

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

ASCE STANDARD

ANSI/ASCE/EWRI 56-10

ANSI/ASCE/EWRI 57-10

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.



**ENVIRONMENTAL &
WATER RESOURCES
INSTITUTE**

Published by the American Society of Civil Engineers

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

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

CONTENTS

FOREWORD	Page 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

This page intentionally left blank

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. Mc Laughlin, 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

This page intentionally left blank

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

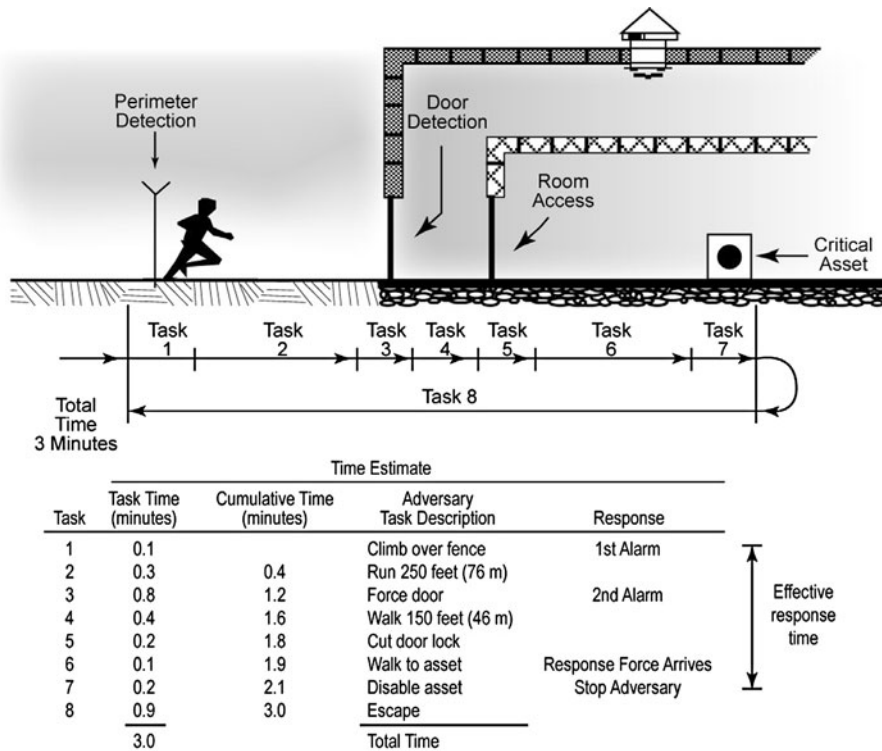


FIGURE 1-1. CONCEPT OF DELAY CALCULATION.
Source: Adapted from Garcia (2001), with permission. © Elsevier.

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 to ensure that

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

Characteristic	Vandal		Criminal		Saboteur		Insider ^a	
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	
	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced
Planning/system knowledge	Little or none	Possible	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-automatic weapons, 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, crowbars), 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

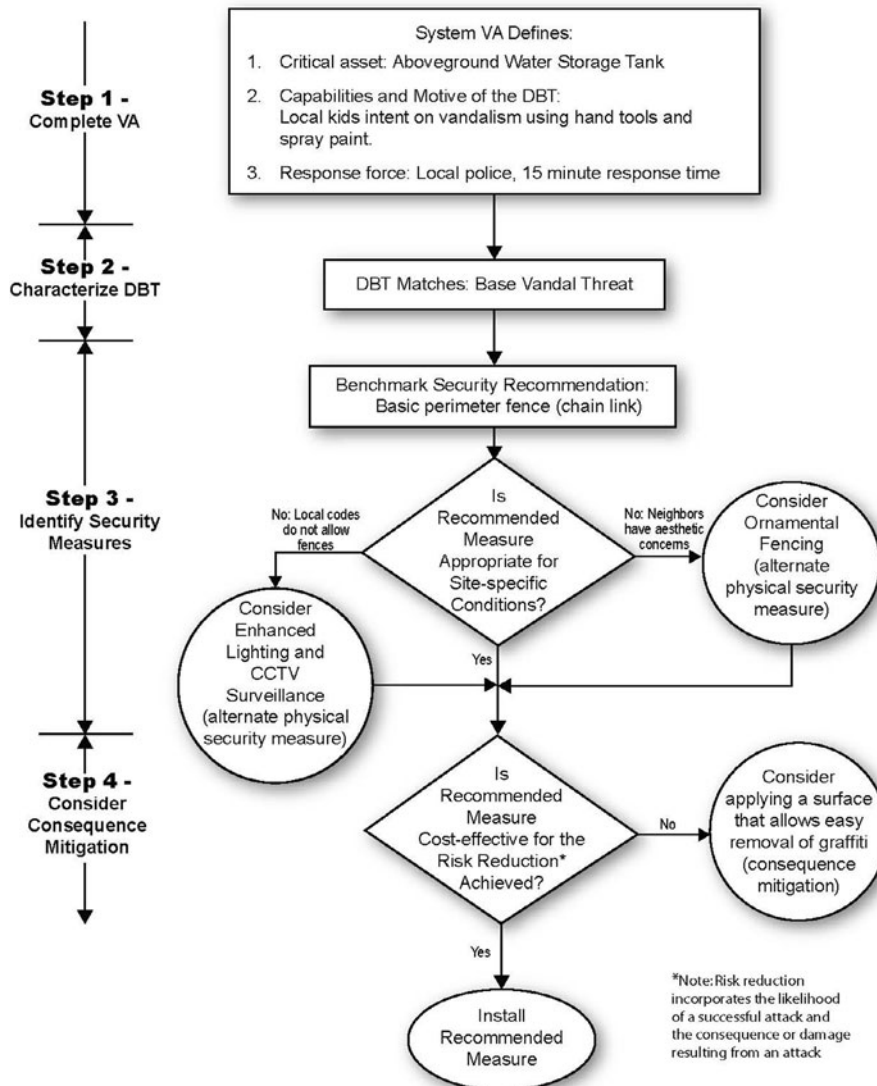


FIGURE 1-2. EXAMPLE DECISION TREE.
Source: ASCE/AWWA/WEF (2006).

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

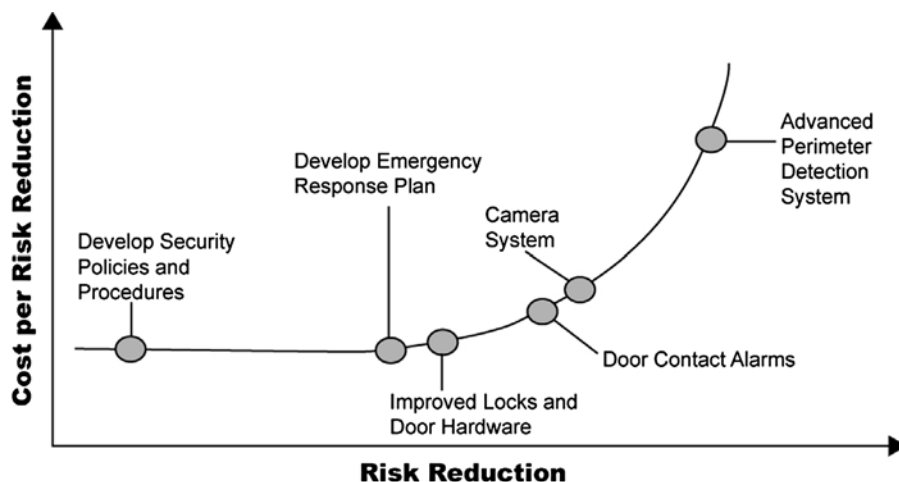


FIGURE 1-3. TYPICAL COST-TO-RISK REDUCTION CURVE.
Source: ASCE/AWWA/WEF (2004b).

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 or more

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.

This page intentionally left blank

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.

This page intentionally left blank

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

TABLE 5-1 BENCHMARK SECURITY MEASURES FOR FINISHED WATER STORAGE 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	
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 tank 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 layer doors with shrouded lock and intrusion detection	•	•						✓		✓	7.0, 9.1, 9.2, 10.2, 11.0
Tank hatch/manway—mechanically fastened or locked with shroud over lock	•		✓								10.2
Tank hatch/manway—double layer doors with shrouded lock	•			✓			✓		✓		10.2
Tank hatch/manway—double layer doors with shrouded lock and intrusion detection	•	•						✓		✓	7.0, 9.1, 9.2, 10.2, 11.0
Tank vent: gooseneck pipe type—double screen	•		✓								
Tank vent: rectangular or circle (larger than pipe)—single layer shroud, locked	•		✓								10.2, 14.1, 14.3
Tank vent: rectangular or circle (larger than pipe)—double layer with shrouded lock	•			✓			✓		✓		10.2, 14.1, 14.3
Tank vent: rectangular or circle (larger than pipe)—double layer with shrouded lock and intrusion alarm	•	•						✓		✓	7.0, 9.1, 9.2, 10.2, 11.0, 14.1, 14.3

TABLE 5-1 BENCHMARK SECURITY MEASURES FOR FINISHED WATER STORAGE 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	
Overflow outlet: 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 tank or tank area		•		✓				✓		✓	7.0, 9.1, 9.2, 11.0
Access ladder—locked shroud	•		✓	✓			✓		✓		
Access ladder—locked shroud with intrusion alarm	•	•		✓				✓		✓	7.0, 9.1, 9.2, 11.0
Remote reservoir isolation by means of automated valve	•						✓	✓		✓	
Protective grating or screen to shield open basins from objects that are thrown from outside the fence	•		✓	✓			✓	✓			
Transformer—locked protective barrier or cage	•						✓	✓	✓		13.1, 13.3
Generator—locked protective barrier or cage	•					✓	✓	✓	✓		13.1, 13.3
Switchgear/motor control center—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											
Online 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, ladder guards		•		✓		✓	✓	✓		✓	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 5-1 BENCHMARK SECURITY MEASURES FOR FINISHED WATER STORAGE 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	
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.

