs and obstruct view or cause data transmission problems (1), CCTV equipment outmoded, will replace (1)
- Card readers: tamper tabs needed adjustment, adjusted (1), placing system on LAN created problems, solved by upgraded LAN but ideally security should have its own LAN (1)
- CyberKey: early generation problematic, installed next generation (1)
- Guards: inadequate performance, solved with more active supervision (2)
- Fire alarms: activated by dust, replaced with heat sensitive sensors (1)
- Gates: open gates, asked tenant to close gate (1), open gates, replaced gate actuators (1), need frequent repair (1), actuator not designed to accommodate as much opening and closing of heavy crash barrier gate arm as needed, may install bollards instead (1), stay open or won't open as a result of data transmission problems, corrected by vendor (1), from Q4, gate's laser sensor can easily be tricked into staying open since it is designed not to close on people or vehicles (1)
- Keys: From Q5, lost keys (1)
- Keypads: various bugs, corrected by vendors (1)
- Mechanical locks: lost keys, will install electronic locks (1)
- Radios: fail from time to time, fixed when they fail (1)
- Switches: Failed intrusion switches and cameras, replaced (1), mechanical limit switches out of adjustment, replaced with magnetic switches (1)
- Communications: Unable to rely on high speed data transmission from remote locations, use alternative communication devices (1)

Typical equipment failures, organized by cause of failure (number of utilities citing similar problems):

- Electrical storms: electrical storms can knock access control readers, cameras and fire alarms; solved with surge protectors or uninterruptible power supplies at some utilities (3)
- False alarms: motion activated fence alarm activated by animals, will address by adding camera (1), fence alarm system has too many false alarms (2), motion activated camera set off by animals (1), vibration alarms on windows triggered by harmonically induced vibrations from pump motors or birds, vibration problem solved after identified (1), video motion detection systems susceptible to false image alarms triggered by a variety of environmental conditions including clouds, overgrown landscape, one utility hopes to solve with software upgrade (2), IR systems subject to temperature changes, weather, rain and yield too many false alarms (1), door sensors require properly adjusted doors, solved with adjustments and costly replacements (1), hotwire detection system too sensitive so rainstorms activated the alarm, fixed with adjustments (1)
- Lack of training (2)
- Maintaining legacy systems when parts become difficult to find (1)
- System integration: inadequate integration between older computer systems and software for newer video camera system (1), cost of integrating new security equipment with existing SCADA high and unexpected, solved by requiring vendors to coordinate proposals with information security department (1)
- Quality standards inadequate for excluding vendors that supply substandard equipment (1)
- Theft and vandalism: holes cut in fences, solved with increased guard patrols (1), lights stolen, solved with tamper resistant screws (1)
- Unreliable phone lines (1)

4. **If you were selecting and installing security equipment in your facilities now, how would it be different from what you currently use, in terms of the type of equipment you would use, the amount you would spend, placement of devices, the support hardware and software you would use, and so on? Please provide as much detail as possible.**

The Summary spreadsheet contains a complete description of each respondent’s answer. The following lists reflect SRIC-BI’s broad classification of the types of responses and the number of times each type of problem was mentioned (in parentheses). Each answer appears in only one list. Two utilities did not report (one “NA”; one blank).

Quick tips and specific items that utilities recommend or intend to install (number of utilities suggesting the equipment):

