

Guidelines for the Physical Security of Water Utilities

ANSI/ASCE/EWRI 56-10

Guidelines for the Physical Security of Wastewater/ Stormwater Utilities

ANSI/ASCE/EWRI 57-10

This document uses both the
International System of Units (SI)
and customary units



American Society of Civil Engineers

Guidelines for the Physical Security of Water Utilities

ANSI/ASCE/EWRI 56-10

Guidelines for the Physical Security of Wastewater/ Stormwater Utilities

ANSI/ASCE/EWRI 57-10

This document uses both the International System of Units (SI)
and customary units.



Published by the American Society of Civil Engineers



Documents
Document Sharing Hub

Library of Congress Cataloging-in-Publication Data

Guidelines for the physical security of water utilities, ASCE/EWRI 56-10. Guidelines for the physical security of wastewater-stormwater utilities ASCE/EWRI 57-10.

p. cm.

Includes bibliographical references and index.

ISBN 978-0-7844-1126-1 (alk. paper)

1. Water treatment plants—Security measures—Standards. 2. Storm sewers—Security measures—Standards. I. American Society of Civil Engineers. II. Environmental and Water Resources Institute (U.S.) III. Guidelines for the physical security of wastewater-stormwater utilities ASCE/EWRI 57-10

TD434.G85 2010

363.6'10684—dc22

2010047168

Published by American Society of Civil Engineers
1801 Alexander Bell Drive
Reston, Virginia 20191
www.pubs.asce.org

This standard was developed by a consensus standards development process which has been accredited by the American National Standards Institute (ANSI). Accreditation by ANSI, a voluntary accreditation body representing public and private sector standards development organizations in the U.S. and abroad, signifies that the standards development process used by ASCE has met the ANSI requirements for openness, balance, consensus, and due process.

While ASCE's process is designed to promote standards that reflect a fair and reasoned consensus among all interested participants, while preserving the public health, safety, and welfare that is paramount to its mission, it has not made an independent assessment of and does not warrant the accuracy, completeness, suitability, or utility of any information, apparatus, product, or process discussed herein. ASCE does not intend, nor should anyone interpret, ASCE's standards to replace the sound judgment of a competent professional, having knowledge and experience in the appropriate field(s) of practice, nor to substitute for the standard of care required of such professionals in interpreting and applying the contents of this standard.

ASCE has no authority to enforce compliance with its standards and does not undertake to certify products for compliance or to render any professional services to any person or entity.

ASCE disclaims any and all liability for any personal injury, property damage, financial loss or other damages of any nature whatsoever, including without limitation any direct, indirect, special, exemplary, or consequential damages, resulting from any person's use of, or reliance on, this standard. Any individual who relies on this standard assumes full responsibility for such use.

ASCE and American Society of Civil Engineers—Registered in U.S. Patent and Trademark Office.

Photocopies and reprints. You can obtain instant permission to photocopy ASCE publications by using ASCE's online permission service (<http://pubs.asce.org/permissions/requests/>). Requests for 100 copies or more should be submitted to the Reprints Department, Publications Division, ASCE (address above); e-mail: permissions@asce.org. A reprint order form can be found at <http://pubs.asce.org/support/reprints/>.

Copyright © 2011 by the American Society of Civil Engineers.

All Rights Reserved.

ISBN 978-0-7844-1126-1

Manufactured in the United States of America.

18 17 16 15 14 13 12 11 1 2 3 4 5

STANDARDS

In 2006, the Board of Direction approved the revision to the ASCE Rules for Standards Committees to govern the writing and maintenance of standards developed by the Society. All such standards are developed by a consensus standards process managed by the Society's Codes and Standards Committee (CSC). The consensus process includes balloting by a balanced standards committee made up of Society members and nonmembers, balloting by the membership of the Society as a whole, and balloting by the public. All standards are updated or reaffirmed by the same process at intervals not exceeding five years.

The following standards have been issued:

- ANSI/ASCE 1-82 N-725 Guideline for Design and Analysis of Nuclear Safety Related Earth Structures
- ASCE/EWRI 2-06 Measurement of Oxygen Transfer in Clean Water
- ANSI/ASCE 3-91 Standard for the Structural Design of Composite Slabs and ANSI/ASCE 9-91 Standard Practice for the Construction and Inspection of Composite Slabs
- ASCE 4-98 Seismic Analysis of Safety-Related Nuclear Structures
- Building Code Requirements for Masonry Structures (ACI 530-02/ASCE 5-02/TMS 402-02) and Specifications for Masonry Structures (ACI 530.1-02/ASCE 6-02/TMS 602-02)
- ASCE/SEI 7-10 Minimum Design Loads for Buildings and Other Structures
- SEI/ASCE 8-02 Standard Specification for the Design of Cold-Formed Stainless Steel Structural Members
- ANSI/ASCE 9-91 listed with ASCE 3-91
- ASCE 10-97 Design of Latticed Steel Transmission Structures
- SEI/ASCE 11-99 Guideline for Structural Condition Assessment of Existing Buildings
- ASCE/EWRI 12-05 Guideline for the Design of Urban Subsurface Drainage
- ASCE/EWRI 13-05 Standard Guidelines for Installation of Urban Subsurface Drainage
- ASCE/EWRI 14-05 Standard Guidelines for Operation and Maintenance of Urban Subsurface Drainage
- ASCE 15-98 Standard Practice for Direct Design of Buried Precast Concrete Pipe Using Standard Installations (SIDD)
- ASCE 16-95 Standard for Load Resistance Factor Design (LRFD) of Engineered Wood Construction
- ASCE 17-96 Air-Supported Structures
- ASCE 18-96 Standard Guidelines for In-Process Oxygen Transfer Testing
- ASCE/SEI 19-10 Structural Applications of Steel Cables for Buildings
- ASCE 20-96 Standard Guidelines for the Design and Installation of Pile Foundations
- ANSI/ASCE/T&DI 21-05 Automated People Mover Standards—Part 1
- ANSI/ASCE/T&DI 21.2-08 Automated People Mover Standards—Part 2
- ANSI/ASCE/T&DI 21.3-08 Automated People Mover Standards—Part 3
- ANSI/ASCE/T&DI 21.4-08 Automated People Mover Standards—Part 4
- SEI/ASCE 23-97 Specification for Structural Steel Beams with Web Openings
- ASCE/SEI 24-05 Flood Resistant Design and Construction
- ASCE/SEI 25-06 Earthquake-Actuated Automatic Gas Shutoff Devices
- ASCE 26-97 Standard Practice for Design of Buried Precast Concrete Box Sections
- ASCE 27-00 Standard Practice for Direct Design of Precast Concrete Pipe for Jacking in Trenchless Construction
- ASCE 28-00 Standard Practice for Direct Design of Precast Concrete Box Sections for Jacking in Trenchless Construction
- ASCE/SEI/SFPE 29-05 Standard Calculation Methods for Structural Fire Protection
- SEI/ASCE 30-00 Guideline for Condition Assessment of the Building Envelope
- SEI/ASCE 31-03 Seismic Evaluation of Existing Buildings
- SEI/ASCE 32-01 Design and Construction of Frost-Protected Shallow Foundations
- EWRI/ASCE 33-09 Comprehensive Transboundary International Water Quality Management Agreement
- EWRI/ASCE 34-01 Standard Guidelines for Artificial Recharge of Ground Water
- EWRI/ASCE 35-01 Guidelines for Quality Assurance of Installed Fine-Pore Aeration Equipment
- CI/ASCE 36-01 Standard Construction Guidelines for Microtunneling
- SEI/ASCE 37-02 Design Loads on Structures during Construction
- CI/ASCE 38-02 Standard Guideline for the Collection and Depiction of Existing Subsurface Utility Data
- EWRI/ASCE 39-03 Standard Practice for the Design and Operation of Hail Suppression Projects
- ASCE/EWRI 40-03 Regulated Riparian Model Water Code
- ASCE/SEI 41-06 Seismic Rehabilitation of Existing Buildings
- ASCE/EWRI 42-04 Standard Practice for the Design and Operation of Precipitation Enhancement Projects
- ASCE/SEI 43-05 Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities
- ASCE/EWRI 44-05 Standard Practice for the Design and Operation of Supercooled Fog Dispersal Projects
- ASCE/EWRI 45-05 Standard Guidelines for the Design of Urban Stormwater Systems
- ASCE/EWRI 46-05 Standard Guidelines for the Installation of Urban Stormwater Systems
- ASCE/EWRI 47-05 Standard Guidelines for the Operation and Maintenance of Urban Stormwater Systems
- ASCE/SEI 48-06 Design of Steel Transmission Pole Structures
- ASCE/EWRI 50-08 Standard Guideline for Fitting Saturated Hydraulic Conductivity Using Probability Density Functions
- ASCE/EWRI 51-08 Standard Guideline for Calculating the Effective Saturated Hydraulic Conductivity
- ASCE/SEI 52-10 Design of Fiberglass-Reinforced Plastic (FRP) Stacks



Documents

Document Sharing Hub

ASCE/G-I 53-10 Compaction Grouting Consensus Guide
ASCE/EWRI 54-10 Standard Guideline for the Geostatistical
Estimation and Block-Averaging of Homogeneous and Isotropic Saturated Hydraulic Conductivity
ASCE/SEI 55-10 Tensile Membrane Structures
ANSI/ASCE/EWRI 56-10 Guidelines for the Physical Security
of Water Utilities

ANSI/ASCE/EWRI 57-10 Guidelines for the Physical Security
of Wastewater/Stormwater Utilities
ASCE/T&DI/ICPI 58-10 Structural Design of Interlocking Concrete Pavement for Municipal Streets and Roadways

ASCE 59-10 Guidelines for the Physical Security of Water Utilities

CONTENTS

	Page
FOREWORD	ix
ACKNOWLEDGMENTS	xi
 GUIDELINES FOR THE PHYSICAL SECURITY OF WATER UTILITIES	
1 Application of Guidelines	1
1.1 Introduction	1
1.1.1 Elements of a Physical Protection System	1
1.1.1.1 Deterrence	1
1.1.1.2 Detection	1
1.1.1.3 Delay	1
1.1.1.4 Response	1
1.1.2 Design Basis Threat	1
1.1.2.1 Vandal	1
1.1.2.2 Criminal	1
1.1.2.3 Saboteur	2
1.1.2.4 Insider	2
1.2 Methodology for Applying These Guidelines	4
1.2.1 Instructions for Applying These Guidelines	4
1.2.1.1 Step 1: Vulnerability Assessment	4
1.2.1.2 Step 2: Characterize Design Basis Threat	5
1.2.1.3 Step 3: Identify Security Measures	5
1.2.1.4 Step 4: Consider Consequence Mitigation	5
1.2.2 Additional Information to Assist in Applying	6
1.2.2.1 New and Existing Facilities	6
1.2.2.2 Local Codes and Required Aesthetics	6
1.2.2.3 Assets Not Under Utility Control	6
1.2.2.4 Balance of the System	6
1.2.2.5 Value of the Asset	6
1.2.2.6 Levels of Security Measures	6
1.2.2.7 Response Time and Capabilities	6
2 Raw Water Facilities	7
2.1 Scope	7
2.2 Facility Mission	7
2.3 Philosophy of Security Approach	7
2.4 Benchmark Security Measures	7
3 Wells and Pumping Stations	13
3.1 Scope	13
3.2 Facility Mission	13
3.3 Philosophy of Security Approach	13
3.4 Benchmark Security Measures	13
4 Water Treatment Plants	19
4.1 Scope	19
4.2 Facility Mission	19
4.3 Philosophy of Security Approach	19
4.4 Benchmark Security Measures	19
5 Finished Water Storage Facilities	25
5.1 Scope	25
5.2 Facility Mission	25