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

This page intentionally left blank

Chapter 6

WATER DISTRIBUTION SYSTEMS

6.1 SCOPE

This section of the guidelines covers the water distribution system component of municipal drinking water systems. It establishes benchmark physical and electronic security features for protecting a water distribution system from vandal, criminal, saboteur, and insider threats. Threats and malevolent acts of concern include damage or destruction of individual facilities or equipment, or introduction of a chemical or biological agent that contaminates the drinking water supply.

6.2 SYSTEM MISSION

The mission of these systems is to distribute drinking water to the customers of the system. Water distribution systems may range up to many square miles (kilometers) in area. They include pipelines, isolation and control valves, hydrants, customer meters, backflow valves, air release valves, pressure-reducing valves, small chemical storage and injection facilities, and related items (Mays 2000). As the name suggests, these facilities are distributed throughout the community that is served by the water system and rarely have defined facility perimeters. Most pipelines and valves are buried and therefore are out of sight of the public. However, appurtenances and the structures enclosing them, such as air valve vaults and the like, are sometimes aboveground and visible. Furthermore, every customer has a direct connection to the system through their service line. Other sections of these guidelines cover finished water storage facilities, pumping stations, and chemical facilities (refer to Section 4.0 for chemical facilities).

6.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for water distribution systems 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, including hydraulic isolation of potentially contaminated sections of the distribution system, are presented in the *Interim Voluntary Security Guidance for Water Utilities* (ASCE/AWWA/WEF 2004c) and are not addressed here.

Because distribution systems are so expansive and include so many assets, utilities may need to conduct evaluations that are in addition to their VAs to identify the most critical facilities and locations within their distribution systems. These evaluations may include extended-period simulation hydraulic modeling to determine the potential water quality impacts of a contamination event and where to focus security measures to minimize risk.

As of the publication of this document, research was ongoing with respect to developing online contaminant monitoring instruments. As these instruments are improved, they will become a more integral part of physical security systems for distribution systems. Refer to the *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System* (ASCE/AWWA/WEF 2004a) and to regular updates on the USEPA Web site for information on the topic of online contaminant monitoring.

6.4 BENCHMARK SECURITY MEASURES

Table 6-1 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 6-1 have been grouped into the following categories:

- System Structures
- Water Quality Monitoring
- 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 distribution systems. 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 6-1 where applicable).

Water distribution systems present challenges in developing adequate detection and delay approaches, as many facilities are not constructed with defined perimeters or site areas and are frequently accessible to the public. Aboveground pipelines, manholes, and vaults where access to pipelines can be accomplished are of special concern. Based on the results of the VA and subsequent evaluations described in the previous sections, utilities

may elect to apply these security measures on a subset of their assets in the most critical locations. For example, the recommendations for valves may be applied to only the most critical valves, rather than every valve in the distribution system. Additional information on water distribution system security can be found in Murphy et al. (2005).

TABLE 6-1 BENCHMARK SECURITY MEASURES FOR DISTRIBUTION SYSTEMS (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	
System Structures											
Bollards or vehicle barriers around critical exposed equipment	•			✓		✓	✓	✓			
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
Provide locking devices for contractor’s temporary connections	•			✓			✓	✓			
Use unidirectional customer meters to reduce backflow potential	•						✓	✓			
Exposed pipelines: provide fence barrier to limit access to appurtenances	•			✓			✓				
Exposed pipelines: provide fence barrier to limit access to appurtenances and include detection	•	•						✓			
Locking covers for control, pressure-reducing, air-relief, and other valves	•		✓			✓	✓		✓		
Locking covers with detection for control, pressure-reducing, air-relief, and other valves	•	•		✓				✓		✓	
Locking cover for sampling stations	•		✓				✓		✓		
Locking cover with detection for sampling stations	•	•						✓			
Hydrants: provide tamper seals, check valve, locking mechanisms, or cross-connection protection	•			✓		✓		✓			18.0
Backflow prevention valves or tamper switches installed on connections to multifamily residential connections and commercial facilities (e.g., motels)	•							✓			

TABLE 6-1 BENCHMARK SECURITY MEASURES FOR DISTRIBUTION SYSTEMS (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	
Backflow valves to limit potential for reverse flow at interconnections to neighboring water systems, wholesale customers, or customer connections to industrial facilities	•						✓	✓			
Water Quality Monitoring											
Online water quality monitoring		•					✓	✓	✓	✓	15.0
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.

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

This page intentionally left blank

Chapter 7

WATER SYSTEM SUPPORT FACILITIES

7.1 SCOPE

This section presents a guideline for security for support facilities that are part of municipal drinking water systems. It establishes benchmark physical and electronic security features for protecting water support facilities from vandal, criminal, saboteur, and insider threats. Threats and malevolent acts of concern include damage or destruction of individual facilities.

7.2 FACILITY MISSION

Water system support facilities include administrative buildings, maintenance yards, sites for material and vehicle storage, and laboratories. The common element linking these facilities is that they may not be in direct contact with the drinking water. If a facility such as a laboratory or storage yard is located at a water treatment plant, then the security guideline for water treatment plants should be referenced. This guideline applies to those facilities that are not located at a water treatment plant, water pumping station, or intake facility, or otherwise in direct contact with the potable water. Because support facilities may be located apart from the water flow, they have a low risk for being avenues of intentional contamination of the water supply.

Support facilities may also have the following common factors that are often different from other water system facilities:

- Large number of people entering and leaving the facility, including the public
- High vehicle traffic
- Fuel tanks to supply the utility fleet
- May provide storage for utility vehicles which, as moving assets, present unique challenges
- In the case of laboratories, may house chemicals or even pathogens that are used in tests
- May be symbolic of the utility's image, such as a headquarters facility
- May be combined with other government facilities, such as an administrative facility within the city hall or a maintenance yard combined with other city maintenance functions

The assets in a support facility may include maps, SCADA/controls, reports, cash, business systems, heavy and mobile equipment, laboratory equipment and chemicals, and tools.

7.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for water support 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.

7.4 BENCHMARK SECURITY MEASURES

Table 7-1 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 7-1 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
- SCADA—Physical Security
- May include storage of chemicals

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 support 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 7-1 where applicable).

Special considerations should be provided for security of extremely critical assets or facilities such as water quality labs, SCADA, emergency operation centers (EOCs), centralized security monitoring centers, security equipment, network computer servers, hubs and related systems, and dangerous

chemicals and pathogens located in analytical laboratories. Special consideration should also be provided for sites that have an intended public open space/access focus, such as headquarters complexes.

TABLE 7-1 BENCHMARK SECURITY MEASURES FOR WATER SYSTEM SUPPORT 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- 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
Minimize vehicle access points and/or number of entrance gates	●	●			✓	✓	✓	✓			
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
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
Public or visitor parking located as far away from the facility as practical, but at least 30 ft (9 m) away	●							✓			
Eliminate parking underneath facilities	●							✓			
Second layer of basic fencing	●						✓			✓	1.0, 1.1
Enhanced second layer of fencing that is climb- and cut-resistant	●							✓			1.2

TABLE 7-1 BENCHMARK SECURITY MEASURES FOR WATER SYSTEM SUPPORT 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	
Intrusion detection at second layer of fencing		•					✓	✓		✓	1.6, 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	•	•				✓		✓		✓	
Fuel storage tanks—locate at least 100 ft (30 m) from all buildings and away from perimeter fence lines	•						✓	✓			
Landscaping that does not obscure building or other assets		•	✓	✓	✓	✓	✓	✓	✓	✓	1.6, 3.0 (3)
Minimize exterior signage indicating the presence or locations of assets	•		✓	✓			✓	✓			
Facility Structures											
Industrial-type, tamper-resistant door hinges	•			✓	✓	✓	✓	✓			
Key-locked entrance door	•		✓		✓				✓		
Exterior doors with status switch contact alarmed to security		•		✓		✓	✓	✓	✓	✓	9.4, 13.2
Electronic access-controlled entrance door	•	•		✓		✓	✓	✓		✓	
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	•	•				✓		✓			
Provide dedicated meeting room located outside secured interior for meetings with visitors or vendors	•					✓		✓			