- Add equipment or replace existing equipment with newer models: cameras (4), reliable card readers (3), closed circuit television/CCTV (1), newer model DR for CCTV equipment (1), gas monitoring system (1), keypads (1), lighting (2), motion sensors/detectors (4)
- Better cameras or camera use: system to record and file images for a defined period of time (1), cameras that recognize people (1), IP cameras (3), instead of DVR get NVR (1), higher quality cameras with features including panning, wide angle, zoom, sound recording, color, broadcasting recorded messages, anti-fog lenses (6), cameras that can send messages by e-mail, text message, pager or phone to appropriate staff (2), infra-red/IR for night viewing
- Camera/alarm interface issues: Add camera monitors to motion-triggered alarms (1), alarms should alert security to significant camera images (1) , snapshot cameras to coincide with intrusion detection sensors/alarms (1)
- Camera image storage: motion sensing cameras that record in response to events and can distinguish between animals and real intruders (5), 15 frames per second video is enough, 30 frames per second takes too much storage space (1), cameras that stay fixed when an incident is detected and filmed (3)
- Central monitoring station (1)
- Communications systems: web-browser based cameras so you don't need SCADA; systems should run off existing phone lines (1), security cameras integrated with SCADA (1), wireless cameras instead of hard-wired cameras (1), LAN communications (1)
- Fences: Smart fence sensors (2), sensors/motion detectors combined with cameras to detect if fence is being cut (3), high-grade iron fences instead of chain link (2)
- Gates: High-quality gate actuators (1)
- Hatch alarms with SCADA or other link to 911 emergency response (1)
- Layered access control (1)
- Locks and Keys: CyberKey, to document all events (2), smart locks that can be programmed (1), electronic locks (1)
- Motion detectors and alarms near metal skinned buildings since steel siding is easy to cut (1)
- Physical hardening of doors, hatches, and windows (1)
- Side gates with locks near sliding gates so plant operators can get in if the gate fails
- Software that eliminates environmentally-caused false alarms (1)

Approaches to security (number of utilities suggesting the approach):

- Active security at entrances, actively monitor security cameras (1)
- Begin by securing the entire perimeter with a reliable fence detection system, to include CCTV and lighting to enhance security response. Provide secure/protective storage facilities for hazmat (chlorine, etc.) followed by vehicle gate access control. (1)
- Begin with a security audit (1)
- Fund projects with state security enhancement fund (1)
- Guards: reduce reliance on guards when possible (1)

- Increased digital video recorder/DVR use (2)
- Include security as part of initial plant design whenever possible (1)
- Place systems on plant SCADA system (1)
- Protect critical equipment with cameras, sensors, alarms (1)
- Security systems require ongoing improvements; the system should not be static (2)
- Simple improvements are best, such as doors and windows that close properly (1)
- Software: Use robust and flexible software, durable hardware (1), be sure operational software and security software work together (1)
- Use common equipment from a common vendor to keep things easy to use and operate (1)
- Use intelligent systems and/or multiple systems to ensure that existing systems work properly (for example, a way to check if a gate is opening and closing for cars or if it is propped open; monitoring exits as well as entrances) (1)
- Implement a “virtual security network”

Things utilities say they would have done differently (number of utilities):

- Buried cable system <buried line sensor designed to detect disturbances both on the surface of and beneath the ground> was expensive and utility isn’t convinced it gets much value from it (1)
- Hard-wire the alarm system; the utility installed a wireless system to reduce cost but would recommend a hard-wired system to improve reliability (1)
- Pay more attention to who installs the systems, use people with experience installing security systems (1)
- Separate the interior of the water treatment plant into zones so operators don’t trigger alarms for the whole plant when they go on patrol. If the plant is zoned, then the operators can go patrol in one zone, and not disturb the alarm for the other zone. This way they can separate the false alarm and the true issues more easily.
- Use video motion detection.

5. **Of your installed security equipment, which is particularly effective and where, if relevant, is it installed? Please describe.**

The Summary spreadsheet contains a complete description of each respondent’s answer. The following lists reflect SRIC-BI’s broad classification of the types of responses and the number of times each type of problem was mentioned (in parentheses). Four utilities left this question blank.

- Access control systems: Access control systems (3), access card readers (9), combination of fences, gates, barriers, card readers, and hatch alarms for access control (1)
- Alarms: Door alarms/building intrusion alarms (7), fence alarms (1), gate alarms (1), hatch alarms (3), Cameras fixed on all outside hatches; the system will alarm for movement (1), window alarms (1)
- Barriers (1)
- Cameras/video equipment; one utility uses them for both security and process control (15)
- Doors or Locks: Astragals (1), city locks and city tumble locks (1), dead bolts (1), CyberKey system (1), Keyso lock system (1), mechanical locks (1)