5.3	Philosophy of Security Approach	25
5.4	Benchmark Security Measures	25
6	Water Distribution Systems	31
6.1	Scope.	31
6.2	System Mission	31
6.3	Philosophy of Security Approach	31
6.4	Benchmark Security Measures	31
7	Water System Support Facilities.	35
7.1	Scope.	35
7.2	Facility Mission	35
7.3	Philosophy of Security Approach	35
7.4	Benchmark Security Measures	35
Appendix A	Physical Security Elements	41
A.1.0	Fencing and Perimeter Walls	41
A.1.1	Chain-Link Fencing	41
A.1.2	Anti-Climb/Anti-Cut Fencing.	41
A.1.3	Ornamental Fencing.	41
A.1.4	Perimeter Wall.	42
A.1.5	Fencing Topping.	42
A.1.6	Perimeter Line.	42
A.1.7	Fence Foundation Enhancements	42
A.2.0	Gates	42
A.2.1	Chain-Link Gates	42
A.2.2	Electronic Gate Opening	42
A.2.3	Electronic Gate Control System	43
A.3.0	Site Areas	43
A.3.1	Clear Zones	43
A.3.2	Site Utilities	43
A.4.0	Facility Entrances	43
A.4.1	Sallyport Entrances	43
A.4.2	Building Entrances	44
A.5.0	Bollards and other Vehicle Barriers	44
A.6.0	Exterior Surfaces	44
A.7.0	Outdoor Security Lighting.	44
A.8.0	Signage.	44
A.8.1	Fence Signage	44
A.8.2	Primary Site Entrance Signage	44
A.8.3	Water Intake Delineation	45
A.9.0	Electronic Security Systems.	45
A.9.1	Intrusion Detection Sensors: General.	45
A.9.2	Exterior Intrusion Detection.	45
A.9.2.1	Active Infrared Sensors	45
A.9.2.2	Microwave Sensors.	45
A.9.2.3	Dual-Technology Sensors	45
A.9.2.4	Buried Line Sensors	45
A.9.2.5	Fence-Mounted Sensors	45
A.9.3	Interior Intrusion Detection	46
A.9.3.1	Dual-Technology Motion Sensors	46
A.9.3.2	Linear Beam Sensors.	46
A.9.3.3	Glass-Break Sensors	46
A.9.4	Door and Hatch Contact Alarm Switches.	46
A.9.5	Pipeline Vibration Detection	46
A.10.0	Access Control Systems	46
A.10.1	Access Control Systems: General.	46
A.10.2	Locks and Padlocks	46
A.10.3	Numeric Keypad Locks	46
A.10.4	Card Reader Systems	46
A.11.0	Closed-Circuit Television (CCTV) Surveillance	47
A.11.1	General Considerations	47

A.11.2	Field of View	47
A.11.3	CCTV Housings and Mounts	47
A.11.4	Video Network Servers	47
A.11.5	Digital Video Recorders.	47
A.11.6	CCTV Computer Application Software.	48
A.12.0	Security, Controls, and SCADA Wiring.	48
A.12.1	SCADA and Electrical Control Panel Enclosures	48
A.13.0	Building Elements	48
A.13.1	General	48
A.13.2	Doors	48
A.13.3	Security Grilles	48
A.13.4	Security Cages.	48
A.14.0	Hatches, Vaults, and Vents	48
A.14.1	Hatch, Vault, and Vent Alarms: General	48
A.14.2	Roof or Sidewalk Hatches	48
A.14.3	Roof Vents.	49
A.14.4	Vault Hatch with Elevated Curb	49
A.14.5	Vault Door Hatch Set Flush with Top of a Structural Slab.	49
A.15.0	Online Water Quality Monitoring	49
A.16.0	Operator Devices	49
A.16.1	Man-Down Transmitter	49
A.17.0	Chemical Fill-Line Locking Devices	49
A.18.0	Hydrants	49
A.19.0	Manholes.	49
GLOSSARY AND ABBREVIATIONS		51
REFERENCES		55
GUIDELINES FOR THE PHYSICAL SECURITY OF WASTEWATER/STORMWATER UTILITIES.		67
INDEX		111

10/04/2014 00:24:12 MDT

FOREWORD

These guidelines were developed as a joint effort between the American Society of Civil Engineers (ASCE) and the American Water Works Association (AWWA) with technical input from the Water Environment Federation (WEF), in accordance with ASCE Rules for Standards Committees, and were published initially as a proposed draft, *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA/WEF 2006). That consensus process included balloting by a balanced Standards Committee and reviewing during a public comment period. The provisions of this document have been written in permissive language and, as such, offer to the user a series of options or instructions but do not prescribe a specific course of action. Significant judgment is left to the user of these documents.

These guidelines use customary units with the International System of Units (SI) in parentheses. This approach was in the best interest of ASCE, AWWA, and WEF at the time of development of the initial Draft of these guidelines.

PURPOSE OF THE GUIDELINES

These guidelines apply to physical security for facilities used in potable water source, treatment, and distribution systems.

BACKGROUND OF THE DEVELOPMENT

Highlights related to the creation of all the Water Infrastructure Security Enhancements (WISE) guidance documents and/or standards in the early years of the twenty-first century are summarized below:

1. Under the U.S. Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107-188), drinking water utilities serving more than 3,300 customers were required to conduct vulnerability assessments (VAs) of their water systems. The VAs often recommended security improvements to reduce the risk of malevolent acts (such improvements may also reduce the risk associated with natural events). Similar requirements for wastewater utilities have yet to be promulgated, but the protection of wastewater utility facilities using similar approaches has been promoted by the U.S. Environmental Protection Agency (USEPA) and various industry organizations. In addition, ASCE, AWWA, and WEF agreed to work together to develop materials to assist in the implementation of security recommendations and the overall improvement of water and wastewater infrastructure security. The project was funded by USEPA under a cooperative agreement to foster public/private partnership in water and wastewater security. This project was known as the USEPA Water Infrastructure Security Enhancements (WISE) Project.
2. The three organizations each became responsible for a portion of the project: AWWA led the drinking water supply, treatment, and distribution systems effort; WEF led the wastewater and stormwater collection, treatment, and disposal systems effort; and ASCE led the effort concerning the methodology and characteristics pertinent to design of contaminant detection and monitoring systems for both water and wastewater systems.
3. Phase 1 of the USEPA WISE project focused on the creation of Interim Voluntary Security Guidance documents (ASCE/AWWA/WEF 2004a, 2004b, 2004c). The purpose of these documents was to provide a centralized starting point for utilities as they integrate modern security practices into the management, operation, construction, or retrofit of their water, wastewater, and stormwater systems. Training materials were developed in Phase 2 to disseminate the information contained in the Phase 1 guidance documents.
4. Under the direction of USEPA, Phase 3 focused solely on the development of physical security guidelines for water, wastewater, and stormwater facilities. These voluntary consensus guidelines were first developed as the Draft and were published initially as *Guidelines for Physical Security for Water Utilities* (ASCE/AWWA/WEF 2006). The primary reviewers were members of the Water Supply Subcommittee of the ASCE WISE Standards Committee (SC), and the USEPA/ASCE/AWWA/WEF WISE Project Phase 3 Team.
5. The sections compiled in these guidelines are intended to provide direction to water utilities on how to design or retrofit their infrastructure, with consideration given to their unique circumstances and threats. A discussion of the various security threats and incidents that have occurred at water and wastewater utilities is provided in an American Water Works Association Research Foundation report by Welter (2003). This document can provide additional information in the assessment of security measures for utilities.
6. The USEPA Water Security Working Group presented its report *Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on Water Security Practices, Incentives, and Measures* to the National Drinking Water Advisory Council (NDWAC) on May 18, 2005 (WSWG 2005). Those findings included 18 features of an “active and effective” security program. These guidelines address the following NDWAC recommendations, which discuss physical security:
 - a. Establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.
 - b. Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; this should include consideration of opportunities to reduce risk through physical hardening and the adoption of inherently lower-risk design and technology options.
7. These guidelines should be implemented in concert with the other features and approaches described in the NDWAC report (WSWG 2005).

USE OF THESE GUIDELINES

The major points for the use of this document imply:

1. It is the responsibility of the user of an ASCE/EWRI standard or guideline to determine that the products and approaches described in the standard or guideline are suitable for use in the particular application being considered.
2. To effectively use these guidelines, a water utility should first complete a VA of its system. This VA should be completed in accordance with a generally accepted methodology such as the Risk Assessment Methodology for Water (RAM-W; Sandia Corporation 2002), the Vulnerability Self-Assessment Tool (VSAT; NACWA 2005), or other acceptable method. The resulting information will guide the utility in defining the capabilities and motives of its design basis threat (DBT) and in ranking each asset's criticality within the facility's system. The VA will also help to define the anticipated response time and response capability that, given the capabilities of the DBT, will characterize the robustness required for an effective security system.
3. The selection and recommendation of the physical protection approaches and measures contained in these guidelines are best engineering practices based on the collective experience and judgment of the WISE Standards Committee members. The physical security measures should be combined with management policies, operational procedures, and network security systems to form a comprehensive security system that provides multiple layers of protection or "protection in depth" for critical assets.
4. These guidelines contain information that utilities should consider when applying specific security technologies and methods to individual facilities or assets. These are described in Sections 2.0 through 7.0 (called "Guideline" in each section), which, in conjunction with the Foreword, Section 1.1 Introduction and its subsections, and the Appendices in this document, can be used as stand-alone documents. Most of the tables and figures of these guidelines were taken directly from ASCE/AWWA/WEF (2006) as cited herein, but Table 6-1 was adapted from that source due to public comments during the development process during the first six months of 2007 and the ASCE/EWRI Standards Committee ballots of 2008 and 2009.
5. It is important to recognize that a physical protection system should be designed as a site-specific system integrated into facility operations, response force capabilities, and the overall utility's security system to ensure that there are no gaps in protection. Furthermore, simply implementing the recommendations contained herein is no guarantee that an adversary cannot compromise a specific facility or critical asset.

SPECIAL ISSUES

1. These guidelines describe physical security approaches to delay or detect malevolent parties whose actions may oth-

erwise defeat the mission of the utility. Enterprise-wide security approaches, while extremely important to any balanced security system, are beyond the scope of these guidelines. These approaches include management policies, administrative procedures, operational practices, and network security approaches, including supervisory control and data acquisition (SCADA) networks. Contaminant detection and monitoring systems, although briefly referenced in these guidelines, are also best employed as an integrated, enterprise-wide system. Guidance on enterprise-wide security approaches is provided in the USEPA WISE Phase 1 Interim Voluntary Security Guidance documents (ASCE/AWWA/WEF 2004a, 2004b, 2004c).

2. Added water security is beneficial for continuity of business, protection of water quality, provision of sufficient water quantity, ensuring public confidence, and protection of public health and safety. Thus, when implementing the security measures provided in these guidelines, the multiple benefits should be taken into account by utility staff and other stakeholders.
3. Within the scope of this document, domestic and international terrorists have been considered a special category of DBTs. With significantly enhanced tool and weapon capabilities, terrorists may be politically or ideologically motivated to cause maximum human casualties, often without regard for the terrorist's personal survival. Effectively protecting a facility from such a threat requires specialized security knowledge and equipment, and response forces typically not available to utilities. A utility that concludes that it is facing such a threat should seek guidance from specialized security experts and/or enhance its emergency response planning and execution to mitigate the consequences of such a terrorist attack. Strategies to counter such a defined threat may require higher-level measures than described in these guidelines.

DISCLAIMER

The information presented in these guidelines is intended to assist water utilities as they strive to improve the safety and security of their facilities, their employees, and the public. While the strategies and methods described here can reduce risk and enhance response and recovery actions, they cannot guarantee that any possible act of vandalism, violence, or terrorism will be prevented or stopped. As such, those responsible for the content and publication of this document can provide no guarantees for the performance of any actions taken in response to this guidance.

This document has been prepared in accordance with recognized engineering principles and should not be used without the user's competent knowledge for a given application. The publication of this document does not intend to warrant that the information contained herein is suitable for any general or specific use, and those responsible for the content and publication of this document take no position respecting the validity of patent rights. The user is advised that the determination of patent rights or risk of infringement is entirely their own responsibility.

ACKNOWLEDGMENTS

These voluntary guidelines were developed during the USEPA WISE Project, Phase 3 under the direction of the ASCE/EWRI WISE Standards Committee (ASCE/AWWA/WEF 2006). This committee consisted of the individuals listed below through the end of the Committee balloting process of August 2007. The members of the WISE Water Supply Subcommittee, which was the primary review group before the first ASCE/EWRI WISE SC

pilot sections ballot, are also provided below. The CH2M HILL WISE Project Phase 3 Team members listed below drafted the document and assisted in the resolution reporting during the balloting process. The USEPA personnel listed with the Project Team reviewed material during the monthly WISE Project Partners conference calls of the USEPA WISE Project that ended around October 1, 2008.