TABLE 7-1 BENCHMARK SECURITY MEASURES FOR WATER SYSTEM SUPPORT 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	
Design building circulation to provide unobstructed views of people approaching controlled areas or critical assets		•		✓		✓		✓			
Blast-resistant exterior doors ^b	•							✓			
Bollards or vehicle barriers protecting vehicle and personnel doors	•					✓		✓			5.0
Break-resistant glass	•		✓	✓	✓	✓	✓				
Blast-resistant windows ^b	•							✓			
Glass-break detection at windows		•		✓		✓	✓	✓			9.3.1
Interior motion detection		•				✓		✓	✓	✓	9.3
Windows located away from doors so that intruders cannot unlock the doors through the windows	•		✓	✓	✓	✓	✓	✓			
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	•	•		✓	✓		✓		✓		
Chemical fill lines at building exterior—locked access with intrusion detection	•	•				✓		✓		✓	
Chemical storage (indoor)—locked access	•						✓		✓		13.1
Chemical storage (indoor)—locked with intrusion detection	•	•		✓		✓		✓		✓	10.1, 10.3, 10.4, 13.1
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

TABLE 7-1 BENCHMARK SECURITY MEASURES FOR WATER SYSTEM SUPPORT 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	
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)
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	●							✓		✓	
Incoming site utilities—harden power, gas, water, waste and their facility entry points	●							✓			
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.

This page intentionally left blank

Appendix A

PHYSICAL SECURITY ELEMENTS

The design of any security measure must always take safety and maintenance considerations into account.

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.

A.1.0 FENCING AND PERIMETER WALLS

The primary goals of fencing and perimeter walls are to establish a legal demarcation by defining the perimeter boundaries of a facility; to present a barrier that causes an intruder to make an overt action to penetrate that demonstrates intent; and to create a delay barrier against unauthorized access.

Secondary goals may include screening the facility against visual observation; establishing a clear zone that enhances lighting and surveillance; and providing a means to install intrusion detection sensors.

A.1.1 Chain-Link Fencing. For terms related to chain-link fencing systems, refer to ASTM F552, *Standard Terminology Relating to Chain Link Fencing* (ASTM 2005d). For detailed specifications and design information related to chain-link fencing and posts, refer to *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b), and *Federal Specification RR-F-191/2D, Fencing, Wire and Post, Metal (Chain-Link Fence Gates) (Detail Specification)* (NCBC 1990a). Both documents have been approved for public release and are available online. Aluminum fabric, poles, or accessories are not recommended for security applications.

The base-level fence guideline is galvanized steel chain-link fence post with a 6-ft (1.8-m) or greater fabric height. The enhanced-level fence guideline is galvanized steel chain-link fence post with an 8-ft (2.4-m) or greater fabric height.

Fence fabric should be one piece and should be coated with zinc or polyvinyl chloride (PVC). PVC over zinc-coated steel is recommended in harsh, corrosive environments.

The base-level fabric wire gauge should be a minimum standard No. 9 wire gauge and mesh pattern of 2-in. (50-mm) diamond mesh or smaller.

Enhanced-level chain-link fencing should comply with the requirements for the base-level guideline chain-link fencing, except using No. 6 or No. 8 gauge fencing fabric in place of No. 9 gauge, and mesh patterns 1 in. (25 mm) or less across.

Post strength and stiffness for base-level and enhanced-level chain-link fences should meet ASTM F1043, *Standard Specification for Strength and Protective Coatings on Steel Industrial Chain Link Fence Framework*, Group 1A requirements (ASTM 2005c) for heavy industrial fences. Follow the manufacturer's standard with allowance for minimum embedment below finished grade.

The average distance between line posts for chain link fences is recommended to be no more than 10 ft (3 m) when measured center-to-center between posts and parallel to the fence grade

(ASIS 2004, Chapter 3—Chain Link Fencing). For additional guidance on installing chain-link fencing, refer to *RR-F-191K/GEN, Fencing, Wire, and Post Metal (and Gates, Chain-Link Fence Fabric, and Accessories) (General Specification)* (NCBC 1990b); ASTM F567, *Standard Practice for Installation of Chain-Link Fence* (ASTM 2005e); and *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b) for guidelines on connection of fencing mesh to posts for security applications.

The American Society of Industrial Security (ASIS) *Protection of Assets* manual (ASIS 2004) further identifies that post hole depths be a minimum of 24 in. (610 mm), plus an additional 3 in. (76 mm) for each 1-ft (0.3-m) increase in fence height over 4 ft (1.2 m), such that an 8-ft (2.4-m) fence requires a 36-in. (910-mm) depth for post holes. The hole should be backfilled with concrete into the excavation hole [2,500 lb/in.² (psi) (17,000 kPa)] and the concrete extended 2 in. (50 mm) above grade, with a crowned surface to shed water.

Where fences cross a stream, culvert, swale, depression, or other openings that fencing does not enclose, where the opening size is 96 in.² (62,000 mm²) or larger, these openings should be protected by additional grilles, fencing, or other barriers against penetration. Refer to Section 13.3 of this Appendix and to *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b), for recommendations and construction of grilles.

A.1.2 Anti-Climb/Anti-Cut Fencing. If the DBT warrants, a specialized anti-climb/anti-cut fence such as wire-panel mesh fencing should be considered.

Wire-panel mesh fabric wire gauge should be a minimum of No. 8 wire gauge.

Wire-panel mesh pattern should be non-climbable, with a 0.5-in. by 3-in. (13-mm by 76-mm) mesh pattern, welded at each intersection.

Fabric wire should conform to ASTM A853-04, *Standard Specification for Steel Wire, Carbon, for General Use*, Grade AISI 1006 as specified by the American Iron and Steel Institute (AISI) (ASTM 2005b). After welding, the fabric is hot-dipped and galvanized with a zinc coating followed by a PVC coating.

A.1.3 Ornamental Fencing. Site conditions and local codes may dictate the use of aesthetically pleasing fence materials. In such cases, ornamental fences of steel, aluminum, or wrought iron should be considered.

As an example of aluminum fencing meeting the requirements, base-level ornamental fence should be a picket fence, 8-ft (2.4-m) picket height or greater, constructed of HS-35 aluminum alloy. Nominal picket spacing should be 5 in. (130 mm) on center or less. Pickets may include spiked tops, depending on the DBT.

Suggested minimum sizes for fence pickets are 1 in. (25 mm) square by 0.062 in. (1.6 mm) thick, while suggested minimum fence rail dimensions are 1.625 in. (41 mm) by 0.070 in.

(1.8 mm) thick top walls, and 1.625 in. (41 mm) by 0.100 in. (2.54 mm) thick side walls.

Line posts for aluminum ornamental fences should be constructed of HS-35 aluminum alloy, with suggested dimensions of 2.5 in. (64 mm) square by 0.075 in. (1.9 mm) thick. Follow the manufacturer's standard with allowance for minimum embedment below finished grade.

Gate posts for aluminum ornamental fences should be constructed of HS-35 aluminum alloy of minimum dimensions 6 in. (150 mm) square by 0.125 in. (3.2 mm) thick. Follow the manufacturer's standard with allowance for minimum embedment below finished grade.

Fencing should have a powder-coated finish or other appropriate protective finish.

A.1.4 Perimeter Wall. The need for solid perimeter walls, such as concrete masonry walls, may be dictated by the DBT, hardening needs, aesthetics, or the desire to fully screen a facility or asset from outside view. In those instances where hardening and aesthetics are both objectives, hardened (or crash-resistant) ornamental fencing is available.

A base-level concrete masonry unit (CMU) wall height should be 6 ft (1.8 m) or greater. An enhanced-level CMU wall height should be 8 ft (2.4 m) or greater. Wall thickness should be 8 in. (200 mm) as a suggested minimum, with additional thickness as required to meet hardened designs.

Intermediate wall columns should be spaced per design criteria and site conditions.

Corner columns should be positioned where directional changes in wall alignment occur.

Wall foundation and reinforcement should be provided per local design criteria and geotechnical conditions.

A sheer exterior surface should have no protruding, climbable edges.

A.1.5 Fencing Topping. Fence topping may include barbed-wire topping or concertina barbed-wire tape topping, or a combination of both.

For base-level barbed-wire topping, attach a three-strand of barbed wire, conforming to ASTM A176, *Standard Specification for Stainless and Heat-Resisting Chromium Steel Plate, Sheet, and Strip* (ASTM 2004b) and ASTM A666, *Standard Specification for Annealed or Cold-Worked Austenitic Stainless Steel Sheet, Strip, Plate, and Flat Bar* (ASTM 2005a) for a 1-ft (0.3-m)-high single outrigger; for enhanced-level climb resistance, use double Y-style outriggers with three-strand barbed wire.

For concertina-wire topping, attach 12-gauge stainless steel wires to 2-ft (0.6 m)-high double Y-style outriggers. Concertina wire should conform to ASTM F1910, *Standard Specification for Long Barbed Tape Obstacles* (ASTM 2003), and should be 24-in. to 30-in. (610 to 760 mm)-diameter double-coil concertina type. Each concertina loop should consist of 43 ± 2 clusters of needle-sharp barbs on 4-in. (100-mm) centers, each barb measuring a minimum of 1.2 in. (30 mm) in length.