- Expanded metal cages on reservoir vents (1)
- Gates: Double entrance gates with separate gates for arrival and departure (1), card-controlled gates (1), sliding gates at vehicle entrances (1)
- Fencing: fencing (6), hotwire fencing (1), at facility perimeter
- Lighting (3), at all facilities
- Motion detectors (1)
- Products utilizing LAN for communication (1)
- Radios for security staff (1)
- Staff: Guards/security staff (3), mind-set of personnel changed to recognize importance of security (1), gate house (1)

6. **What suggestions, if any, would you make to utilities that are selecting/ installing/operating security equipment?**

The Summary spreadsheet contains a complete description of each respondent's answer. The following lists reflect SRIC-BI's broad classification of the types of responses and the number of times each type of problem was mentioned (in parentheses). Two utilities left this question blank.

- Access: access control is important (1), use active security at entrances (1)
- Cameras: feature that has cameras selects view based on which doors are open is helpful (1), use cameras that don't use too much bandwidth (1), plan for monitoring costs if using cameras (2)
- Design: Design facilities with security in mind (3) use security experts not civil engineers (2), use a long-term frame of mind (1), select equipment with future expansions in mind (1), identify the most probable risks and secure to that level (1), be sure you know what you intend to accomplish before investing in a system (6), think like a criminal when designing systems, keep things locked up (1), use web-based systems, digital systems (1), use layering, simple systems are often an effective initial layer, add complexity as needed (1), prepare for internal threats, such as disgruntled employees, as well as outside threats, such as terrorists (1), use integrated systems for maximum effectiveness (1), consider your utility's culture when picking out systems (2), use industry guidelines (2)
- Effective equipment: cameras (3), card readers (1), fences (2), intruder alarms/motion detectors (1), sensors on fences, gates (1)
- Equipment purchasing: use quality, compatible equipment, preferably non-proprietary equipment (3), use proven technologies (1), specify equipment carefully, especially if you need to buy based on the lowest bid (1), shop around (2), talk to other utilities and/or visit to see what works (7),
- Funding: get grants/outside funds when you can (1)
- Keep systems simple to understand and use (1)
- Installation: Be sure installer is competent and experienced (2), secure surety bonding with contractors (1)
- Investigate unauthorized access, alarms (1)
- Maintenance: plan for maintenance costs/don't buy equipment you can't maintain (3)
- Pilot systems for false positives and maintenance (1)

- Policies: develop policies for approving access (1), consider an emergency response plan for extreme situations that seem unlikely (1), establish a routine inspection procedure to ensure all security equipment and systems are functioning properly (1), develop a good public relations policy to inform rate payers of efforts to secure assets (1)
- Redundancies: build redundancies into your system (2)
- Security audit: get a complete security audit/risk assessment (4)
- Software House is the best (1)
- Staff: educate staff on why security is needed (2), develop a proprietary patrol operation (1), supervise guard staff (1), have trained in-house staff to filter false alarms, trouble shoot (2), perform background checks on personnel (1), hire experienced and trusted security personnel and guard companies (1), provide regular security training to personnel (1)
- Vendors: use competent vendors (3), create a strategic alliance with your vendor (1), try to use a minimum number of trusted vendors when purchasing equipment (1), for support and installation, make sure the vendors are well established, local, and provide 24x7 support (1)

7. Taken together, how effective would you say your utility's physical security equipment is currently? (Please "X" one response)

Not at all Effective	Somewhat Effective	Quite Effective	Extremely Effective
1/2%	19/44%	22/51%	1/2%

8. Do you have any improvements or changes planned in your physical security equipment? If yes, please describe the improvements and the types of facilities at which the improvements will be made.

No: 6/14% (5 utilities stated that they did not have plans; 1 utility left the answer blank)
Yes: 37/86%

The Summary spreadsheet contains a complete description of each respondent's answer. The following lists reflect SRIC-BI's broad classification of the types of responses and the number of times each type of answer was mentioned (in parentheses).