Clifford L. Bowen, P.E.
William C. Boyle, Ph.D., P.E., B.C.E.E.
Erica M. Brown
Jeanette A. Brown, P.E., B.C.E.E.
Jonathan W. Bulkley, Ph.D., P.E.
Ivan Burrowes
James B. Conboy, P.E., B.C.E.E.
Joseph W. Dellapenna, Esq.
Clyde R. Dugan
John H. Easton, Ph.D.
Findlay G. Edwards, Ph.D., P.E.,
Vice Chair
Wayne Einfeld
Jorge A. Garcia, Ph.D., P.E.
Neil S. Grigg, Ph.D., P.E.
Yakir J. Hasit, Ph.D., P.E.
Todd Humphrey, P.E.
C. Dale Jacobson, P.E., B.C.E.E.
Jyung Seok Jeong
Conrad G. Keyes, Jr., Sc.D., P.E., P.S.,
D.W.R.E., Dist.M.ASCE, Chair

M. Patricia Lamb, C.U.S.A.
Thomas J. Lane, P.E.
Srinivasa Lingireddy, Ph.D., P.E.
Thomas J. Linville, P.E.
Daniel L. Lynch, P.E., B.C.E.E.
John W. McLaughlin, P.E.
Brian M. Murphy, P.E.
Irwin M. Pikus, Ph.D., Esq.
J. Alan Roberson, P.E.
Kyle E. Schilling, P.E., B.C.E.E.,
D.W.R.E.
Charles R. Stack, M.P.H.
C. Wesley Strickland, Esq.
Lloyd V. Urban, Ph.D., P.E.
James Van Norman
Gregory J. Welter, P.E., B.C.E.E.
James F. Wheeler, P.E.
Harold F. Wiedeman, P.E.
Robert C. Williams, P.E., B.C.E.E.

Water Supply Subcommittee

Edward E. Baruth (AWWA)
Beth Behner (AWWA)
Clifford L. Bowen, P.E.
Scott Brooks
Erica M. Brown
Clyde R. Dugan
Neil S. Grigg, Ph.D., P.E.
Todd Humphrey, P.E.
M. Patricia Lamb, C.U.S.A., Vice Chair
Thomas J. Lane, P.E.
Thomas J. Linville, P.E.
John W. McLaughlin, P.E., Chair
Brian M. Murphy, P.E.
James A. Roberson, P.E.
Roy Robinson, Past Chair
James S. Wailes, P.E. (AWWA)

The USEPA ASCE/AWWA/WEF WISE Project Team that worked with the CH2M HILL and its subconsultant Richard Brady and Associates, Inc. team members listed below organized

and carried out the Phase 3 plan during June 2005 through the end of 2006 (ASCE/AWWA/WEF 2006). They included:

L. Christian Hanson, C.A.E. (ASCE),
WISE Project Manager and Recording
Secretary for the WISE SC
Conrad G. Keyes, Jr., Sc.D., P.E., P.S.,
D.W.R.E., WISE Standards Committee
Chair
Findlay G. Edwards, Ph.D., P.E., WISE
Standards Committee Vice Chair
John W. McLaughlin, P.E., Water Supply
Subcommittee Chair
M. Patricia Lamb, C.U.S.A., Water
Supply Subcommittee Vice Chair
Irwin M. Pikus, Ph.D., Esq.,
Methodology and Characteristics
Subcommittee Chair

Yakir J. Hasit, Ph.D., P.E., Methodology
and Characteristics Subcommittee Vice
Chair
Jeanette A. Brown, P.E., B.C.E.E.,
Wastewater Stormwater Subcommittee
Chair
William C. Boyle, Ph.D., P.E., B.C.E.E.,
Wastewater Stormwater Subcommittee
Vice Chair
Stacy Passaro, P.E., B.C.E.E. (WEF),
WISE Project Manager
James S. Wailes, P.E. (AWWA), WISE
Project Manager

CH2M HILL Team

Jason M. Assouline
Paul A. Berg, P.E.
Richard D. Brady, P.E., B.C.E.E.
(Richard Brady and Associates, Inc.)
Dale D. Gabel, P.E.
Forrest M. Gist, P.E.
Kristine K. Hargreaves, AIA
Yakir J. Hasit, Ph.D., P.E.
Sam Irrinki, P.E.
Alan B. Ispass, P.E., B.C.E.E.
Jacqueline T. Kepke, P.E.
M. Jane Mailand
Lena Perkins

USEPA

Gregory Spraul

Guidelines for the Physical Security of Water Utilities

Chapter 1

APPLICATION OF GUIDELINES

1.1 INTRODUCTION

These water utility guidelines recommend physical and electronic security measures for physical protection systems to protect against identified adversaries, referred to as design basis threats (DBTs), with specified motivations, tools, equipment, and weapons. Additional requirements and security equipment may be necessary to defend against threats with greater capabilities.

1.1.1 Elements of a Physical Protection System. Effective physical and electronic protection systems balance four elements (ASCE/AWWA/WEF 2004c): deterrence, detection, delay, and response.

1.1.1.1 Deterrence. Security measures such as lighting, the presence of closed-circuit television (CCTV), a clearly visible facility with no visual obstructions, or people in the area may deter an adversary from attacking a facility. Deterrence is not generally considered a part of a physical protection system with a predictable level of effectiveness; however, it can reduce the occurrence of crime or low-level vandal attacks.

1.1.1.2 Detection. Security measures such as sensors are intended to detect the presence of an intruder. An effective detection system should include electronic features such as sensors as well as cameras or visual observation for assessment of alarm validity. Depending on the types of sensors, a detection system may include lighting systems, motion detectors, monitoring cameras, access control equipment, or other devices.

1.1.1.3 Delay. Security features such as physical barriers are designed to delay an adversary until a response force can interrupt the adversary's actions. Delay features consist primarily of physical hardening devices often employed in multiple layers to provide protection in depth. Delay features are only effective when placed within a layer of detection.

1.1.1.4 Response. "Response" refers to actions taken to interrupt the adversary's task. Utility staff, the utility's security response force, or law enforcement may carry out the response, with the appropriate responder dependent on the threat and policy of the utility.

The capabilities of the responders to a security event, including number, authority, and weaponry, should be greater than the capabilities of the perceived threat to the facility. The appropriate response force should be identified during the facility's vulnerability assessment (VA) with notification, communication, and protocol requirements established in the utility's emergency response plan or a similar plan.

Figure 1-1 illustrates the interaction of detection (at the perimeter fence and exterior door), delay (fence, exterior door, and interior door), and the response time to an adversary's sequence of actions. This figure was originally developed by Mary Lynn Garcia of Sandia National Laboratories and uses a thief (that is,

a criminal) as the DBT to illustrate the time required for delay. Utilities should develop their own time sequence as part of their vulnerability assessment process.

1.1.2 Design Basis Threat. DBTs considered in these guidelines address persons who intend to interrupt the water treatment or delivery processes, contaminate the water, or trespass on the water utility property in order to commit a malevolent act. The following subsections summarize the objectives, motives, and fundamental security approaches for each DBT used in this guideline. Table 1-1 contains additional information on the objectives, motives, and capabilities of DBT levels. The table also elaborates on the differences between base and enhanced DBT levels.

1.1.2.1 Vandal. Vandals are intent on defacing, damaging, or destroying property. They primarily seek targets of opportunity, using stealth to avoid detection. Adversaries in this group do not intend to injure or kill people (although such may occur as an accidental result of their actions), and are assumed to be unarmed.

Security approaches for a base-level vandal threat generally consist of placing physical barriers between the assets and public areas, and visual detection of intruders by utility staff or the general public. Use of appropriate perimeter fences and gates, adequate perimeter and area lighting, and hardened locks often provides sufficient deterrence from all but the most motivated vandals. Where the damage that could be caused by vandals is of relatively low cost to repair, utilities should consider whether it is more cost-effective to focus on consequence mitigation (i.e., the repair or replacement of assets) rather than on investing in expensive security systems and protective measures.

An enhanced threat created by a more intense or invasive vandal (one consisting of a greater number of individuals who plan the activities or who have access to larger or more capable tools) requires security approaches that detect and delay the intruder until the appropriate response force can stop the threat. These measures are generally only appropriate when the value of the assets is sufficient that consequence mitigation is a more costly or an unacceptable approach. Liability issues should also be considered.

1.1.2.2 Criminal. The primary motivation for a criminal is the desire to obtain equipment, tools, or components that have inherent value and can be sold. Criminals typically use stealth to avoid apprehension, and response times should focus on the time required for the adversary to obtain the asset. Depending on their level of desperation or sophistication, criminals may be armed and willing to injure or kill to accomplish their objectives.

Protective approaches against the base-level criminal threat with limited hand tools are focused on deterrence and delay. Visual barriers act as a deterrent to prevent the detection of assets by an opportunistic criminal. Prevention or delay of the removal of equipment and other targets can result from physical separation from public areas, adequate lighting, and physical barriers.

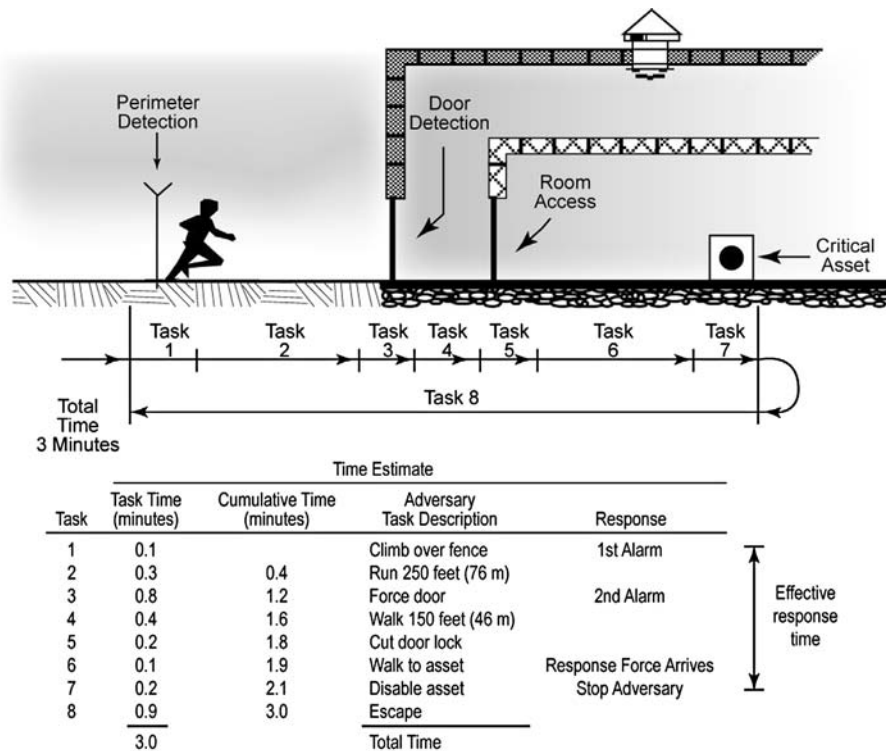


FIGURE 1-1. CONCEPT OF DELAY CALCULATION.
Source: Adapted from Garcia (2001), with permission. © Elsevier.

such as fences, protected heavy-duty locks, high-quality doors and strikes, cabinets, and similar features. Multiple layers of protection provide additional delay to the adversary in completing his objective. Replacement or repair of some equipment in lieu of extensive security systems may be an appropriate and cost-effective approach.

Equipment with significant monetary or mission-related value that the utility determines must be protected from an enhanced criminal threat with significant planning or substantial hand, power, and possibly thermal tools requires a security system that detects the adversary and physically delays the theft until the appropriate response force arrives.

1.1.2.3 Saboteur. A saboteur is typically motivated by political, doctrinal, or religious causes, although revenge may also be a motivation. These individuals primarily use stealth to achieve their objectives, but they can be armed and willing to injure or kill others if threatened. The saboteur is intent on damage or destruction of the utility's facilities or generating a lack of public confidence in the utility's ability to serve and protect the public. Effectively defeating a saboteur may require a response force more robust than that typically needed for the other DBT categories and may require the capabilities of a trained Special Weapons and Tactics (SWAT) team.

The difference between a base and enhanced level of threat from a saboteur is defined by the capabilities and methods. The base-level saboteur threat often possesses simple tools and attempts to either contaminate the water system by introducing a toxic compound, or damage the facility components to prevent its operation. The security approach for defeating this threat is to detect the intruders, quickly assess that the intruders are a threat, and delay them until a response force interrupts their actions.

Additional physical delay features are required to adequately impede an enhanced saboteur threat with more sophisticated tools and weapons, which can include explosives, and the ability to not only contaminate the water but also to destroy critical facilities. Depending on the capabilities of the saboteurs, security features may be required to resist an attack from an improvised explosive device (IED) such as a pipe bomb, or an improvised incendiary device (IID).

1.1.2.4 Insider. An insider is a person with knowledge of the utility who has access to the facilities or portions of the system as part of his or her daily work activities. Insiders may be disgruntled employees or contractors with employee-level access, and may be armed. Insiders may also include personnel being manipulated by or working in collusion with criminals or saboteurs. Objectives of insiders may include compromising the effectiveness of the utility facilities, contaminating the public water supply, humiliating the utility's management, stealing records or other information, stealing items of value (for example, tools, money, parts, computers, or televisions), or injuring other employees.