Refer to ASTM A121, *Standard Specification for Metallic-Coated Carbon Steel Barbed Wire* (ASTM 2004a) and *Federal Specification RR-F-191/4D, Fencing, Wire, and Post, Metal (Chain-Link Fence Accessories)* (NCBC 1990c) for installation guidance.

Ornamental fencing with angled "pikes" can be provided as a fence topping to discourage or prevent access to a facility by climbing.

A.1.6 Perimeter Line. Periodic treatment of the perimeter line is recommended to prevent vegetation growth.

Provide a 1-ft (0.3-m)-wide vegetation-free zone with the fence or wall placed in the center of zone, using a 2-in. (50-mm)-thick layer of 0.375-in. to 0.75-in. (10-mm to 19-mm) aggregates, and treat with herbicide.

A.1.7 Fence Foundation Enhancements. To prevent stretching of the fence fabric to allow an adversary to move under the fence, it may be appropriate to anchor the bottom fabric of the fence to create a delay similar to that of solid fencing. For anchorage of fabric, the bottom of the fence fabric should be secured to a bottom rail and securely anchored at the midpoint between the fence posts along the fence line. For the base-level threat guideline, the bottom rail may be anchored to an eyebolt embedded in a "deadman" anchor, a concrete cube 3 ft by 3 ft (0.9 m by 0.9 m) as described in *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b); the deadman should be buried in the soil below the fence rail. As an alternative, 12-in. (300-mm)-deep rows of metal bars or pickets may be embedded at 12-in. (300-mm) intervals along the base of the fencing.

For the enhanced-level guideline to prevent tunneling under fences, provide a continuous concrete curb at the base of the fence 8 in. (200 mm) wide by 24 in. (610 mm) deep. The maximum clearance between the bottom rail and the top of the grade strip should be no more than 2 in. (50 mm) maximum clearance, with the bottom rail of the fencing secured to the concrete strip at the mid-point between the posts and at intervals of 10 ft (3 m) or less.

A.2.0 GATES

Personnel gates should be of similar construction guidelines as fences, or stronger, while vehicle gates will need additional strength due to the weight of the gate assembly, and to prevent vehicle incursion, if dictated by the DBT. Where the DBT justifies additional layered security, hardened (or crash-resistant) gates are available.

A.2.1 Chain-Link Gates. For detail specifications on chain-link gates, refer to *Military Handbook MIL-HDBK-1013/1A, Design Guidelines for Physical Security of Facilities*, Table 6—Common Chain Link Fence Materials (NFESC 1993a), and *Federal Specification RR-F-191/2D, Fencing, Wire and Post, Metal (Chain-Link Fence Gates)* (NCBC 1990a).

Entry gates using perimeter fence double-swing gates should have maximum 2.5-in. (64-mm) clearance between the bottom rail and the finished grade.

Entry gates should have a reinforced steel latch with hardened steel padlock protection.

Posts for swing gates with fabric height up to 8 ft (2.4 m) should have nominal minimum dimensions of 2.875-in. (73-mm) outside diameter (OD) to 8.625-in. (219-mm) OD, depending upon the gate leaf width.

Posts for swing gates with fabric height of 9 to 10 ft (2.7 to 3 m) should have nominal minimum dimensions of 3.5-in. (89-mm) OD to 8.625-in. (219-mm) OD, depending upon the gate leaf width.

A.2.2 Electronic Gate Opening. Electronic gate operators should be Underwriters Laboratory (UL)-listed, heavy-duty, high-frequency electronic models designed to open and close sliding or other types of gates as selected for specific applications. Gates should have maximum 2.5-in. (64-mm) clearance between the bottom tension bar and finished grade.

Electric motors should be sized appropriately for the gate size, duty rating, and frequency of operation. Provide industrial-

quality motor overload protection with manual reset. Gate operators and other electrical appurtenances should be positioned within the fenced perimeter to avoid vandalism and tampering.

Recommended gate travel speed is a minimum 1 ft (0.3 m) per sec. A speed-adjusting feature that provides a range of appropriate speeds for slide gate operation is recommended.

Provide positive limit switches that sense the position of the gate and provide control to prevent damage to the gate operator.

Provide a manual operation feature or disconnect for operation during power failure, malfunction, or emergency. The manual gate operator should be secured inside a locked weather-resistant cabinet, with an attached key box as required. Gate operators should be located so they cannot be reached or tampered with from outside the fence. A variety of types of manual and automatic gate operators, from simple push-button-type operators to complex electronic operating systems, as well as associated hardware and safety devices, are available from gate manufacturers. Gate storage, housing for operators, and site-specific operating systems, warning devices, or signage should also be considered to ensure safe operation when authorized.

Component parts of the gate operator, including attachments, should be constructed with materials or plated, coated, or finished as necessary to provide reliable service in an all-weather environment.

A.2.3 Electronic Gate Control System. A push-button or card-reading sensor in a weatherproof enclosure should be mounted on a steel tube post or concrete bollard anchored to a concrete foundation outside the gate as required.

Consider providing loop, beam, or other vehicle detectors a minimum of 4 ft (1.2 m) away from each side of the gate for safety.

A communication interface should enable remote monitoring of the gate position from a central location, such as a central security office. The suggested operation sequence is:

1. *Entry:* The gate opens when activated by a valid card presented to a card-reading sensor. The gate closes after a sensing loop/sensing beam has determined that the vehicle has passed through the gate.
2. *Exit:* The gate opens when activated by a detector loop in the pavement or a push button inside the gate. The gate closes as for entry.

Other options for automated gate access control systems include radio-controlled, remote-operated (from a control room or operations center), guard-operated, key-switched, and others. Each type will have specific features to consider with respect to the overall access control system.

A.3.0 SITE AREAS

A.3.1 Clear Zones. The purpose of a clear zone is for intrusion detection surveillance and assessment using visual observation or cameras, and to provide an unobstructed area in which placed devices can be readily observed or detected. Clear zone regions are typically established:

- On both sides of a perimeter security fence to allow unobstructed surveillance of the fence area
- Between a perimeter fence and structures, buildings, or other critical assets enclosed within the fence to maintain a clear area for detection of intruders or placed devices
- Around the perimeter of a building to prevent areas of concealment of intruders or placed devices.

For additional information regarding clear zones, see *Minimum Antiterrorism Standards for Buildings, Unified Facilities Criteria (UFC) 4-010-01* (DoD 2002).

Effective clear zone distances should be in accordance with the DBT, but a suggested minimum distance is 20 ft (6 m) or more between the outer perimeter fence and interior structures per *UFC 4-010-01* (DoD 2002).

Within the clear zone, prune or trim vegetation to a height of 4 in. (100 mm) or less, and remove large obstacles or rocks that can shield intruders from view. Avoid locating equipment within clear zones or in spaces below which devices can be readily concealed.

A.3.2 Site Utilities. Wherever possible, incoming site utilities need to be protected from accidental or deliberate damage that might affect operations. It is recommended that the core site utility connections entering the site and facility be hardened. Hardening techniques may include burying, protecting within conduit, security cages, or grilles, or by adding redundant service feeds. The following utilities should be examined and protected to the extent possible:

- Electrical power
- Natural gas
- Incoming water
- Wastewater
- Fire water main(s)
- Communications (phone, data, etc.)

Exposed pipelines should be protected, where possible, using fence barriers to limit access. Alternatively, exposed pipelines could be run within carrier pipes to enable double-wall protection.

Redundant utility connection sources should be provided if available. Dual electrical systems that feed off separate circuits, or incoming water supplies from different source mains, should be utilized where available.

Electrical lines should be placed underground where applicable.

A.4.0 FACILITY ENTRANCES

A.4.1 Sallyport Entrances. A sallyport is a combination of electrically operated gates or portals that are interlocked to prevent more than one gate from opening at a time. The sallyport provides a means for secured, controlled entry through the fence perimeter of the facility. Entry processing, paperwork review, and driver/load identification or verification occur within the sallyport. Sallyports may also be used to enable searching the interior and undercarriage of vehicles for explosives.

Typical vehicle sallyport dimensions are in the range of 75 ft (23 m) long by 20 ft (6 m) wide, and should be sized to accommodate the largest delivery vehicle. The sallyport should be enclosed by fenced sides of height, construction, and configuration consistent with the site perimeter fencing. Vehicle gates should be consistent with the gate guidelines provided in Section A.2.0, Gates, of this Appendix.

Sallyport gates should be equipped with an interlocking system to ensure that the inner and outer gates are not capable of being opened at the same time. However, a keyed manual override switch should be provided that allows the gates to be opened simultaneously. This override switch must be protected and covered such that the possibility of accidental operation is eliminated.

Gate controls should be located in an area such that the person operating the controls maintains a constant visual observation of

the sallyport area. The controls should be protected and covered so that unauthorized use is eliminated.