- Access control: access control (3), layered access control (2), at remote sites (1)
- Alarms: alarms on access doors (1), plant perimeter alarms (1), intrusion alarms (2), 24/7 alarm monitoring, fence alarms (1)
- Cameras: Cameras, CCTV, video/video management (25), IR camera (1), at remote sites (1)
- Cameras and lighting (2)
- Card readers (4)
- Central monitoring station (1)
- Chemical replacement: eliminate chlorine and generate hypochlorite on site (1), gas chemicals replaced with UV system (1)
- Fencing: fencing (8), cable fence barrier (1), cabling within the fences at remote sites (1), hotwire fencing (1), anti-climb fencing (1), enhanced fence foundation (1)
- Fence sensors (1)
- Fire suppression (1)

- Gas monitoring system (1)
- Gates (2)
- Hardening: hardening doors, hatches, or windows (2), access hardening (1)
- Internal controls (1)
- Lighting (3)
- Locks: electronic locks (2), CyberKey (1), locks on manhole covers
- Maintenance: develop and improve upon existing security maintenance issues (1)
- Motion detection (2)
- Network security (1), SCADA enhancements (4)
- Secure storage for hazmat (1)
- Security system package (1)
- Sensors: sensors (2), fence (perimeter) detection, hatch sensors/alarms (3)
- Shielding to isolate staff from storage tank (1)
- Signage (1)
- Software (2)
- Vehicle barriers (2)
- Water monitoring for contaminants or water contamination alarms (4)

9. Do you maintain and monitor your security equipment with internal personnel, with contracted support personnel, or with both internal and contracted personnel? (Please "X" one response)

Internal personnel only	10/23%
Contracted personnel only	1/2%
Both internal and contracted personnel	32/74%

10. Has the public expressed any concerns regarding your utility's physical security equipment? If so, please describe.

No: 35/81% (2 utilities left this blank but SRIC-BI counted these responses as "No"; 25 utilities responded with "No," "None," "Not much at all," or Not that we know of" "Not really," or "Nothing really important." The remaining six utilities responded with phrases SRIC-BI interpreted as "No.")

Yes: 8/19%

SRIC-BI treated general inquiries from the public regarding security as "No" responses. SRIC-BI also treated concerns that were quickly addressed with information as "No" responses. SRIC-BI only considered concerns expressed by the public; two utilities reported that their employees had concerns ("Some employees have felt resentful in the belief that security systems are there to monitor their work rather than security threats." And "No – just some employees that resent the intrusions to their freedom."), but these responses were also counted as "No."

Utilities reported public concerns in the areas of cameras, fencing, and lighting:

- Cameras: Some are suspicious of cameras (1)
- Fences: Unspecified dislikes (2), dislike concertina "razor" wire (1), dislike having access cut off (2), dislike appearance (1)
- Light: Dislike stray light or too much light (2)

COMMUNICATION SYSTEMS

11. Which of the following kinds of communication systems do you use to support your security equipment? (Please "X" all that apply)

Hard-wire	Fiber optics	Microwave (wireless)	Radio (wireless)	Dial-up telephone modem	DSL, T1, or other network broadband connection	SCADA
37/86%	31/72%	16/37%	33/77%	20/47%	22/51%	33/77%

12. Are the security-systems communications encrypted to protect the signals from outsiders? (Please "X" one response)

Yes, all are	Yes, some are	No, none are	Have no idea
15/35%	13/30%	8/19%	7/16%

13. Do you have any concerns regarding the security of the communication systems your utility currently uses? If yes, please describe.

No: 29/69% (three blank, 25 "No" or other negative responses)

Yes: 13/31%

Areas of concern:

- Bandwidth
- Easily disabled
- Encryption: Some older equipment might not have the same level of encryptions as newer ones
- Encryption: Is the information encrypted? If not, why not?
- Hacking: Outside intrusion (hacking) and internal/threats to the system
- Hacking: Potential damage or hacking at transponder box
- Reliability: Reliability of the communication equipment, and how secure the encryption is.
- Reliability: unreliability of hard-wired systems and fiber optics
- The possibility of false information being sent could cause problems but they should not be able to directly control things from outside the facility.
- The system can fail, which is a concern.
- We have examined encrypted 900 MHz with little success
- Wireless communications are somewhat dependent on weather conditions and interference from either natural or man-made obstacles. Network broadband communications are typically managed by third parties and utilities depend on their reliability to maintain and support their equipment. Cost is also a concern for broadband communications.
- Wireless would be the largest concern – still a newer technology!