The approach for preventing insider threats includes effective control of staff access to critical areas through management policies (for example, a two-person access rule) and possibly an electronic access control system (for example, individualized card readers) to document and control entry. Access to the facility's supervisory control and data acquisition (SCADA) and other instrumentation and control software and hardware should also be controlled. Effective access control to prevent insider tampering is typically achieved through tiered access strategies, such that higher levels of access rights are necessary to access increasingly more critical physical areas or software systems. This should be combined with background checks on utility staff.

TABLE 1-1 DESIGN BASIS THREAT CAPABILITY MATRIX (ASCE/AWWA/WEF 2006)

Characteristic	Vandal		Criminal		Saboteur		Insider ^a	
	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced
Objective	Damage, deface, or destroy targets of opportunity		Theft of valuable assets		Disruption, destruction, or contamination; destroy public confidence in utility/governmental agency		Property damage, theft, disruption, destruction, or contamination	
Motivation	Thrill, dare, grudge		Financial gain, grudge		Political, doctrinal, or religious causes, grudge		Revenge, financial gain, political cause, collusion with outsider	
Planning/system knowledge	Little or none	Possible	Base	Enhanced	Base	Enhanced	Base	Enhanced
			Little, opportunistic	Definite	Definite	Definite	Limited access to equipment, facilities, SCADA, or networks	Extensive access to equipment, facilities, SCADA, networks, and security systems; greater system knowledge
Weapons	None	None	Unlikely	Knives, hand guns, or rifles	Knives or hand guns, toxic materials	Automatic and semi-toxic materials	Unlikely	Knives, hand guns, or rifles, toxic materials
Tools and implements of destruction	Readily available hand tools or equipment available at the facility, spray paint	Basic hand tools (e.g., pliers, wire cutters, hammers, baseball bats, or firecrackers.)	Hand tools or readily available tools or equipment at the facility (as needed)	Sophisticated hand and/or power tools	Basic hand tools (e.g., pliers, wire cutters, hammers, crowbars)	Unlimited variety of hand, power, and thermal tools (including tools such as cutting torches, contaminant agents, IEDs and IIDs)	Tools or equipment available at the facility.	Tools or equipment available at the facility.
Contaminants	None	Possible	None	None	Probable	Probable	Possible	Possible
Asset damage	Minimal	Possible	Minimal	Possible	Possible	Significant	Significant	Significant
Injuries	None	Possible (unintentional)	Possible	Possible	Possible	Possible	Possible	Possible
Fatalities	None	Possible (unintentional)	Possible	Possible	Possible	Possible	Possible	Possible

^aThe insider may possess similar objectives or motivations to the other DBT categories, but will have access to facilities without causing suspicion. Insiders include: employees, vendor representatives, delivery persons, consultants, and onsite contractors.
 DBT: design basis threat; SCADA: supervisory control and data acquisition; IED, improvised explosive device; IID, improvised incendiary device.

only trusted individuals have access to critical assets. Consequence mitigation should also be considered.

An enhanced insider threat has more in-depth system knowledge and generally has a higher level of access rights to critical equipment, facilities, SCADA, computer networks, and security systems. Protection from an enhanced threat requires additional management policies, increasingly more robust electronic access control, and computerized monitoring systems where consequence mitigation is unacceptable. Management policies are not addressed in these physical security guidelines; however, the physical security elements that complement those policies are presented.

1.2 METHODOLOGY FOR APPLYING THESE GUIDELINES

This section applies to all subsequent sections in this document and contains instructions that describe the basic steps for its use. This section also contains information that utilities should consider when applying the overall guidelines to their specific

facilities and needs. Sections 2.0 through 7.0 describe specific security technologies and methods that can be applied to individual facilities or assets. These sections, in conjunction with the Foreword, Section 1.1 Introduction and its subsections, and the Appendices in these guidelines, can be used as standalone documents.

1.2.1 Instructions for Applying These Guidelines. The following steps list, in order, the actions a utility should take as it applies these guidelines to its facilities. Figure 1-2 presents an example of a decision tree a utility would use as it follows these steps for a particular asset.

1.2.1.1 Step 1: Vulnerability Assessment

1. Complete a water system-wide VA and define the following:
 - a. Critical assets to be protected
 - b. DBT and its capabilities and motives
 - c. Response force capabilities and response time
 - d. Recommended security approach to reduce risk

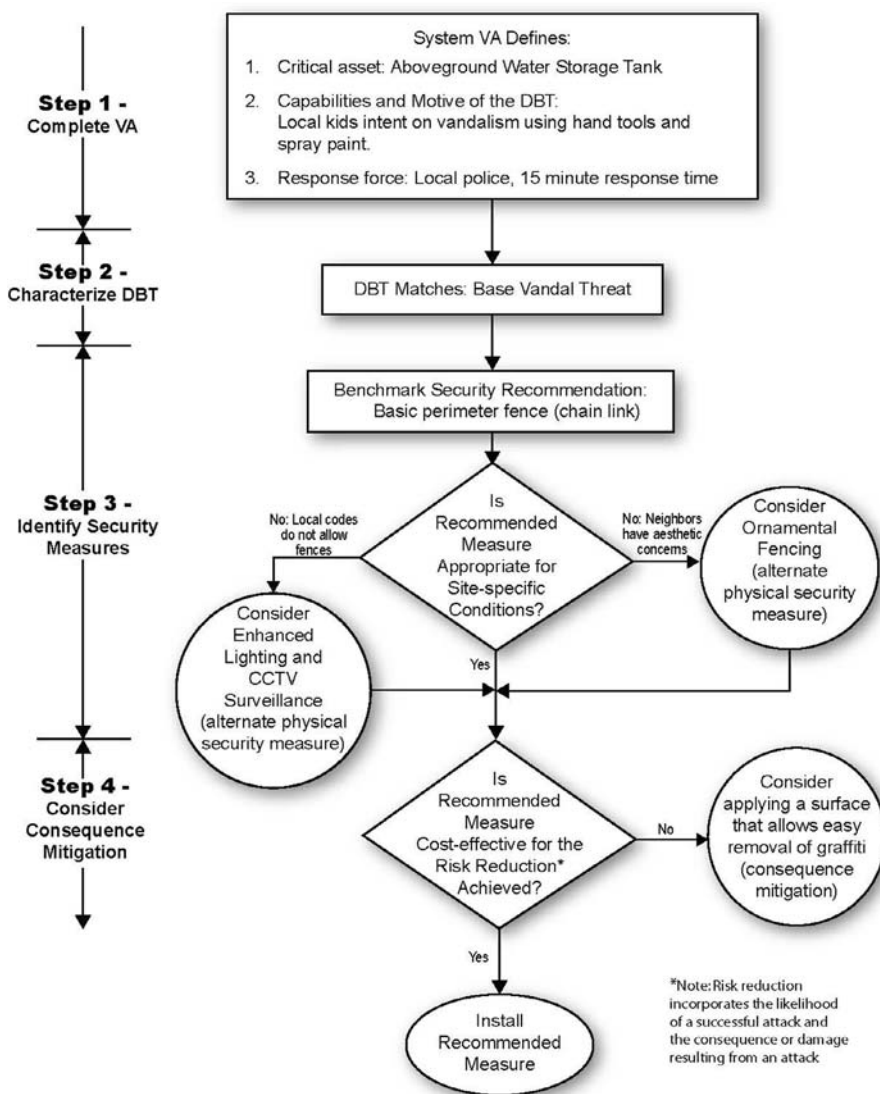


FIGURE 1-2. EXAMPLE DECISION TREE.
Source: ASCE/AWWA/WEF (2006).

2. Several methodologies have been developed to assist utilities in completing vulnerability assessments. These include:
 - a. Risk Assessment Methodology for Water Utilities (RAM-W) developed by Sandia National Laboratories in partnership with the former American Water Works Association Research Foundation, which is now the Water Research Foundation (Sandia Corporation 2002)
 - b. Vulnerability Self-Assessment Tool (VSAT) developed by the Association of Metropolitan Sewerage Agencies [AMSA, which is now known as the National Association of Clean Water Agencies (NACWA)] (NACWA 2005)
 - c. *Asset-Based Vulnerability Checklist for Wastewater Utilities*, produced by AMSA (NACWA 2002)
 - d. *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*, prepared by the Association of State Drinking Water Administrators (ASDWA) and the National Rural Water Association (NRWA) (ASDWA/NRWA 2002a, 2002b)
 - e. *Protecting Your Community's Assets: A Guide for Small Wastewater Systems* published by the National Environmental Training Center for Small Communities (NETCSC 2002)

The last three documents are suited primarily for small utilities with a limited number of assets.

1.2.1.2 Step 2: Characterize Design Basis Threat

1. Compare the DBT identified in the VA to the DBT levels described in Section 1.1.2. Select the appropriate DBT category (more than one may be selected): vandal, criminal, saboteur, or insider.
2. Within each of these DBT categories (refer to Table 1-1), determine whether the base level or enhanced level of security is appropriate.

1.2.1.3 Step 3: Identify Security Measures

1. Using the security measures table contained within the appropriate facility section of these guidelines, locate the column that applies to the selected DBT category at either the base level or the enhanced level to identify the recommended physical and electronic security measures. Ensure

that the appropriate level of protection is applied consistently to all elements of the facility to avoid any weak points.

2. Compare VA-recommended security approaches to the recommendations in the table and determine whether changes to the recommendations are warranted.
3. Deviations may be appropriate for a DBT that is defined differently (for example, with greater capabilities) from those presented in Section 1.1.2. Based on an analysis of the DBT's capabilities and the anticipated response time for an adequate response force, a utility may determine that it is necessary to apply the recommended enhanced-level measures plus additional security measures to provide a greater or more consistent level of security.
4. Deviations may also be appropriate based on specific site conditions or external requirements (for example, local ordinances, standards, or codes), the criticality of the asset, or the response time or capability of the responders. In these cases, the utility should consider alternate security measures that accomplish objectives similar to the measure recommended in the table. Where certain measures may be less desirable (such as barbed wire in a residential neighborhood), they may be offset by other measures (such as providing natural surveillance that may deter intruders averse to being caught in the act).

1.2.1.4 Step 4: Consider Consequence Mitigation

1. Consider the costs of the recommended security features and determine whether mitigation of the consequences is more cost-effective than applying the recommended security measures. A utility may wish to reduce the amount of physical hardening and electronic security (such as secure fencing, hardened doors and windows, CCTV cameras) that is applied if it is more feasible, reliable, and cost-effective to repair or replace a damaged asset. For example, a utility may decide to bypass a booster pumping station or use a portable pump located off-site in the event that a permanent pump is damaged, instead of implementing additional security measures.
2. As illustrated in Figure 1-3, a cost-risk reduction curve can be a useful tool in determining the point at which the

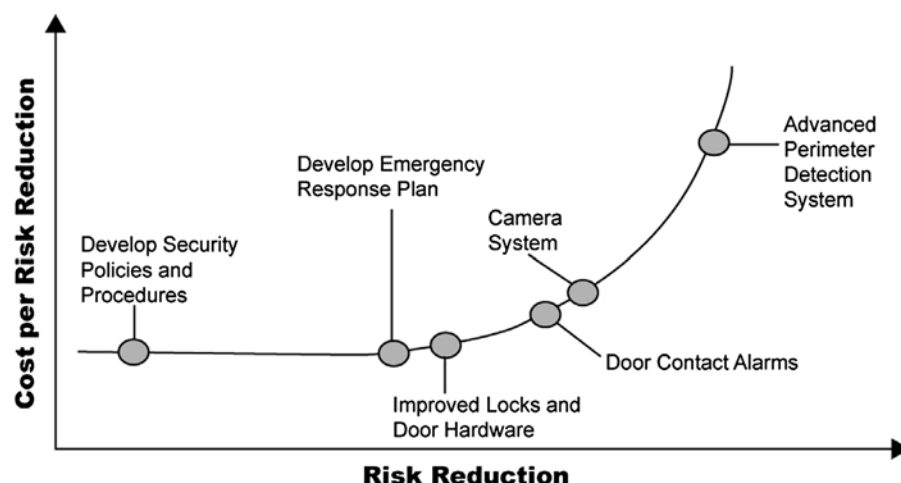


FIGURE 1-3. TYPICAL COST-TO-RISK REDUCTION CURVE.
Source: ASCE/AWWA/WEF (2004b).

risk reduction associated with implementing additional security measures is marginal (ASCE/AWWA/WEF 2004b). Management and operational measures to lower consequences are important elements of a utility or facility security plan that are not addressed in these guidelines.