A.4.2 Building Entrances. Building entrances should provide a space for screening visitors. The area should provide enough space for visitors to wait, queue, and be logged-in prior to entering the interior secure spaces. If frequent visitor entry is anticipated, vandal-resistant furniture may be provided within the visitor waiting area.

Visitor management software can facilitate the log-in and registration of incoming visitors. Some systems permit preregistration prior to entry and notification upon visitor arrival.

If the DBT warrants, x-ray screening of incoming personnel and visitors may be considered. Additionally, explosive screening may be considered for incoming mail and packages.

A.5.0 BOLLARDS AND OTHER VEHICLE BARRIERS

Bollards, jersey barriers, decorative planters, or other vehicle barriers, where applied, should be capable of stopping a 4,000-lb (1,800-kg) vehicle traveling at 30 mph (48 km/h) within 3 ft (0.9 m) or less.

Refer to Department of Defense Handbook *MIL-HDBK-1013/14, Selection and Application of Vehicle Barriers* (NFESC 1999) for detailed descriptions, attributes, and stopping capabilities of several barrier types. This document has been approved for public release and is available online.

A.6.0 EXTERIOR SURFACES

At surfaces subject to vandalism, incorporate glazed concrete masonry units, glazed ceramic tiles, or fiberglass coatings to resist vandalism attempts.

Apply nonstick, unmarkable, polyurethane-based paints and coatings for external surfaces subject to vandalism.

A.7.0 OUTDOOR SECURITY LIGHTING

Depending on the DBT and the local site environment, the amount of recommended illumination may vary. Consult with local code officials for additional restrictions that may apply to lighting levels.

In addition to the suggested illumination levels provided below, refer to the Illumination Engineering Society of North America (IESNA) handbook, *Guideline on Security Lighting for People, Property, and Public Spaces (G-1-03)* (IESNA 2003).

General perimeter roadways and parking areas should be illuminated to 1 to 2 horizontal foot-candles (fch) [11 to 22 lumens/square meter (lux)] on average.

Vehicle gate areas should be illuminated to 3 to 5 fch (32 to 54 lux), average, measured horizontally. If this area will receive CCTV camera coverage, a recommendation is that the illumination levels be 5 to 10 vertical foot-candles (fcv) (54 to 108 lux), measured vertically at the subject height.

- Horizontal illumination measures the lighting at a horizontal surface or plane, such as the ground surface.
- Vertical illumination measures the illumination received on a vertical plane, such as a person's face or the license plate of a vehicle.

If a gatehouse or sallyport entrance is used, an illumination level of 10 to 30 fcv (110 to 320 lux) is the goal.

Building exterior door areas should be illuminated to 3 to 5 fch (32 to 54 lux), on average, for a radius of 15 ft (4.5 m) beyond the exterior door.

General outdoor areas should be illuminated to 0.5 fch (5 lux), average.

Provide a minimum light-to-dark illumination ratio of maximum 6:1, preferably 4:1. Preferably, a lighting engineering study should be performed using point-by-point lighting calculations with a point spacing not more than 25 ft (7.6 m) on center.

Where applicable, incorporate motion-activated lighting to provide instant-on lighting upon motion alarm activation. Such a system will raise the illumination from 0.5 fch (5 lux) to 2 to 3 fch (22 to 32 lux). If motion-activated lighting is included, make sure that the lamp re-strike time is quick enough to support instant-on activation.

When CCTV cameras are used, these additional lighting considerations should be taken (ASIS 2004, *Protection of Assets*, Chapter 19—Security and Protective Lighting):

- *Color Rendering Index:* Choose an appropriate lamp that has accurate color reproduction.
- *Reflectance of Materials:* Consider the material that will be illuminated, and its ability to reflect and transmit light.
- *Direction of Reflected Lighting:* Identify whether reflected lighting will assist or interfere with camera operation.

A.8.0 SIGNAGE

A.8.1 Fence Signage. Post “No Trespassing” signs at 50-ft (15-m) intervals in multiple languages as is consistent with the local population. From a general legal standpoint, the fence and signage establishes a boundary that intruders must cross for violation.

Include appropriate federal, state, and local laws prohibiting trespassing. For example, U.S. Code Title 42, Section 300i-1, titled, “Tampering with Public Water Systems,” states the following (U.S. Code 2009):

1. *Tampering:* Any person who tampers with a public water system shall be imprisoned for not more than 20 years, or fined in accordance with Title 18 “Crimes and Criminal Procedure,” or both.
2. *Attempt or Threat:* Any person who attempts to tamper, or makes a threat to tamper, with a public drinking water system be imprisoned for not more than 10 years, or fined in accordance with Title 18, or both.
3. *Civil Penalty:* The Administrator may bring a civil action in the appropriate United States district court (as determined under the provisions of Title 28 “Judiciary and Judicial Procedure”) against any person who tampers, attempts to tamper, or makes a threat to tamper with a public water system. The court may impose on such person a civil penalty of not more than \$1,000,000 for such tampering or not more than \$100,000 for such attempt or threat.
4. *“Tamper” Defined:* For purposes of this section, the term “tamper” means:
 - a. To introduce a contaminant into a public water system with the intention of harming persons; or
 - b. To otherwise interfere with the operation of a public water system with the intention of harming persons.

A.8.2 Primary Site Entrance Signage. At the primary entrance to the site, post the address of the site so that first responder crews (such as police and fire departments) can confirm the address location.

A.8.3 Water Intake Delineation. At lake or river intakes, provide buoys or float lines with appropriate signage to delineate no-entry zones.

A.9.0 ELECTRONIC SECURITY SYSTEMS

A.9.1 Intrusion Detection Sensors: General. The intrusion detection system should be capable of detecting an individual [weighing 75 lb (34 kg) or more] crossing the detection zone walking, crawling, jumping, running, or rolling [at speeds between 0.5 and 15 ft (0.2 and 4.6 m) per sec], or climbing the fence, if applicable.

Perimeter intrusion detection systems should provide average false alarm rates of not more than one false alarm per week, per sensor, while maintaining proper detection sensitivity.

Interior intrusion detection should provide false alarm rates of not more than one false alarm every three months, per sensor system.

Detection probability should be at a 95% confidence level. When calculating the detection probability for multiple sensor systems, detection is assumed if any of the sensors detects the intrusion.

Intrusion detection systems should cover the entire length of the perimeter of a detection area, including gates.

Intrusion detection sensors should be provided with a redundant power source for a period of not less than 4 h.

Detection sensors should be monitored for alarm and fault conditions by an attendant security monitoring system (an electronic system that monitors security alarms).

A.9.2 Exterior Intrusion Detection. Prevalent sensor technologies include active infrared, microwave, dual-technology, buried-line, fence-mounted sensors, and video motion detection.

Appropriate detection technology should be selected based on factors such as facility environment, location, climate, and ambient temperature conditions, and on the DBT.

A.9.2.1 Active Infrared Sensors. Active infrared sensors transmit infrared signals to a receiver. Interruption of the signal indicates that an intruder or object has blocked the path.

Active infrared sensors require a line of sight; the signal must be projected over a clear path where the line of sight remains unblocked.

Transmitters and receivers should be installed where they will not be misaligned due to Earth tremors, objects hitting the unit (such as falling rocks, branches, or falling trees), or freezing and thawing of the ground.

Active infrared sensors do not work well in areas with heavy snowfall because drifts or snow mounds cover sensors and block transmission and reception paths. Weather conditions such as fog, heavy rain, or severe sand or dust will affect the reliable detecting range.

Nuisance alarm sources for active infrared sensors include animals and wind-blown debris. Fencing can minimize animal false alarms. Vegetation can also pose a problem if it is allowed to grow to a size where its movement will generate an alarm.

A.9.2.2 Microwave Sensors. Microwave sensors transmit or flood a designated area with an electronic field. A movement in the area disturbs the field and sets off an alarm.

The detection area should be free of bushes and obstructions. Close proximity to other high-frequency signals can adversely affect the detection reliability of microwave sensors. Areas that contain strong emitters of electric fields (such as radio

transmitters) or magnetic fields (such as large electric motors or generators) can affect the ability of the microwave sensors to function properly and should be avoided.

Grass should be cut to less than 3 in. (76 mm). A gravel surface prepared for water drainage is better than a grass surface. Avoid dead spots or areas of no detection created by metal objects such as Dumpsters, shipping crates, trash cans, and electrical boxes. These dead spots create areas for intrusion attempts.

Nuisance alarm sources for microwave sensors include wind creating wave action on puddles or moving nearby fences or vegetation, or movement adjacent to, but outside of, the protected area because the signal can easily pass through standard walls, fences, glass, sheet rock, and wood.

A.9.2.3 Dual-Technology Sensors. Dual-technology sensors use both microwave and passive infrared (PIR) sensor circuitry within the same housing. PIR sensors pick up heat signatures from intruders by comparing infrared receptions to typical background infrared levels. Typically, activation differentials are 3 °F (1.7 °C).

Dual-technology sensors generate an alarm condition if either the microwave or PIR sensor detects an intruder.