SECURITY EQUIPMENT COSTS AND BUDGETS

14. About how much has your utility spent since 2001 on physical security equipment?

One utility did not respond to this question.

Minimum spent: less than $1000

Maximum spent: $10,000,000

Majority of respondents spent in the range of $100,000 to $10,000,000.

Results are compiled in two ways; (1) categorized into ranges of dollars spent since 2001 and (2) all responses listed in ascending order. Results are reported as thousands of dollars.

< $1	**>$1 and <$100**	**>$100 and <$1,000**	**>$1,000 and <$10,000**	**>$10,000 and <$50,000**	**>$50,000**
1/2%	4/10%	18/43%	15/36%	3/7%	1/2%

< $1
$5
$30
$50
$85
$100
$120
$150
$170
$200
$200
$240
$250
$300
$350
$350
$400
$400
$450
$500
$500
$500
$750
$1,000
$1,000
$1,400
$1,500
$1,500
$1,500
$1,500
$1,800
$2,000
$2,268
$3,000
$5,000
$6,700
$7,200
$9,000
$11,200
$13,000
$30,000
$50,000

15. Does your utility have a separate annual budget for physical security equipment?

No: 25/58%

Yes: 18/42%

16. What percentage of your utility's total annual operating budget is devoted to security equipment? (If uncertain, is it less than 1%? Between 1% and 5%? Between 6 and 10%? Between 11 and 15%? More than 15%?)

Two utilities reported the percentage of the utility's capital budget that is devoted to security equipment.

<1%	23/53%
1-5%	16/37%
6-10%	1/2%
11-15%	1/2%
>15%	1/2%
No response	1/2%

SURVEY COVER LETTER

A CH2M HILL representative contacted your organization in the past month to invite you to participate in a survey to collect information on security technologies that your utility uses, their effectiveness, and features that could be improved. The survey also collects information on the amount spent and budgeted annually to address physical security concerns. SRI Consulting Business Intelligence is working with CH2M HILL and the project sponsors—the American Water Works Association Research Foundation (AwwaRF), the Water Environment Research Foundation (WERF), and the United Kingdom Drinking Water Inspectorate—to collect this information. Your participation is essential to making the physical security technologies application guidelines that will come out of this project relevant and useful to the industry.

A copy of the questionnaire is attached. We anticipate that it will take about 30 minutes to complete. You are welcome to fill it out on your own and return it to me. Alternatively, you may wait for one of SRIC-BI's interviewers (John Bomben, Barbara Heydorn, and Franklyn Wu) to contact you within the next five days to schedule a time to conduct the survey by phone. If you wish to complete the questionnaire yourself, please return a hardcopy version of the completed Word document to me at the following address (due to the sensitivity of the information, we prefer not to use e-mail to collect your data):

Barbara Heydorn
SRI Consulting Business Intelligence
333 Ravenswood Ave.
Menlo Park, CA 94025
Phone: 650 859 5717

Your answers will be incorporated into a summary document designed to provide the utility industry with useful information on real-world security experiences. In the summary document, no information will be attributed to your organization directly; instead, your information will summarized with the information from all of the other participating utilities. We understand the importance of maintaining your organization's confidentiality and respecting your security concerns. Access to the individual surveys will be limited to project team members at SRIC-BI and CH2M HILL.

If you have any questions regarding this AwwaRF-sponsored project, please contact Frank Blaha, AwwaRF Project Manager (303.347.6244 or fblaha@awwarf.org) or Ken Thompson, CH2M HILL Principal Investigator (720.286.5407 or ken.thompson@CH2M.com).

REFERENCES

American National Standards Institute (ANSI). 2007. eStandards Store. http://webstore.ansi.org/ansidocstore/default.asp

American National Standards Institute (ANSI)/National Association of Architectural Metal Manufacturers (NAAMM) Hollow Metal Manufacturers Association (HMMA). 2003. 862-03, Guide Specifications for Commercial Security Hollow Metal Doors and Frames. Chicago, IL. http://www.naamm.org/hmma/pdfs/HMMA862-03.pdf

American Society of Civil Engineers (ASCE)/American Water Works Association (AWWA)/Water Environment Federation (WEF). 2006a. *Guidelines for the Physical Security of Wastewater/Stormwater Utilities.* Reston, VA. December.