1.2.2 Additional Information to Assist in Applying These Guidelines. The following sections provide additional information that will be helpful as the subsequent sections of these guidelines are reviewed and considered for implementation.

1.2.2.1 New and Existing Facilities. These guidelines can be applied to new and existing facilities. For new facilities, the VA to identify the key assets and appropriate DBT should be conducted during the early design phases, for example, during conceptual design, and should be consistent with the VA for the utility's other facilities. In addition to incorporating the appropriate security measures identified in these guidelines into the design, consideration should be given to using security-focused design approaches. Examples would include limiting routes of access to critical assets; selecting building materials that are less prone to vandalism or forced entry; arranging building orientations to provide visual site control; providing redundant critical assets; and locating redundant critical assets in nonadjacent areas.

Most of the security measures can be applied as retrofits to an existing facility. The exceptions are those measures that require minimum site dimensions to be effective (for example, double-layer fencing or set-back distances) or are dependent on other site-specific conditions (for example, landscaping or site lighting). In applying these guidelines to existing facilities, a utility should ensure that a consistent protection layer is achieved; for example, the delay capability of a pry- or break-resistant door added to a facility should match the resistance provided by the facility's other doors, windows, walls, and roof.

1.2.2.2 Local Codes and Required Aesthetics. The application of these guidelines needs to consider local codes,

ordinances, restrictive covenants, and aesthetic requirements. For example, local codes may limit the extent and intensity of site lighting. Required aesthetics may limit the height or material type of a fence, or it may not be appropriate to use a fence with outriggers and barbed wire for a facility that is located in a park-like or residential neighborhood setting.

1.2.2.3 Assets Not Under Utility Control. These guidelines apply only to assets that are within the control of the utility. For critical assets that are not owned by the utility, the utility needs to coordinate protection of the assets with their owners.

1.2.2.4 Balance of the System. Where multiple facilities are located in a single complex, consider the security measures needed for each type of facility and integrate the measures to provide the most effective approach.

1.2.2.5 Value of the Asset. The relative value of an asset or facility is determined through the VA process and may be contingent on perceived or actual monetary value, value to the process, value to the community, or potential consequences if out of service. A higher-value asset may warrant enhanced security measures when compared to a lower-value asset.

1.2.2.6 Levels of Security Measures. Each section of this document recommends security measures for base and enhanced levels in each DBT category that are deemed appropriate to a wide range of facility types. The choice between applying the base level or enhanced level of security depends upon the DBT, the criticality of the asset, and the response time and capability of the responders. It may be appropriate for a utility to apply security features in excess of those identified as enhanced. It may also be appropriate for a utility to apply alternative solutions to achieve a similar level of security for all facilities.

1.2.2.7 Response Time and Capabilities. If the anticipated response time is lengthy or if the response capability is low, additional security measures may be warranted.

Chapter 2

RAW WATER FACILITIES

2.1 SCOPE

This guideline covers raw water facilities that are components of a municipal drinking water system and are under the control of the utility. It is limited to surface raw water facilities: river and lake intakes; pipelines and canals that are used to convey raw water; valve vaults and control structures used on these transmission lines and structures; and other facilities upstream of the treatment plant. It does not include wells or pumping stations, as these facilities are addressed in Section 3.0, Wells and Pumping Stations. It also does not include chemical feed facilities; these are addressed in Section 4.0, Water Treatment Plants.

This section establishes benchmark physical and electronic security features for protecting raw water facilities from vandal, criminal, saboteur, and insider threats. Threats and malevolent acts of concern include damage or destruction of individual facilities, or introduction of a chemical, radiological, or biological agent that contaminates the water supply or renders the facilities unusable.

A dam is commonly a raw water facility that may be under the control of a utility. Large reservoir dams are not addressed in this guideline because destruction of dams is considered a terrorist activity and therefore is not within the capability of the DBTs addressed in this guideline. Dam appurtenances can be protected in a similar manner to other raw water appurtenances described herein. Small dams, including diversion dams, can be protected using the approaches outlined for other raw water facilities and, therefore, are addressed in this guideline.

2.2 FACILITY MISSION

The mission of this type of facility is to provide a supply of water to treatment plants. The facilities include storage reservoirs, basins, intakes, pipelines, and vaults (meter, valve, etc.). Generally, these facilities are not continuously staffed. They may be visited periodically by staff who check the facilities, perform maintenance activities, conduct raw water monitoring, and respond to alarms. The facilities are often isolated from the general public, although in some cases raw water impoundments and rivers are popular recreation areas. These facilities may vary greatly in size, from large raw water reservoirs covering many acres to smaller conveyance structures. The security strategy for a given facility may vary depending on its size. For example, installation of a continuous perimeter fence may not be feasible at facilities with large areas. In these cases, alternate security strategies should be employed.

2.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for raw water facilities includes equipment or systems to deter, detect, delay, and respond to a threat prior to an adversary achieving its objective, or mitigation of the consequences of a successful attack by the threat. The

equipment and systems for successful detection and delay of a threat should be matched to the capabilities of the DBT, which are usually established during a facility's VA. In addition, equipment and systems should be selected bearing in mind that the adversary must be adequately delayed until the utility's identified response force arrives.

DBTs considered in this guideline include vandals, criminals, saboteurs, and insiders. Characteristics and capabilities of the two levels of threats—base and enhanced—upon which the benchmark security measures in this guideline are based, are presented in Table 1-1, Design Basis Threat Capability Matrix. Threats with capabilities less than or greater than those identified in Table 1-1 require a less or more robust security system as appropriate. Physical security measures are recommended without regard to cost or other factors that may preclude their implementation.

Benchmark security measures for Deter, Delay, Detect, and Respond are provided in this guideline. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (ASCE/AWWA/WEF 2004c) and are not addressed here.

2.4 BENCHMARK SECURITY MEASURES

Table 2-1 establishes the benchmark measures for a recommended security system to deter a threat or detect and delay the threat until the appropriate response force arrives. If the threat includes more than one DBT, for example, an enhanced criminal and a base insider, the security system should include the recommended security measures for both threats. Recommended security measures for a specific DBT are indicated with a check mark (✓). A security measure without a check mark for a specific DBT indicates that either the security measure is not recommended or a more robust security measure is recommended. The security measures of Table 2-1 have been grouped into the following categories:

- Perimeter (reservoir impoundments, intake structures, raw water pumping stations, open channels)
- Site (area between perimeter and facility structures)
- Facility Structures
- Water Quality Monitoring
- Closed-Circuit Television—Alarm Assessment (fixed cameras)
- Closed-Circuit Television—Surveillance [pan-tilt-zoom (PTZ) cameras]
- Power and Wiring Systems
- Supervisory Control and Data Acquisition (SCADA)—Physical Security

Security decisions are site- and utility-specific, and the measures identified in the table are good practice options to be considered, not rules to be followed. Additionally, the measures presented in the table are for typical raw water facilities. Facilities with different attributes or threats with capabilities in excess of the descriptions in Table 1-1 may require additional measures.

robust security measures. Appendix A provides additional details on security measures (specific sections are referenced in Table 2-1 where applicable).

Special considerations may be warranted for:

- Large dams, because of their potential public safety implications and because they are not addressed within this guideline

- Raw water components that do not have redundancy, such as single raw water transmission pipelines
- Facilities with public access, such as intakes on rivers or impoundments
- Raw water intakes/supplies for systems without barriers, such as watersheds whose water is delivered to the public without filtration or typical treatment

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR RAW WATER FACILITIES (ASCE/AWWA/WEF 2006)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Perimeter (reservoir impoundments, intake structures, raw water pumping stations, open channels)											
Basic perimeter fencing or perimeter walls	●		✓								1.0, 1.1, 8.1
Enhanced climb- and cut-resistant fencing or walls	●			✓	✓	✓	✓	✓			1.2, 1.4, 1.5
Foundation enhancements for fencing to prevent tunneling	●						✓	✓			1.7
Bollards or vehicle barriers limiting vehicle access	●							✓			5.0
Intrusion detection at perimeter		●		✓		✓	✓	✓			1.6, 3.0, 7.0, 9.1, 9.2, 11.0
Key-locked entrance gate	●		✓		✓		✓		✓		2.1, 10.2
Entrance gate controlled by using access control system	●	●		✓		✓		✓		✓	2.2, 2.3, 10.3, 10.4, 10.5
Intercom and remotely controlled electronic gate lock for visitors	●	●		✓		✓		✓		✓	2.2, 2.3
Guardhouse and manned entrance gate to control site access	●	●						✓			
Perimeter site lighting		●	✓	✓	✓	✓	✓	✓			7.0
Gate entrance lighting		●		✓		✓	✓	✓			7.0 (4), (5), (6)
Hardened site openings larger than 96 in. ² (62,000 mm ²) in area (e.g., grates on culverts)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3
“No Trespassing” signage [every 50 ft (15 m)]			✓	✓	✓	✓	✓	✓			8.1
Site (area between perimeter and facility structures)											
Motion-activated lighting		●		✓		✓	✓	✓			7.0 (9)
Perimeter minimum clear zone distance	●	●		✓		✓	✓	✓			3.0
Second layer of basic fencing	●						✓			✓	1.0, 1.1
Enhanced second layer of fencing that is climb- and cut-resistant	●							✓			1.2,
Intrusion detection at second layer of fencing		●					✓	✓		✓	3.0, 7.0, 9.1, 9.2, 11.0
Foundation enhancements for second layer of fencing	●							✓			1.7
Bollards or vehicle barriers around critical exterior equipment	●			✓		✓	✓	✓			

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR RAW WATER FACILITIES (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Bollards or vehicle barriers limiting vehicle access to area within second layer of fencing	•							✓			5.0
Electronic access-controlled entrance gate for second fence	•	•						✓		✓	2.2, 2.3, 10.4
Signage, buoys and/or float lines to delineate no-entry zone around lake or river intakes	•			✓							
Transformer (outdoor)—locked protective barrier or cage	•			✓			✓	✓	✓		13.3
Generator (outdoor)—locked protective barrier or cage	•			✓		✓	✓	✓	✓		13.3
Switchgear/motor control center (outdoor)—locked protective cage	•			✓			✓	✓	✓		13.3
Landscaping that does not obscure building or other assets		•	✓	✓	✓	✓	✓	✓	✓	✓	1.6, 3.0 (3)
Manholes—locked with security fastener	•		✓	✓			✓	✓	✓		
Manholes—intrusion detection on lock	•	•		✓				✓		✓	
Facility Structures											
Locking caps for valve operator covers	•			✓			✓	✓	✓		
Vault (meter, valve, etc.) hatches—mechanically fastened or locked with shroud over lock	•		✓								10.2, 14.2
Vault (meter, valve, etc.) hatches—double hatch doors with shrouded lock	•			✓			✓		✓		10.2
Vault (meter, valve, etc.) hatches—double hatch doors with shrouded lock and intrusion detection	•	•						✓		✓	7.0, 9.1, 9.2, 10.2, 11.0
Protective grating or screen to shield open basins from objects that are thrown from outside the perimeter fence	•		✓	✓			✓	✓			
Industrial-type, tamper-resistant door hinges	•			✓	✓	✓	✓	✓			
Key-locked entrance door	•		✓		✓				✓		10.1, 10.2, 13.2 (6)
Exterior doors with status switch contact alarmed to security		•		✓		✓	✓	✓	✓	✓	8.2, 13.1
Electronic access-controlled entrance door	•	•		✓		✓	✓	✓		✓	10.1, 10.3, 10.4, 13.2
Automatic locking critical interior doors, with access control	•	•				✓	✓	✓	✓	✓	
Double entry system or secured lobby entry (mantrap)	•	•						✓			
Blast-resistant exterior doors ^b	•							✓			
Bollards or vehicle barriers protecting vehicle doors	•					✓		✓			5.0
Break-resistant glass	•		✓	✓	✓	✓	✓				