Dual-technology sensors can be installed along a perimeter line, a fence, or a buffer zone, or as a defense against intruders approaching a door or wall.

Nuisance alarms for microwave sensors are described in Section A.9.2.2. Nuisance alarms for PIR sensors include reflected light and radiated heat.

In some dual-technology sensors, alarm settings may be adjusted to require that both the microwave and the PIR unit detect an intruder before an alarm condition is generated. With two independent means of detection, false alarms are reduced.

A.9.2.4 Buried Line Sensors. There are several types of buried line sensors, including fiber-optic cable, ported cable, and ported co-axial cable.

The two principal advantages of buried cable are that it is covert and it follows the terrain.

Buried line systems do not work well with shrubbery or trees that require landscaping and maintenance.

It is important that the cable be buried to a uniform depth. Changes in soil conductivity can affect the sensor readings.

Nuisance alarms can be caused by the ground shifting due to standing or puddling water, or erosion. Tree roots can also cause nuisance alarms when windy conditions aboveground cause movement in the roots. Large animals passing over the detection zone can also generate alarms.

A.9.2.5 Fence-Mounted Sensors. Fence-mounted sensors detect vibrations on fence fabric associated with sawing, cutting, climbing, or lifting the fence fabric.

Fence-mounted sensors are not reliable in areas where high vibrations are likely to be encountered, such as in close proximity to roadway activity or construction. Do not use in areas with high wind or numerous animal interactions with the fence line.

Fence-mounted sensors perform best when mounted directly to the fence fabric. Each sensor is connected in series along the fence with a common cable to form a single zone of protection.

Sensor zone lengths have a typical recommended range of 300 ft (90 m), although some systems permit longer sensing zones.

Install these sensors on high-quality fencing. Poor-quality fences with loose fabric can create too much background activity due to flexing, sagging, or swaying.

Nuisance alarms can be generated from shrubbery and tree branches as well as animals and severe weather that contacts the fence, causing it to vibrate.

A.9.3 Interior Intrusion Detection. Provide appropriate interior intrusion detection according to the DBT and the building environment.

Applicable technologies include dual-technology (passive infrared and microwave), linear beam, and glass-break sensors.

Select products that are consistent with the ambient temperature, environment, and moisture content of the structure to be protected.

A.9.3.1 Dual-Technology Motion Sensors. Dual-technology motion sensors use passive infrared and microwave technology to detect motion. Described in Section A.9.2.3, these sensors are applicable for both interior and exterior applications.

Do not use dual-technology sensors in areas where the PIR sensor can be exposed to sudden changes in temperature, such as near an exterior door.

Nuisance alarms can be generated from heat-radiating objects such as heat system registers or other warm objects (including things as innocuous as a mop bucket with hot water in it).

A.9.3.2 Linear Beam Sensors. Linear beam sensors transmit a beam of infrared light to a remote receiver, creating an “electronic fence.” Once the beam is broken, an alarm signal is generated. It has a high probability of detection and a low false alarm rate.

This type of sensor is often used to cover openings such as doorways or hallways, acting essentially as a trip wire. The infrared beam is unaffected by changes in thermal radiation, fluorescent lights, electronic frequency interference (EFI), or radio frequency interference (RFI).

The transmitter and receiver can be up to 1,000 ft (300 m) apart.

Nuisance alarms can be created by any objects that may break the beam, such as paper blowing off of a shelf or desk.

A.9.3.3 Glass-Break Sensors. There are three basic types of glass-break sensors: acoustic sensors (listen for an acoustic sound wave that matches the frequency of broken glass), shock sensors (feel the shock wave when glass is broken), and dual-technology sensors (sense acoustic and shock vibrations).

Using dual-technology sensors significantly reduces false alarms from background noise such as RFI and frequency noise created by office machines.

Glass-break sensors provide intrusion detection for windows and doors with glass panes. They are mounted on a window, window frame, wall, or ceiling. If mounted on a wall or ceiling (this is the preferred placement), place it opposite the window. If mounted on glass, place it in the corner, approximately 2 in. (50 mm) from the edge of the frame.

Use mounting adhesive specified to withstand long exposure to summer heat, winter cold, or condensation.

Regardless of the type of sensor, coverage typically does not exceed 100 ft² (9 m²) of glass surface.

Nuisance alarms can be caused by improper calibration or installation. In addition, RFI, sharp impact noises, and background noise such as office, industrial, and cleaning machinery can cause false alarms.

A.9.4 Door and Hatch Contact Alarm Switches. Door and hatch contact alarm switches should interface with a security monitoring system in addition to the SCADA system.

Magnetic door contact switches should be installed at all building exterior doors to monitor for door-ajar and door-forced-open conditions.

Exposed exterior locations, such as exterior hatches or vaults, should utilize high-security balanced magnetic switches.

Industrial doors, gates, and roll-up doors should use high-security, rugged-duty, sealed, wide-gap magnetic switches.

A.9.5 Pipeline Vibration Detection. Emerging technologies are being developed that provide vibration detection within pipeline sections. Incorporating this technology can detect attempts at sabotage such as cutting, hammering, or detonation of the pipeline, and a response can be initiated. Such detection systems might be considered for critical pipeline sections that do not have redundancy. The detection systems monitor vibration within the pipeline section. If the vibration level exceeds a threshold amount, then an alarm could be transmitted back to a central monitoring station. Such systems are relatively new technology but are currently in operation for critical utility (oil, natural gas) pipelines within the United States.

A.10.0 ACCESS CONTROL SYSTEMS

A.10.1 Access Control Systems: General. A means of providing access control should be incorporated into all security systems. Access control measures should consist of one or more of the following systems: key locks and/or padlocks, numeric keypad locks, or card reader systems.

A.10.2 Locks and Padlocks. Padlocks should be weather-resistant with a hardened-steel shackle.

Padlock pulling resistance should be 4,500 lb (20,000 N) at minimum.

Padlock pressure resistance to bolt cutters should be 10,000 lb (44,000 N) at minimum.

Key locks should use hardened steel inserts protecting the plug face, shell, and sidebar from drilling attack.

Provide an access guard of channel steel or other material against bolt-cutter or torch access to padlocks.

Whenever possible, avoid using “daisy chains” of padlocks. Instead, use a programmable lock that allows for authorized entry by multiple individuals using unique codes.

A.10.3 Numeric Keypad Locks. Numeric keypad locks are locking systems that include a programmable keypad in addition to the door latch or deadbolt and lever handle. A user must enter a code at a keypad before the door will unlock and allow access. New codes can be added or changed at the keypad.

Models are available that require both a credential and a code. This dual method can provide an additional layer of protection.

Models are available to mount on various door thicknesses and doors with narrow stiles.

A.10.4 Card Reader Systems. Card reader systems should incorporate:

1. *Alarm Display and Programming:* A computer server or workstation that displays alarm conditions and allows programming of the system.
2. *Badge Creation:* A badge station, allowing creation and programming of badges.
3. *Local Control:* Local control panels that control the doors, card reader units, and access cards.
4. *Printer Unit:* A printer unit that can print a report for each event and alarm condition.

Under normal operation, the system should grant access at doors with card readers by comparing the time and location of any attempted entry with information stored in local (at the door controller) memory.

Access is granted only when the security card used has a valid entry code at the card reader for the designated time frame.

The access card should be a standard credit-card-size passive component with an integral coding technology, such as coding contained within a chip in the card.

Electrical locking means should be electric strike, magnetic lock, or other approved means. Great care should be taken in designing access control for doors used for egress to ensure that free egress is permitted at all times.

Refer to NFPA 101, *Life Safety Code* (NFPA 2006) and NFPA 101B, *Code for Means for Egress for Buildings and Structures* (NFPA 2002) for code guidance on egress and ingress doors.

A.11.0 CLOSED-CIRCUIT TELEVISION (CCTV) SURVEILLANCE

A.11.1 General Considerations. CCTV cameras can be analog or Internet Protocol (IP)-network cameras, depending on factors such as the suitability to the installation, site conditions, and availability of local area networks.

The ASIS publication *Protection of Assets*, Chapter 38—Television in Security (ASIS 2004), identifies the following specification items to consider when specifying CCTV cameras:

- *Imager:* The size of the image-sensing device within the camera.
- *Resolution:* The measure of detail that the camera can distinguish, usually measured in horizontal TV lines per in. (25 mm). The larger the number, the sharper the image and the better the camera.
- *Sensitivity:* Typically, the minimum lighting illumination level required for full video. The lower the required illumination level, the more sensitive the camera.
- *Signal-to-Noise Ratio:* The ratio of the peak value of the video signal to the peak value of the noise or electromagnetic interference, measured in decibels. The greater the ratio, the sharper and better the picture image.
- *Automatic Light Compensation:* The process whereby the amount of illumination on the image sensor is automatically adjusted to the scene brightness. A high ratio indicates that the camera can automatically adjust to wide variations in scene illumination without noticeable distortion in the transmitted image.
- *Backlight Compensation:* A feature available in many cameras that automatically reduces contrast and silhouetting between near and far objects.
- *Video Output:* A measurement, stated in volts peak-to-peak, between the darkest black to brightest light levels of the signal. A typical value is 1.0 V peak-to-peak.
- *Synchronization:* A means of controlling the image scanning so that the camera image will not roll when switched between video monitors. Better cameras allow for synchronization adjustment to accommodate multiphase power supplies.
- *Environment:* Upper and lower temperature and humidity limits for the cameras. It is important to specify a camera that works in the intended environment, including weather.
- *Dimensions:* The outside measurements of the camera case.
- *Weight:* The weight of the camera within its case.