American Society of Civil Engineers (ASCE)/American Water Works Association (AWWA)/Water Environment Federation (WEF). 2006b. *Guidelines for the Physical Security of Water Utilities.* Reston, VA. December.

American Society of Industrial Security (ASIS). 2004. Protection of Assets. Alexandria, VA. http://www.protectionofassets.com/

American Society of Sanitary Engineers (ASSE). 1996. ASSE Standard #1060-2006 Performance Requirements for Outdoor Enclosures for Fluid Conveying Components. http://www.asse-plumbing.org/Stds%20Prog%20Info/Stds%20Desc.html#1060

American Water Works Association (AWWA). 2004. *Interim Voluntary Security Guidance for Water Utilities.* Denver, CO. www.awwa.org/science/wise/

ASTM International. 2003. *F 1910, Standard Specification for Long Barbed Tape Obstacles.* http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874

ASTM International. 2004a. A 121, Standard Specification For Metallic-Coated Carbon Steel Barbed Wire. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/A.htm?L+mystore+qkng6334+1140140874

ASTM International. 2004b. A 176, Standard Specification for Stainless and Heat-Resisting Chromium Steel Plate, Sheet, and Strip. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/A.htm?L+mystore+qkng6334+1140140874

ASTM International. 2005a. A 666, Standard Specification for Annealed or Cold-Worked Austenitic Stainless Steel Sheet, Strip, Plate, and Flat Bar. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/A.htm?L+mystore+qkng6334+1140140874

ASTM International. 2005c. F 1043, Standard Specification for Strength and Protective Coatings on Metal Industrial Chain Link Fence Framework. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874

ASTM International. 2005d. F 552, Standard Terminology Relating to Chain Link Fencing. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874

ASTM International. 2005e. F 567, Standard Practice for Installation of Chain-Link Fence. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874

ASTM International. 2006. F993-86(2006) Standard Specification for Valve Locking Devices. http://www.astm.org/cgi-bin/SoftCart.exe/STORE/filtrexx40.cgi?U+mystore+qkng6334+-L+F993+/usr6/htdocs/astm.org/DATABASE.CART/REDLINE_PAGES/F993.htm

Awwa Research Foundation (AwwaRF). 2004. *Request for Proposals: Assessment of Physical Security Technologies for Water and Wastewater Utilities (RFP 3044).* Denver, Colorado.

Axis Communications AB. 2006. Technical Guide to Network Video. Lund, Switzerland. http://www2.axis.com/files/brochure/bc_techguide_26553_en_0604_lo.pdf

Department of Defense (DoD). 2002. Minimum Antiterrorism Standards for Buildings. Unified Facilities Criteria UFC 4-010-01. www.tisp.org/files/pdf/dodstandards.pdf

Department of Defense (DoD). 2005. Unified Facilities Criteria (UFC) 4-022-01: Security Engineering: Entry Control Facilities/Access Control Points. http://65.204.17.188/report/doc_ufc.html

GlobalSpec – Engineering Search and Industrial Supplier Catalogs. GlobalSpec, Inc., Troy, NY. Last updated 11/21/06. Last viewed 12/06/06. http://www.globalspec.com/industrial-directory/Water_Pressure_Sensors/

Group 4 Technology. 2005. Security Management System User's Guide. Tewkesbury, U.K.