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR RAW WATER FACILITIES (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Blast-resistant windows ^b	•							✓			
Glass-break detection at windows		•		✓		✓	✓	✓			9.3
Interior motion detection		•				✓		✓	✓	✓	9.3
Grilles or other barriers at skylights and louvers over 96 in. ² (62,000 mm ²)	•			✓	✓		✓				13.3
Grilles or other barriers with intrusion detection at skylights and louvers over 96 in. ² (62,000 mm ²)	•	•				✓		✓		✓	
Locked roof hatches	•		✓	✓	✓		✓		✓		14.3
Locked roof hatches with intrusion alarm	•	•				✓		✓		✓	
Roof access ladder with locked shroud	•		✓	✓	✓		✓		✓		
Roof access ladder with locked shroud and intrusion alarm	•	•				✓		✓		✓	
Transformer (indoor)—locked protective barrier or cage	•						✓	✓	✓		13.4
Generator (indoor)—locked protective barrier or cage	•					✓	✓	✓	✓		13.4
Switchgear/motor control center (indoor)—locked protective cage	•						✓	✓	✓		13.4
Water Quality Monitoring											
On-line water quality monitoring		•					✓	✓		✓	15.0
Closed Circuit Television—Alarm Assessment (fixed cameras)											
CCTV—All facility exterior doors		•		✓		✓	✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Hatches, vaults		•		✓		✓	✓	✓		✓	11.0, 11.1, 11.2
Closed Circuit Television—Surveillance [pan-tilt-zoom (PTZ) cameras]											
CCTV—Main gate		•					✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Impoundment, immediate area near intake, open channels, similar facilities		•					✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Main entrance door		•					✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Site surveillance		•				✓	✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Interior protected areas		•					✓	✓	✓	✓	11.0, 11.1, 11.2
Power and Wiring Systems											
All electrical panels locked	•		✓	✓	✓	✓	✓	✓	✓		12.0
Backup power to security components (as indicated): UPS, typically	•	•		✓		✓	✓	✓	✓	✓	12.0 (5)
All electrical wiring in conduit	•		✓	✓	✓	✓	✓	✓	✓	✓	12.0 (1)
Redundant communication paths	•							✓		✓	
Electronically supervised security wiring	•			✓		✓	✓	✓	✓	✓	12.0 (2)
Redundant critical utility (power, natural gas, etc.) connections	•							✓		✓	

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR RAW WATER FACILITIES (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
SCADA—Physical Security											
Locked PLC/RTU enclosure(s)	●		✓	✓	✓	✓	✓	✓	✓		13.0
Tamper switch on enclosure(s)		●		✓		✓	✓	✓	✓	✓	12.1
All instrumentation wiring in conduit	●		✓	✓	✓	✓	✓	✓	✓	✓	12.0 (1)

^aMany of the security measures identified in this table may also provide deterrence.

^bBlast-resistant doors and glass are also bullet-resistant.

UPS, uninterruptible power supply; SCADA, supervisory control and data acquisition; PLC/RTU, programmable logic controller/remote terminal unit.

11

Downloaded from ascelibrary.org by University of Texas at Austin on 10/04/2014

Chapter 3

WELLS AND PUMPING STATIONS

3.1 SCOPE

This guideline covers water wells and pumping stations used within a water system. It establishes benchmark physical and electronic security features for protecting a well or a booster pumping station (referred to as “the facility” in this section) from vandal, criminal, saboteur, and insider threats. Threats and malevolent acts of concern include contamination of the aquifer or contamination of the water that enters the distribution system from a well or pumping facility, or damage or destruction of the pumping station equipment that creates a public health hazard or prevents transmission of water to the end user.

3.2 FACILITY MISSION

The mission of a well facility is to withdraw groundwater from an aquifer to be used as drinking water supply. Generally, operations and maintenance staff periodically visit these facilities to perform maintenance and inspection/monitoring activities or to respond to failure alarms. These facilities may be isolated from the general public or located in residential, park-like settings or in the midst of denser populated urban areas. Multiple wells can be found at one location, and well facilities are often co-located with storage tanks or other utility-owned infrastructure such as maintenance buildings.

The mission of a pumping station is to pump raw water to a treatment facility (an intake pumping station), or to lift potable water from a lower service zone to a higher zone. Pumping stations may be exposed or in buildings above grade or may be located in below-grade vaults. Their capacities may range from 1,000 gal/day (3.8 m³/day) to more than 1 million gal/day (>3,800 m³/day).

Wells and pumping stations have been grouped together in this guideline because they have similar components, staffing patterns, and types of locations, and thus can be protected in similar ways.

More detailed information on wells can be found in AWWA A100-06: *Water Wells* (AWWA 2006). More detailed information on pumping stations can be found in *Pumping Station Design* by Jones et al. (2005).

3.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for wells and pumping stations includes equipment or systems to deter, detect, delay, and respond to a threat prior to an adversary achieving its objective, or mitigation of the consequences of a successful attack by the threat. The equipment and systems for successful detection and delay of a threat should be matched to the capabilities of the DBT, which are usually established during a facility’s VA. In addition, equipment and systems should be selected bearing in mind that the adversary must be adequately delayed until the utility’s identified response force arrives.

DBTs considered in this guideline include vandals, criminals, saboteurs, and insiders. Characteristics and capabilities of the two levels of threats, base and enhanced, upon which the benchmark security measures in this section are based, are presented in Table 1-1, Design Basis Threat Capability Matrix. Threats with capabilities less than or greater than those identified in Table 1-1 require a less or more robust security system as appropriate. Physical security measures are recommended without regard to cost or other factors that may preclude their implementation.

Benchmark security measures for Deter, Delay, Detect, and Respond are provided in this section. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (ASCE/AWWA/WEF 2004c) and are not addressed here.

3.4 BENCHMARK SECURITY MEASURES

Table 3-1 establishes the benchmark measures for a recommended security system to deter a threat or detect and delay the threat until the appropriate response force arrives. If the threat includes more than one DBT, for example an enhanced criminal and a base insider, the security system should include the recommended security measures for both threats. Recommended security measures for a specific DBT are indicated with a check mark (✓). A security measure without a check mark for a specific DBT indicates that either the security measure is not recommended or a more robust security measure is recommended. The security measures of Table 3-1 have been grouped into the following categories:

- Perimeter
- Site (area between perimeter and enclosed facilities)
- Facility Structures
- Water Quality Monitoring
- Closed-Circuit Television—Alarm Assessment (fixed cameras)
- Closed-Circuit Television—Surveillance [pan-tilt-zoom (PTZ) cameras]
- Power and Wiring Systems
- Supervisory Control and Data Acquisition (SCADA)—Physical Security

Security decisions are site- and utility-specific, and the measures identified in the table are good practice options to be considered, not rules to follow. Additionally, the measures presented in the table are for typical well and pumping station facilities. Facilities with different attributes or threats with capabilities in excess of the descriptions in Table 1-1 may require additional or more robust security measures. Appendix A provides additional details on security measures (specific sections are referenced in Table 3-1 where applicable).

TABLE 3-1 BENCHMARK SECURITY MEASURES FOR WELLS AND PUMPING STATIONS (ASCE/AWWA/WEF 2006)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Perimeter											
Basic perimeter fencing or perimeter walls	●		✓								1.0, 1.1, 8.1
Enhanced climb- and cut-resistant fencing or walls	●			✓	✓	✓	✓	✓			1.2, 1.4, 1.5
Foundation enhancements for fencing to prevent tunneling	●						✓	✓			1.7
Bollards or vehicle barriers limiting vehicle access	●							✓			5.0
Intrusion detection at perimeter		●		✓		✓	✓	✓			1.6, 3.0, 7.0, 9.1, 9.2, 11.0
Key-locked entrance gate	●		✓		✓		✓		✓		2.1, 10.2
Electronic access-controlled entrance gate	●	●		✓		✓		✓		✓	2.2, 2.3, 10.3, 10.4, 10.5
Perimeter site lighting		●	✓	✓	✓	✓	✓	✓			7.0
Gate entrance lighting		●		✓		✓	✓	✓			7.0 (4), (5), (6)
Hardened site openings larger than 96 in. ² (62,000 mm ²) in area (e.g., grates on culverts)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3
“No Trespassing” signage [every 50 ft (15 m)]			✓	✓	✓	✓	✓	✓			8.1
Site (area between perimeter and enclosed facilities)											
Motion-activated lighting		●		✓		✓	✓	✓			7.0 (9)
Perimeter minimum clear zone distance	●	●		✓		✓	✓	✓			3.0
Second layer of basic fencing	●						✓			✓	1.0, 1.1
Enhanced second layer of fencing that is climb/ cut resistant	●							✓			1.2,
Intrusion detection at second layer of fencing		●					✓	✓		✓	3.0, 7.0, 9.1, 9.2, 11.0
Foundation enhancements for second layer of fencing	●						✓	✓			1.7
Bollards or vehicle barriers around critical exterior equipment	●			✓		✓	✓	✓			
Bollards or vehicle barriers limiting vehicle access to area within second layer of fencing	●							✓			5.0
Electronic access-controlled entrance gate for second fence	●	●					✓	✓		✓	2.2, 2.3, 10.4
Transformer (outdoor)—locked protective barrier or cage	●			✓			✓	✓	✓		13.3
Generator (outdoor)—locked protective barrier or cage	●			✓		✓	✓	✓	✓		13.3
Switchgear/motor control center (outdoor)—locked protective cage	●			✓			✓	✓	✓		13.3
Chemical storage and feed equipment (outdoor)—locked access	●			✓	✓		✓		✓		13.3, 17.0

TABLE 3-1 BENCHMARK SECURITY MEASURES FOR WELLS AND PUMPING STATIONS (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Chemical storage and feed equipment (outdoor)—locked access with intrusion detection	•	•				✓		✓		✓	13.3, 17.0
Landscaping that does not obscure building or other assets		•	✓	✓	✓	✓	✓	✓	✓	✓	1.6, 3.0 (3)
Manholes—locked with security fastener	•		✓	✓					✓		19.0
Manholes—intrusion detection on lock	•	•		✓				✓		✓	
Minimize exterior signage indicating the presence or locations of assets	•		✓	✓			✓	✓			
Facility Structures											
Locking cap on aboveground well casing	•		✓		✓		✓		✓		
Locking cap on air lines extending through well casing	•		✓		✓		✓		✓		
Protective cage around aboveground well casing and air lines	•			✓		✓		✓			
Locking cap on monitoring wells	•		✓		✓		✓		✓		
Protective cage around monitoring wells	•			✓		✓		✓			
Locking caps for valve operator covers	•			✓			✓	✓	✓		
Valve vault hatches—mechanically fastened or locked with shroud over lock	•		✓								10.2, 14.2
Valve vault hatches—double hatch doors with shrouded lock	•			✓			✓		✓		10.2
Valve vault hatches—double hatch doors with shrouded lock and intrusion detection	•	•						✓		✓	7.0, 9.1, 9.2, 10.2, 11.0
Industrial-type, tamper-resistant door hinges	•			✓	✓	✓	✓	✓			
Key-locked entrance door	•		✓		✓				✓		10.1, 10.2, 13.2 (6)
Exterior doors with status switch contact alarmed to security		•		✓		✓	✓	✓	✓	✓	9.4, 13.2
Electronic access-controlled entrance door	•	•		✓		✓	✓	✓		✓	10.1, 10.3, 10.4, 13.2
Automatic locking critical interior doors with access control	•	•				✓	✓	✓	✓	✓	10.1, 10.3, 10.4, 13.2
Double entry system or secured lobby entry (mantrap)	•	•						✓			
Blast-resistant exterior doors ^b	•							✓			
Bollards or vehicle barriers protecting vehicle doors	•					✓		✓			5.0
Break-resistant glass	•		✓	✓	✓	✓	✓				
Blast-resistant windows ^b	•							✓			

TABLE 3-1 BENCHMARK SECURITY MEASURES FOR WELLS AND PUMPING STATIONS (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Glass-break detection at windows		•		✓		✓	✓	✓			9.3
Interior motion detection		•				✓		✓	✓	✓	9.3
Grilles or other barriers at skylights and louvers over 96 in. ² (62,000 mm ²)	•			✓	✓		✓				13.3
Grilles or other barriers with intrusion detection at skylights and louvers over 96 in. ² (62,000 mm ²)	•	•				✓		✓		✓	14.1
Locked roof hatches	•		✓	✓	✓		✓		✓		14.3
Locked roof hatches with intrusion alarm	•	•				✓		✓		✓	
Roof access ladder with locked shroud	•		✓	✓	✓		✓		✓		
Roof access ladder with locked shroud and intrusion alarm	•	•				✓		✓		✓	
Transformer (indoor)—locked protective barrier or cage	•						✓	✓	✓		13.3
Generator (indoor)—locked protective barrier or cage	•					✓	✓	✓	✓		13.3
Switchgear/motor control center (indoor)—locked protective cage	•						✓	✓	✓		13.3
Chemical fill lines at building exterior—locked access	•			✓	✓		✓	✓	✓		17.0
Chemical fill lines at building exterior—locked access with intrusion detection	•	•				✓		✓		✓	
Chemical storage and feed equipment (indoor)—locked access	•			✓	✓		✓		✓		13.1
Chemical storage and feed equipment (indoor)—locked with intrusion detection	•	•				✓		✓		✓	10.1, 10.3, 10.4, 13.1
Water Quality Monitoring											
On-line water quality monitoring		•					✓	✓		✓	15.0
Closed Circuit Television—Alarm Assessment (fixed cameras)											
CCTV—All facility exterior doors		•		✓		✓	✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Hatches, vaults		•		✓		✓	✓	✓		✓	11.0, 11.1, 11.2
Closed Circuit Television—Surveillance (pan-tilt-zoom [PTZ] cameras)											
CCTV—Main gate		•					✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Main entrance door		•					✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Site surveillance		•				✓	✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Interior protected areas		•					✓	✓	✓	✓	11.0, 11.1, 11.2
Power and Wiring Systems											
All electrical panels locked	•		✓	✓	✓	✓	✓	✓	✓		12.0
Backup power to security components (as indicated): UPS, typically	•	•		✓		✓	✓	✓	✓	✓	12.0 (5)