Because camera technology is improving so rapidly, detailed performance specifications are not provided here; it is recommended that utilities consult with a security engineer for current camera hardware standards and sensitivity ratings.

A.11.2 Field of View. Provide fixed-position or pan/tilt/zoom (PTZ) cameras depending upon the desired field of view and the intended application.

Provide appropriate camera lenses corresponding to the camera application and field of view requirements.

The CCTV surveillance system should be capable of viewing prescribed objects within the field of view as follows, considering a screen height of 480 pixels to be full-screen (100% = 480 pixels).

- For intrusion detection purposes, the object should occupy a minimum of 10% of the screen height or be 48 pixels tall.
- For recognizing a person's face, the body of the person should be a minimum of 50% of the screen height or 240 pixels tall.
- To identify a license plate, the plate height should be a minimum of 5% of the screen height or 24 pixels tall.

In some cases, the field of view of a camera may include public areas or private residential areas that should not be monitored by video surveillance. In these cases, to minimize liability issues, a current capability of modern CCTV systems allows masking of these areas or views so that they cannot be seen by the attendant staff.

A.11.3 CCTV Housings and Mounts. CCTV housings should be adequate for the intended application and site location.

Incorporate heater/blower units, wipers, or other elements as necessary to accommodate site environmental conditions.

Incorporate pole-mount, building-mount, or other mounting means so that the camera obtains a clear field of view of the intended target.

Specify and locate the housing and camera mount such that tampering or vandalism of the camera units is prevented.

A.11.4 Video Network Servers. The video network server should be a high-performance IP network-compatible video system.

The network server should be capable of streaming images at a frame rate of 30 frames per sec.

The video communication system should be capable of transmitting live video across communication networks and enable video cameras to be remotely monitored and controlled over the network, provided password authentication requirements are met.

The desired camera view should be selectable by designated camera name and IP address.

A.11.5 Digital Video Recorders. As a minimum, it is recommended to provide adequate digital recording capacity for all cameras for 30 days of continuous storage at 5 frames per sec.

Provide a means for archiving video to digital video disc (DVD) or other long-term storage format.

Specify the physical location of the recorder unit based on environmental considerations, location, network, and bandwidth availability.

Identify appropriate video compression technology to conserve network bandwidth and storage needs.

A.11.6 CCTV Computer Application Software. CCTV application software should be full management software to monitor and manage single or multiple sites.

The software should allow monitoring and recording of images from multiple simultaneous cameras at frame rates up to 30 frames per sec.

The system should enable customized layouts for intuitive and interactive ways of representing the camera network.

The software should provide flexible live and recording settings per individual camera input.

The software should allow connectivity to other systems, via application programming interface (API) alarm and pre-alarm recordings, and enable support for external joysticks to perform pan and tilt operations.

A.12.0 SECURITY, CONTROLS, AND SCADA WIRING

All security, controls, and SCADA wiring should be protected within conduit.

All interconnecting wiring between security components should be monitored for integrity so that an abnormal condition (e.g., wire-to-wire short, wire break, or wire ground-fault condition) is automatically indicated to the user upon arming the system.

The security wiring configuration at the end device should be a four-state configuration using an end-of-line (EOL) resistor network where neither the alarm nor the normal condition are 0 ohms or open-circuit.

Conceal security conduits, telephone lines, and other critical utility connections from view and access, or locate them in the interior of buildings.

Provide a backup power source (4-h minimum) to security components and SCADA and other crucial control systems. Backup power sources may include battery units, auxiliary power supplies, uninterruptible power supplies (UPSs), or generators.

Refer to NFPA 70, *National Electrical Code* (NFPA 2005), for code guidance on electrical wiring requirements.

A.12.1 SCADA and Electrical Control Panel Enclosures. Provide a tamper switch at all security and SCADA control panel enclosures. Upon enclosure door opening, an alarm condition should be logged by the system.

Though panels should be locked, the electrical disconnect should never be locked.

A.13.0 BUILDING ELEMENTS

A.13.1 General. When new buildings are being designed, discuss with the building architect and structural engineers the opportunity to incorporate design elements that prevent progressive collapse of the facility in the event of explosion within or adjacent to the building. Progressive collapse is defined by ASCE and the Structural Engineering Institute (SEI) in *Minimum Design Loads for Buildings and Other Structures* (ASCE 2010) as “The spread of an initial local failure from element to element eventually resulting in the collapse of an entire structure or a disproportionate large part of it.”

A.13.2 Doors. Exterior doors should be heavy-duty, steel-metal doors conforming to ASTM F476-84(2002) Grade 40 high-security-level door (ASTM 2002), prepped for security door hardware. Doors should comply with ANSI/NAAMM/HMMA 862-03 *Guide Specifications for Commercial Security Hollow Metal Doors and Frames* (ANSI/NAAMM/HMMA 2003).

Doors should have a maximum window opening of 96 in.² (62,000 mm²) or nominal 4-in. by 16-in. (100-mm by 400-mm) size with a minimum side panel size.

The door frame should be heavy-duty with concrete fill.

Hinge pins should be on the secure side or be nonremovable or tamper-resistant to eliminate door compromise by removing hinge pins.

Consider electronic door status monitoring for door-forced and door-ajar conditions.

The following door recommendations are provided for example purposes from the U.S. General Services Administration publication *Facilities Standards for the Public Buildings Service*, Section 3.5—Building Elements (GSA 2005).

- Glazed exterior doors and frames should be steel and meet the requirements of SDI Grade III with a G-90 galvanic zinc coating.
- Hinges, hinge pins, and hasps must be secured against unauthorized removal by using spot welds or pinned mounting bolts.
- All exterior doors must have automatic closers.
- The exterior side of the door should have a lock guard or astragal to prevent jimmying of the latch hardware.
- Doors used for egress only should not have any operable exterior hardware.

A.13.3 Security Grilles. Base-level security grilles (for windows, louver openings, roof hatches, culverts, etc.) should be woven No. 10 wire gauge steel, 1.5-in. (38-mm) diamond mesh, or welded No. 10 wire gauge, 2-in. (50-mm) square welded mesh screens.

The grilles should be hot-galvanized with a hot-powdered-coat finish.

Use tamper-resistant and tamper-proof fasteners for mounting window grilles.

For enhanced-level threat protection, refer to *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b) for security grilles.

A.13.4 Security Cages. Caged partitions (for critical equipment, pumps, motor control centers, and so on) should be No. 10 wire gauge steel with 2-in. (50-mm) welded openings in 1.25-in. by 1.25-in. by 0.125-in. (32-mm by 32-mm by 3-mm) angle iron framework.

Ensure that the partitions include framework supports, access gates, locks, and other accessories.

A.14.0 HATCHES, VAULTS, AND VENTS

A.14.1 Hatch, Vault, and Vent Alarms: General. Hatch, vault, and vent alarms should use similar alarm contact hardware, such as magnetic door contact switches, depending on the final hatch or vault design.

Interconnect the alarm contacts to a security monitoring system.

Note that curb and sidewalk devices may become a tripping or safety hazard. Consider the location and application carefully when designing the system.

Provide locking covers for valve operators.

A.14.2 Roof or Sidewalk Hatches. Provide a lock on a manufacturer's metal door system that is set into concrete curb with a gutter and drain.

Consider an additional protected keyed bar lock across a door that is mounted directly to a structural curb, especially for large, publicly accessible pumping stations.

Consider an elevated upper structure cover surrounding a sidewalk door, especially for large, publicly accessible pumping stations. This cover is to prevent drilling through the door-plate and adding liquids to the contents, as well as to delay access to the sidewalk door hatch. This additional layer delays someone attempting to gain access to water to introduce a contaminant.

Alarm the upper structure using exterior-rated, balanced magnetic door contacts.

A.14.3 Roof Vents. Provide metal roof vents with numerous small openings rather than vents with fewer, larger openings [96 in.² (62,000 mm²) is considered a person-passable opening]. Contaminants can be introduced through much smaller vents; prevent direct passage of contaminants through a vent by using traps.

Position or barricade vent openings to prevent spray of a contaminant liquid into a vent opening.

Provide a metal structure cover surrounding the vent to delay access to the vent structure, with adequate standoff [nominally 8 in. (200 mm) or more] from the vent to limit drilling attempts into the vent assembly.

Provide protected dual locks on a metal vent cover system set on a concrete curb.

Alarm the protective cover using exterior-rated magnetic door contacts.

A.14.4 Vault Hatch with Elevated Curb. Provide a lock on a manufacturer's door system. Alarm the vault hatch using exterior-rated magnetic door contacts.