Illumination Engineering Society of North America (IENSA). 2000. Lighting Handbook (9th edition). New York, NY. July. https://www.iesna.org/shop/publications.index.cfm

Illumination Engineering Society of North America (IESNA). 2003. Guideline for Security Lighting for People, Property, and Public Spaces (G-1-03). New York, NY. https://www.iesna.org/shop/publications.index.cfm

National Fire Protection Association (NFPA). 2002. NFPA 101B: Code for Means of Egress for Buildings and Structures. Quincy, MA. http://www.nfpa.org/catalog/product.asp?category%5Fname=&pid=101B02&target%5Fpid=101B02&src%5Fpid=&link%5Ftype=search

National Fire Protection Association (NFPA). 2005. National Electrical Code® (NFPA 70) Handbook. Quincy. MA. http://www.nfpa.org/catalog/product.asp?category%5Fname=&pid=7005SB&target%5Fpid=7005SB&src%5Fpid=&link%5Ftype=search

National Fire Protection Association (NFPA). 2006. NFPA 101®: Life Safety Code®. Quincy, MA. http://www.nfpa.org/catalog/product.asp?pid=10106&src=catalog

National Law Enforcement and Corrections Technology Center (NLECTC). 1997. Perimeter Security Sensor Technologies Handbook. http://www.nlectc.org/perimetr/full2.htm

Naval Construction Battalion Center. 1990. Fencing, Wire and Post, Metal (Chain-Link Fence Gates) (Detail Specification) (RR-F-191/2D). http://www.wbdg.org/ccb/FEDMIL/rrf1912d.pdf

Naval Construction Battalion Center. 1990. Fencing, Wire and Post Metal (and Gates, Chain-Link Fence Fabric, and Accessories) (General Specification) (RR-F-191K/GEN). http://www.wbdg.org/ccb/FEDMIL/rrf191k.pdf

Naval Construction Battalion Center. 1990. Fencing, Wire and Post Metal (Chain-Link Fence Accessories) (Detail Specification) (RR-F-191/4D). http://www.wbdg.org/ccb/FEDMIL/rrf1914d.pdf

Naval Facilities Engineering Command (NAVFAC). 1999. Selection and Application of Vehicle Barriers (MIL-HDBK-1013/14). http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_14.pdf

Naval Facilities Engineering Service Center (NFESC). 1993. Design Guidelines for Physical Security of Facilities (MIL-HDBK-1013/1A). Washington Navy Yard, DC. http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_1a.pdf

Naval Facilities Engineering Service Center (NFESC). 1993. Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities (MIL-HDBK-1013/10). Washington Navy Yard, DC. http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_10.pdf

Stratus Consulting. 2007. *Critical Information Policies for Water Utilities.* Denver, Colo.: AwwaRF and AWWA, forthcoming.

U.S. Environmental Protection Agency. 2006. Water and Wastewater Security Product Guide. Last viewed December 5, 2006. http://cfpub.epa.gov/safewater/watersecurity/guide/tableofcontents.cfm

U.S. General Services Administration (GSA). 2005. Facilities Standards for the Public Buildings Service. Washington, DC. http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8195&channelPage=%2Fep%2Fchannel%2FgsaOverview.jsp&channelId=-17304

Underwriters Laboratories (UL). 1998. Surveillance Closed Circuit Television Equipment, UL 3044. http://ulstandardsinfonet.ul.com/scopes/scopes.asp?fn=3044.html

Water Environment Federation (WEF). 1998. Design of Municipal Wastewater Treatment Plants, Manual of Practice No. 8, 4th Edition. Alexandria, VA.

Water Environment Federation (WEF). 2004. Interim Voluntary Security Guidance for Wastewater/Stormwater Utilities, Alexandria, VA. http://www.awwa.org/science/wise/

ABBREVIATIONS

ASCE	American Society of Civil Engineers
ANSI	American National Standards Institute
ASIS	American Society for Industrial Security
AWWA	American Water Works Association
AwwaRF	Awwa Research Foundation
CD	compact disc
DHS	Department of Homeland Security
EPA	U.S. Environmental Protection Agency
ft	feet
IT	information technology
PAC	Project Advisory Committee
PC	personal computer
pdf	portable document format
QC	quality control
VA	vulnerability assessment
WEF	Water Environment Foundation
WERF	Water Environment Research Foundation
WISE	Water Infrastructure Security Enhancements

Awwa
Research
Foundation®

6666 West Quincy Avenue
Denver, CO 80235-3098 USA
P 303.347.6100
www.awwarf.org
email: info@awwarf.org

Sponsors Research

Develops Knowledge

Promotes Collaboration

1P-3C-91232-12/08-NH

ISBN 978-1-60573-034-9

9 781605 730349