TABLE 3-1 BENCHMARK SECURITY MEASURES FOR WELLS AND PUMPING STATIONS (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
All electrical wiring in conduit	•		✓	✓	✓	✓	✓	✓	✓	✓	12.0 (1)
Redundant communication paths	•							✓		✓	
Electronically supervised security wiring	•			✓		✓	✓	✓	✓	✓	12.0 (2)
Redundant critical utility (power, natural gas, etc.) connections	•							✓		✓	
SCADA—Physical Security											
Locked PLC/RTU enclosure(s)	•		✓	✓	✓	✓	✓	✓	✓		13.0
Tamper switch on enclosure(s)		•		✓		✓	✓	✓	✓	✓	12.1
All instrumentation wiring in conduit	•		✓	✓	✓	✓	✓	✓	✓	✓	12.0 (1)

^aMany of the security measures identified in this table may also provide deterrence.

^bBlast-resistant doors and glass are also bullet-resistant.

UPS, uninterruptible power supply; SCADA, supervisory control and data acquisition; PLC/RTU, programmable logic controller/remote terminal unit.

Downloaded from ASCE Library by University of Texas at Austin

Chapter 4

WATER TREATMENT PLANTS

4.1 SCOPE

This section of the guidelines covers water treatment plants used within a municipal drinking water system. It establishes benchmark physical and electronic security features for protecting a water treatment plant (referred to as “the facility” in this section) from vandal, criminal, saboteur, and insider threats. Threats and malevolent acts of concern include damage or destruction of individual treatment processes or equipment, or introduction of a chemical, radiological, or biological agent that contaminates the drinking water supply or renders the facilities unusable. Employee safety and public health concerns can be caused by the intentional release of hazardous chemicals or toxic gases, or by damaging ventilation and other life-safety control features. The potential for malevolent individuals to create intentional fire and explosive hazards may be additional concerns requiring security features.

4.2 FACILITY MISSION

The mission of this facility is to treat source water to drinking water standards. Water treatment plants may produce from 100,000 gal (380 m³) to 100 million gal (1,140,000 m³) per day, although there are smaller and larger plants in operation. The facilities to produce treated water include below-grade, ground-level, and elevated basins and tanks; buildings housing chemical systems; electrical and control systems; staff facilities; and clearwell storage facilities.

Large water treatment plants are routinely staffed on a continuous basis; small facilities are likely to be staffed only periodically to adjust treatment settings, perform maintenance activities, conduct process monitoring, and respond to failure alarms. Although often isolated from the general public, these facilities can be located in residential settings or in the midst of denser populated urban areas. Because of safety concerns, the public generally has no direct access.

More detailed information on specific functions and treatment processes is contained in *Water Treatment Plant Design* (AWWA/ASCE 2005).

4.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for water treatment plants includes equipment or systems to deter, detect, delay, and respond to a threat prior to an adversary achieving its objective, or mitigation of the consequences of a successful attack by the threat. The equipment and systems for successful detection and delay of a threat should be matched to the capabilities of the DBT, which are usually established during a facility’s VA. In addition, equipment and systems should be selected bearing in mind that the adversary must be adequately delayed until the utility’s identified response force arrives.

DBTs considered in this guideline include vandals, criminals, saboteurs, and insiders. Characteristics and capabilities of the two levels of threats—base and enhanced—upon which the

benchmark security measures in this guideline are based, are presented in Table 1-1, Design Basis Threat Capability Matrix. Threats with capabilities less than or greater than those identified in Table 1-1 require a less or more robust security system as appropriate. Physical security measures are recommended without regard to cost or other factors that may preclude their implementation.

Benchmark security measures for Deter, Delay, Detect, and Respond are provided in this guideline. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (ASCE/AWWA/WEF 2004c) and are not addressed here.

4.4 BENCHMARK SECURITY MEASURES

Table 4-1 establishes the benchmark measures for a recommended security system to deter a threat or detect and delay the threat until the appropriate response force arrives. If the threat includes more than one DBT, for example an enhanced criminal and a base insider, the security system should include the recommended security measures for both threats. Recommended security measures for a specific DBT are indicated with a check mark (✓). A security measure without a check mark for a specific DBT indicates that either the security measure is not recommended or a more robust security measure is recommended. The security measures of Table 4-1 have been grouped into the following categories:

- Perimeter
- Site (area between perimeter and facilities)
- Facility Structures
- Water Quality Monitoring
- Closed-Circuit Television—Alarm Assessment (fixed cameras)
- Closed-Circuit Television—Surveillance [pan-tilt-zoom (PTZ) cameras]
- Power and Wiring Systems
- Supervisory Control and Data Acquisition (SCADA)—Physical Security

Security decisions are site- and utility-specific, and the measures identified in the table are good practice options to be considered, not rules to follow. Additionally, the measures presented in the table are for typical water treatment plants. Facilities with different attributes or threats with capabilities in excess of the descriptions in Table 1-1 may require additional or more robust security measures. A water treatment facility may have chemical injection facilities downstream of clearwell storage to adjust and maintain the chemical attributes of the finished water. These chemical facilities (chemical supply lines and metering equipment) may be outside of the boundary of the water treatment plant campus, but should be treated using similar security measures to those recommended for the treatment plant perimeter and facilities. Appendix A provides additional details on

security measures (specific sections are referenced in Table 4-1 where applicable).

Special considerations should be provided for security of extremely critical assets or facilities such as in-plant pumping stations, main electrical switchgear, emergency generators, disinfection systems, or SCADA/security computer equipment. Special security considerations should also be provided for water treatment plants that store large volumes of hazardous or toxic chemicals, such as chlorine or ammonia gas. Extremely critical or hazardous assets may be the target of a DBT that is more capable than the DBT for the remainder of the water treatment plant; these critical assets may require additional security measures. Security approaches for these assets should be based on protection-in-depth principles, where multiple layers of security measures are employed around the critical assets to detect and delay the adversary. An example would be the security system

for protecting a chlorine gas disinfection system from an enhanced saboteur threat. This system might include a second fence within the confines of the perimeter fence surrounding only the chlorine storage and feed building and enclosing a minimum 100-ft (30-m), well-lighted clear zone between the second fence and storage facility. The fence system could include intrusion detection, vehicle crash barriers, and access-controlled gates with limited authorization rights. The disinfection building may be constructed of blast-resistant materials and include blast-resistant and access-controlled personnel and vehicle doors. A gas-scrubber system with the capacity to neutralize multiple containers of the hazardous gas should be considered. CCTV cameras could be used to assess the threat of intruders and monitor authorized personnel activities. Depending on site and response-force specifics, additional security measures may be warranted.

TABLE 4-1 BENCHMARK SECURITY MEASURES FOR WATER TREATMENT PLANTS (ASCE/AWWA/WEF 2006)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Perimeter											
Basic perimeter fencing or perimeter walls	●		✓								1.0, 1.1, 8.1
Enhanced climb- and cut-resistant fencing or walls	●			✓	✓	✓	✓	✓			1.2, 1.4, 1.5
Foundation enhancements for fencing to prevent tunneling	●						✓	✓			1.7
Bollards or vehicle barriers limiting vehicle access	●							✓			5.0
Intrusion detection at perimeter		●		✓		✓	✓	✓			1.6, 3.0, 7.0, 9.1, 9.2, 11.0
Key-locked entrance gate	●		✓		✓		✓		✓		2.1, 10.2
Electronic access-controlled entrance gate	●	●		✓		✓		✓		✓	2.2, 2.3, 10.3, 10.4, 10.5
Intercom and remotely controlled electronic gate lock for visitors	●	●		✓		✓		✓		✓	2.2, 2.3
Vehicle sallyport gate entrance for delivery vehicles	●	●				✓	✓	✓			4.0
Guardhouse and manned entrance gate to control site access	●	●						✓			
Perimeter site lighting		●	✓	✓	✓	✓	✓	✓			7.0
Gate entrance lighting		●		✓		✓	✓	✓			7.0 (4), (5), (6)
Hardened site openings larger than 96 in. ² (62,000 mm ²) in area (e.g., grates on culverts)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3
Provide separate visitor vehicular sign-in checkpoint.	●	●						✓			
“No Trespassing” signage [every 50 ft (15 m)]			✓	✓	✓	✓	✓	✓			8.1
Site (area between perimeter and facilities)											
Motion-activated lighting		●		✓		✓	✓	✓			7.0 (9)
Perimeter minimum clear zone distance	●	●		✓		✓	✓	✓			3.0

TABLE 4-1 BENCHMARK SECURITY MEASURES FOR WATER TREATMENT PLANTS (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Locate public or visitor parking as far away from the facility as practical, but at least 30 ft (9 m) away	•							✓			
Second layer of basic fencing	•						✓			✓	1.0, 1.1
Enhanced second layer of fencing that is climb/cut resistant	•							✓			1.2,
Intrusion detection at second layer of fencing		•					✓	✓		✓	3.0, 7.0, 9.1, 9.2, 11.0
Foundation enhancements for second layer of fencing	•						✓	✓			1.7
Bollards or vehicle barriers around critical exterior equipment	•			✓		✓	✓	✓			
Bollards or vehicle barriers limiting vehicle access to area within second layer of fencing	•							✓			5.0
Electronic access-controlled entrance gate for second fence	•	•					✓	✓		✓	2.2, 2.3, 10.4
Transformer (outdoor)—locked protective barrier or cage	•			✓			✓	✓	✓		13.3
Generator (outdoor)—locked protective barrier or cage	•			✓		✓	✓	✓	✓		13.3
Switchgear/motor control center (outdoor)—locked protective cage	•			✓			✓	✓	✓		13.3
Chemical storage and feed equipment (outdoor)—locked access	•			✓	✓		✓		✓		13.3, 17.0
Chemical storage and feed equipment (outdoor)—locked access with intrusion detection	•	•				✓		✓		✓	13.3, 17.0
Landscaping that does not obscure building or other assets		•	✓	✓	✓	✓	✓	✓	✓	✓	1.6, 3.0 (3)
Manholes—locked with security fastener	•		✓	✓			✓	✓	✓		
Manholes—intrusion detection on lock	•	•		✓				✓		✓	
Minimize exterior signage indicating the presence or locations of assets	•		✓	✓			✓	✓			
Facility Structures											
Locking caps for valve operator covers	•			✓			✓	✓	✓		
Valve vault hatches—mechanically fastened or locked with shroud over lock	•		✓								10.2, 14.2
Valve vault hatches—double hatch doors with shrouded lock	•			✓			✓		✓		10.2
Valve vault hatches—double hatch doors with shrouded lock and intrusion detection	•	•						✓		✓	7.0, 9.1, 9.2, 10.2, 11.0

TABLE 4-1 BENCHMARK SECURITY MEASURES FOR WATER TREATMENT PLANTS (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Clearwell hatch/manway—hardened lock with shroud or mechanically fastened	•		✓								8
Clearwell hatch/manway—double layer doors with shrouded lock	•			✓			✓		✓		8
Clearwell hatch/manway—double layer doors with shrouded lock and intrusion detection	•	•						✓		✓	8
Clearwell vent: gooseneck pipe type—use double screen	•		✓								8
Clearwell vent: rectangular or circle (larger than pipe)—single layer with shrouded lock	•		✓								8
Clearwell vent: rectangular or circle (larger than pipe)—double layer with shrouded lock	•			✓			✓		✓		8
Clearwell vent: rectangular or circle (larger than pipe)—double layer with shrouded lock and intrusion alarm	•	•						✓		✓	8
Overflow outlet for clearwell: screen and/or flap valve with cage	•		✓	✓			✓				
Overflow outlet for clearwell: screen and/or flap valve with cage and intrusion detection	•	•						✓		✓	
Intrusion detection on top of clearwell or clearwell area		•		✓				✓		✓	4
Access ladder for clearwell—locked shroud	•		✓	✓			✓		✓		5.2
Access ladder for clearwell—locked shroud with intrusion alarm	•	•		✓				✓		✓	5.2
Remote clearwell isolation by means of automated valve	•						✓	✓		✓	
Protective grating or screen to shield open basins from objects that are thrown from outside the perimeter fence	•		✓	✓			✓	✓			
Industrial-type, tamper-resistant door hinges	•			✓	✓	✓	✓	✓			
Key-locked entrance door	•		✓		✓				✓		10.1, 10.2, 13.1
Exterior doors with status switch contact alarmed to security		•		✓		✓	✓	✓	✓	✓	9.4, 13.2
Electronic access-controlled entrance door	•	•		✓		✓	✓	✓	✓	✓	10.1, 10.3, 10.4, 13.1
Automatic locking critical interior doors with access control	•	•				✓	✓	✓	✓	✓	10.1, 10.3, 10.4
Double entry system or secured lobby entry (mantrap)	•	•						✓			
Visitor waiting area	•	•				✓		✓			



TABLE 4-1 BENCHMARK SECURITY MEASURES FOR WATER TREATMENT PLANTS (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Blast-resistant exterior doors ^b	•							✓			
Bollards or vehicle barriers protecting vehicle doors	•					✓		✓			5.0
Break-resistant glass	•		✓	✓	✓	✓	✓				
Blast-resistant windows ^b	•							✓			
Glass-break detection at windows		•		✓		✓	✓	✓			9.3.1
Interior motion detection		•				✓		✓	✓	✓	9.3
Grilles or other barriers at skylights and louvers over 96 in. ² (62,000 mm ²)	•			✓	✓		✓				13.3
Grilles or other barriers with intrusion detection at skylights and louvers over 96 in. ² (62,000 mm ²)	•	•				✓		✓		✓	14.1
Locked roof hatches	•		✓	✓	✓		✓		✓		
Locked roof hatches with intrusion alarm	•	•				✓		✓		✓	
Roof access ladder with locked shroud	•		✓	✓	✓		✓		✓		
Roof access ladder with locked shroud and intrusion alarm	•	•				✓		✓		✓	
Transformer (indoor)—locked protective barrier or cage	•						✓	✓	✓		13.3
Generator (indoor)—locked protective barrier or cage	•					✓	✓	✓	✓		13.3
Switchgear/motor control center (indoor)—locked protective cage	•						✓	✓	✓		13.3
Chemical fill lines at building exterior—locked access	•			✓	✓		✓	✓	✓		17.0
Chemical fill lines at building exterior—locked access with intrusion detection	•	•				✓		✓		✓	
Chemical storage and feed equipment (indoor)—locked access	•				✓		✓		✓		13.1
Chemical storage and feed equipment (indoor)—locked with intrusion detection	•	•				✓		✓		✓	10.1, 10.3, 10.4, 13.1
Water Quality Monitoring											
On-line water quality monitoring		•					✓	✓		✓	15.0
Closed Circuit Television—Alarm Assessment (fixed cameras)											
CCTV—All facility exterior doors		•		✓		✓	✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Hatches, vaults		•		✓		✓	✓	✓		✓	11.0, 11.1, 11.2
Closed Circuit Television—Surveillance (pan-tilt-zoom [PTZ] cameras)											
CCTV—Main gate		•					✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Main entrance door		•					✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Site surveillance		•				✓	✓	✓	✓	✓	11.0, 11.1, 11.2
CCTV—Interior protected areas		•					✓	✓	✓	✓	11.0, 11.1, 11.2

TABLE 4-1 BENCHMARK SECURITY MEASURES FOR WATER TREATMENT PLANTS (ASCE/AWWA/WEF 2006) (continued)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Power and Wiring Systems											
All electrical panels locked	●		✓	✓	✓	✓	✓	✓	✓		12.0
Backup power to security components (as indicated): UPS, typically	●	●		✓		✓	✓	✓	✓	✓	12.0 (5)
All electrical wiring in conduit	●		✓	✓	✓	✓	✓	✓	✓	✓	12.0 (1)
Redundant communication paths	●							✓		✓	
Electronically supervised security wiring	●			✓		✓	✓	✓	✓	✓	12.0 (2)
Redundant critical utility (power, natural gas, etc.) connections	●							✓		✓	
SCADA—Physical Security											
Locked PLC/RTU enclosure(s)	●		✓	✓	✓	✓	✓	✓	✓		13.0
Tamper switch on enclosure(s)		●		✓		✓	✓	✓	✓	✓	12.1
All instrumentation wiring in conduit	●		✓	✓	✓	✓	✓	✓	✓	✓	12.0 (1)

^aMany of the security measures identified in this table may also provide deterrence.

^bBlast-resistant doors and glass are also bullet-resistant.

UPS, uninterruptible power supply; SCADA, supervisory control and data acquisition; PLC/RTU, programmable logic controller/remote terminal unit.

Chapter 5

FINISHED WATER STORAGE FACILITIES

5.1 SCOPE

This section of the guidelines covers water storage tanks and finished water reservoirs used within a potable water distribution system. It establishes benchmark physical and electronic security features for protecting a storage tank or reservoir (referred to as “the facility” in this section) from vandal, criminal, saboteur, and insider threats. The malevolent act of greatest concern is the intentional contamination of the drinking water with a toxic agent. A similar, related concern is contamination with a foreign substance that does not cause health effects, such as a dye, but does create a loss of confidence or even panic among the utility’s customers. Other concerns include destruction or damage to the tank or reservoir and related appurtenances so that it cannot serve its intended purpose, or destruction or damage such that a rapid release of the stored water causes property damage and possibly harm to people living near the tank or reservoir.

5.2 FACILITY MISSION

The mission of this facility is to store potable water for distribution to customers. Storage is needed to meet daily flow fluctuations, for fire fighting, and for emergencies. Three types of potable water storage are typically employed in the water industry: aboveground water storage tanks, elevated tanks, and covered reservoirs. Aboveground water storage tanks are constructed of concrete, steel, fiberglass-reinforced plastic (FRP), or wood with the tank floor situated at grade (that is, it is not an elevated tank on columns). The diameter and height of this type of tank will vary depending on volume requirements. Elevated tanks are typically of steel construction with the tank itself perched on steel legs. The tank is accessible via a ladder or system of ladders. Covered finished water reservoirs may be slightly larger and are often constructed below grade but with access and vents at or above grade.

Usually, these facilities are not staffed, and operations and maintenance personnel visit the sites infrequently to perform maintenance activities or to respond to failure alarms. The tanks and reservoirs are often located in residential, park-like settings or in the midst of more densely populated urban areas where the public has access to the base of the tank. In other cases, the tanks are isolated from general public access. Potable water storage facilities at more remote locations within a distribution system may be provided with chemical facilities (chlorine and/or ammonia) to maintain the chemical attributes of finished water as it progresses through the distribution system. Measures to address chemical facilities are presented in Section 4.0, Water Treatment Plants, and are not included here.

AWWA Manual M42, *Steel Water-Storage Tanks* (AWWA 1998) and D100-05: *Welded Carbon Steel Tanks for Water Storage* (AWWA 2005) provide additional information on the design and function of steel water storage tanks. Concrete tank standards and information are provided in AWWA D110-04: *Wire- and Strand-Wound, Circular, Prestressed Concrete Water Tanks* (AWWA 2004), AWWA D115-95: *Circular Prestressed*

Concrete Water Tanks with Circumferential Tendons (AWWA 1995), and the American Concrete Institute’s (ACI) 371R-98 *Guide for the Analysis, Design, and Construction of Concrete-Pedestal Water Towers* (ACI 1998). FRP tanks are covered in AWWA D120-02: *Thermosetting Fiberglass-Reinforced Plastic Tanks* (AWWA 2002).

5.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for water storage facilities includes equipment or systems to deter, detect, delay, and respond to a threat prior to an adversary achieving its objective, or mitigation of the consequences of a successful attack by the threat. The equipment and systems for successful detection and delay of a threat should be matched to the capabilities of the DBT, which are usually established during a facility’s VA. In addition, equipment and systems should be selected bearing in mind that the adversary must be adequately delayed until the utility’s identified response force arrives.

DBTs considered in this section include vandals, criminals, saboteurs, and insiders. Characteristics and capabilities of the two levels of threats—base and enhanced—upon which the benchmark security measures in this section are based, are presented in Table 1-1, Design Basis Threat Capability Matrix. Threats with capabilities less than or greater than those identified in Table 1-1 require a less or more robust security system as appropriate. Physical security measures are recommended without regard to cost or other factors that may preclude their implementation.

Benchmark security measures for Deter, Delay, Detect, and Respond are provided in this section. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (ASCE/AWWA/WEF 2004c) and are not addressed here.

5.4 BENCHMARK SECURITY MEASURES

Table 5-1 establishes the benchmark measures for a recommended security system to deter a threat or detect and delay the threat until the appropriate response force arrives. If the threat includes more than one DBT, for example, an enhanced criminal and a base insider, the security system should include the recommended security measures for both threats. Recommended security measures for a specific DBT are indicated with a check mark (✓) in the table. A security measure without a check mark for a specific DBT indicates that either the security measure is not recommended or a more robust security measure is recommended. The security measures of Table 5-1 have been grouped into the following categories:

- Perimeter
- Site (area between perimeter and facilities)
- Facility Structures
- Closed-Circuit Television—Alarm Assessment (fixed cameras)

- Closed-Circuit Television—Surveillance [pan-tilt-zoom (PTZ) cameras]
- Power and Wiring Systems
- Supervisory Control and Data Acquisition (SCADA)—Physical Security

Security decisions are site- and utility-specific, and the measures identified in the table are good practice options to be

considered, not rules to follow. Additionally, the measures presented in the table are for typical water storage facilities. Storage tanks with different attributes or threats with capabilities in excess of the descriptions in Table 1-1 may require additional or more robust security measures. Appendix A provides additional details on security measures (specific sections are referenced in Table 5-1 where applicable).

TABLE 5-1 BENCHMARK SECURITY MEASURES FOR FINISHED WATER STORAGE FACILITIES (ASCE/AWWA/WEF 2006)

Security Measure	System Objective ^a		Vandals		Criminals		Saboteurs		Insiders		Applicable Sections in Appendix A, Physical Security Elements
	Delay	Detection	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	Base Level	Enhanced Level	
Perimeter											
Basic perimeter fencing or perimeter walls	●		✓								1.0, 1.1, 8.1
Enhanced climb/cut-resistant fencing	●			✓	✓	✓	✓	✓			1.2
Foundation enhancements for fencing to prevent tunneling	●						✓	✓			1.7
Bollards or vehicle barriers limiting vehicle access	●							✓			5.0
Intrusion detection at perimeter		●		✓		✓	✓	✓			1.6, 3.0, 7.0, 9.1, 9.2, 11.0
Key-locked entrance gate	●		✓		✓		✓		✓		2.1, 10.2
Electronic access-controlled entrance gate	●	●		✓		✓		✓		✓	2.2, 2.3, 10.4
Perimeter site lighting		●	✓	✓	✓	✓	✓	✓			7.0
Gate entrance lighting		●		✓		✓	✓	✓			7.0 (4), (5), (6)
Hardened site openings larger than 96 in. ² (62,000 mm ²) in area (e.g., grates on vents)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3
“No Trespassing” signage [every 50 ft (15 m)]			✓	✓	✓	✓	✓	✓			8.1
Site (area between perimeter and facilities)											
Motion-activated lighting		●		✓		✓	✓	✓			7.0 (9)
Perimeter minimum clear zone distance	●	●		✓		✓	✓	✓			3.0
Locate public or visitor parking as far away from facility as practical, but at least 30 ft (9 m) away	●							✓			
Second layer of basic fencing	●						✓			✓	1.0, 1.1
Enhanced second layer of fencing that is climb/cut resistant	●							✓			1.2
Intrusion detection at second layer of fencing		●					✓	✓		✓	3.0, 7.0, 9.1, 9.2, 11.0
Foundation enhancements for second layer of fencing	●						✓	✓			1.7
Bollards or vehicle barriers around critical exterior equipment	●			✓		✓	✓	✓			
Bollards or vehicle barriers limiting vehicle access to area within second layer of fencing	●							✓			5.0
Electronic access-controlled entrance gate for second fence	●	●					✓	✓		✓	2.2, 2.3, 10.4