Consider an additional protected key bar lock across a door that is mounted directly to a structural curb.

A.14.5 Vault Door Hatch Set Flush with Top of a Structural Slab. Provide a lock on a manufacturer's door system. Alarm the vault hatch using exterior-rated magnetic door contacts.

Consider an interior keyed bar lock system or secondary horizontal structure immediately below the vault sidewalk door hatch to block access.

A.15.0 ONLINE WATER QUALITY MONITORING

A suite of online instruments to monitor certain surrogate water quality parameters should be installed. Among the parameters to monitor in water distribution systems are pH, chlorine residue (either total or free, depending on the type of residue maintained in the system), specific conductance, turbidity, and total organic carbon.

Among the parameters that could be considered for monitoring wastewater collection systems are pH and volatile organic carbon.

Periodic readings from the online instruments should be compared with baseline water quality values to determine whether there is potential contamination.

The placement of the sampling location for the instruments depends on the type of asset. For example, in water storage tanks the sampling location should be from the outlet pipe near the tank, ideally between the tank and the isolation valve. If there is a common inlet outlet pipe, the sampling location should be installed on the common pipe near the tank, ideally between the tank and the isolation valve.

A.16.0 OPERATOR DEVICES

A.16.1 Man-Down Transmitter. A man-down transmitter is worn by personnel for automatic man-down signaling. The

unit should be portable, lightweight, and supplied with a belt clip or holster for mounting. Built-in tilt switches should automatically activate the man-down transmitter when the user is knocked down. A pull cord should activate the alarm or emergency signal when an attempt is made to remove the unit from a belt.

The transmission mode should integrate both radio frequency (RF) and infrared (IR) signaling for redundant communications.

Power should be provided by a long-life lithium battery.

A.17.0 CHEMICAL FILL-LINE LOCKING DEVICES

Connections for filling chemical tanks should be locked to restrict access to authorized personnel only. Chemical fill lines usually are fitted with quick-connect, cam-arm actuated couplings for ease of use by the chemical vendor. Locking devices for the contractor's temporary connections are recommended.

Lockable dust caps or dust plugs with hardened key locks should be installed on the individual couplings.

Where multiple fill lines are co-located, a hardened box or port integrated into the building masonry, complete with a shrouded and hardened lock, can be used in lieu of individual coupling locks.

A.18.0 HYDRANTS

Provide tamper seals on hydrants. Tamper seals reduce the possibility of tampering or unauthorized operation of the hydrant.

Provide a one-way check valve minimizing the possibility of accidental or intentional contamination of drinking water via the hydrant. The device should not hinder or slow response time to firefighters or reduce flow below the flows referred to by standards ANSI/AWWA C502-05 and ANSI/AWWA C503-05 (ANSI/AWWA 2005). The check valve must be capable of being tested without being removed from the hydrant to ensure a leak-proof seal.

Provide locking mechanisms on hydrants. Hydrant locking systems should be designed so that the hydrants can be operated using a special keyed wrench without the need to remove the lock.

- If locking mechanisms are used on hydrants, it is important that training on unlocking the mechanisms be provided to all local firefighting personnel and any other fire departments with which there are mutual aid agreements in place, who would respond in an emergency.
- Provide the specialized wrenches in sufficient quantity to the fire department and other authorized persons so they can operate the hydrants as needed. These wrenches are typically only sold to fire authorities and water utilities.

A.19.0 MANHOLES

Securing manholes can be accomplished in three ways: tack welding, bolt locks, and pan locks.

1. *Tack Welding:* Provides a fast method of securing manholes. It is economical and effective for manholes not frequently accessed. The disadvantage is that the tack weld must be removed or broken before utility staff can access the manhole.

2. *Bolt Locks:* Anchor the manhole to the manhole frame. They have a specialized bolt head that requires a specialized tool to unbolt or unlock the manhole. To remove or access the manhole, the bolt locks must be removed. This system of locking manholes is more flexible than the tack welding method, but more expensive to install. There are some challenges with noise and rattling on locking manhole covers.
3. *Pan Locks:* Prevent entry into the manhole, as well as eliminating dumping into the collection system. The pan unit is installed into the manhole, with the edge of the pan resting within the manhole opening. The manhole is then locked in place in the pan unit. This system of locking manholes is more flexible than the tack welding and bolt locking methods, but more expensive to install.

GLOSSARY AND ABBREVIATIONS

Access Control: The physical guidance of vehicles and/or people going to and coming from a space through judicious placement of entrances, exits, landscaping, lighting, and controlling devices (such as guard stations, turnstiles, etc.)

ACI: American Concrete Institute.

Agent: Any physical, chemical, or biological entity that can be harmful to an organism.

AISI: American Iron and Steel Institute.

AMSA: Association of Metropolitan Sewerage Agencies [now National Association of Clean Water Agencies (NACWA)].

ANSI: American National Standards Institute.

API: Application programming interface.

ASCE: American Society of Civil Engineers.

ASDWA: Association of State Drinking Water Administrators.

Asset: Anything of value (such as people, information, hardware, software, facilities, equipment, reputation, activities, or operations) that may be a target of the design basis threat (DBT) adversary. Assets are what an organization needs to get the job done—to carry out the mission. The more critical the asset is to an organization accomplishing its mission, the greater the effect of its damage or destruction.

ASTM: ASTM International (formerly the American Society for Testing and Materials).

AWWA: American Water Works Association.

AwwaRF: The former American Water Works Association Research Foundation, now called the **Water Research Foundation**.

Base: Minimum recommended.

Bollard: One of a series of posts preventing vehicles from entering an area.

CCTV: Closed-circuit television.

Check Valve: A valve that allows fluid to flow through it in one direction but prevents flow in the opposite direction.

Clear Zone: An area surrounding the perimeter of a facility that is free of shrubs and trees, and features well-maintained landscaping that does not provide hiding places for an adversary.

CMU: Concrete masonry unit.

Contaminant: Any physical, chemical, biological, or radiological substance or matter that has an adverse effect on air, water, or soil.

Contamination: Introduction of microorganisms, chemicals, toxic substances, wastes, or wastewater into water, air, and soil in a concentration that makes the medium unfit for its intended use.

Countermeasure: A reaction to or a defense against a hostile action to deal with a threatening situation.

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 for the adversary to obtain the asset. See also Table 1-1.

Cross Connection: Any temporary or permanent connection between a public water system for consumer's potable (i.e., drinking) water system and any source or system containing or which may contain nonpotable water or other substances.

Daisy Chain: Groups of padlocks connected and hooked to a common chain in such a way as to allow access through a key that can unlock any one of the padlocks.

Delay Features: Security objects such as physical barriers designed to occupy or limit an adversary until a response force can interrupt accomplishment of the adversary's objectives. Delay features consist primarily of physical hardening features and are often employed in multiple layers to provide protection in depth. Delay features are only effective when placed within a layer of detection.

Design Basis Threat (DBT): The adversary against which a utility must be protected. Determining the DBT requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence.

Detection: The point at which a potential attack is discovered, assessed, and determined to be an attack in progress rather than a false alarm.

Detection Features: Security items such as sensors that are intended to detect the presence of an intruder. A complete detection system generally includes 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 also include lighting systems, motion detectors, monitoring cameras, access control equipment, or other devices.

Deterrence: Security measures such as lighting or the presence of closed-circuit television or people in the area that may discourage an adversary from attacking the 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.

DoD: U.S. Department of Defense.

DVD: Digital versatile disc, digital video disc.

EFI: Electronic frequency interference.

Enhanced: Augmented with improved, advanced, or sophisticated features.

EOC: Emergency operation center.

EOL: End-of-line.

EWRI: Environmental and Water Resources Institute of the ASCE.

Foot-Candle: A unit of light intensity defined as the amount of light measured on a surface one foot from a uniform point source of light equal to the light of one candle. A foot-candle is equal to one lumen per square foot.

FRP: Fiberglass-reinforced plastic.

GSA: U.S. General Services Administration.

Harden: To improve the physical strength of a protective measure.

IESNA: Illuminated Engineering Society of North America.

Improvised Explosive Device (IED): An apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, harass, or distract through high-speed projectiles and overpressure.

Improvised Incendiary Device (IID): An apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, harass, or distract by creating intense heat and fire.

Insider: An individual who is granted normal access to a facility. This may be an employee, a contractor, a custodial worker, or an authorized visitor. See also Table 1-1.

Intrusion: Entrance by force or without permission or authorization, either physically or via electronic methods.

IP: Internet Protocol.

IR: Infrared.

Key Card Reader/Access: Entry to a facility via a device used by an individual(s).

lb: Pound.

Lumen: The SI unit of measuring the power of light being produced by a light source or received by a surface.

Lux: The SI unit of light intensity defined as the amount of light equal to one lumen per square meter.

m: Meter.

mm: Millimeter.

Mantrap: Secured entry system that prevents an individual from gaining access to an area by holding them first in an assessment area.

NACWA: National Association of Clean Water Agencies [formerly Association of Metropolitan Sewerage Agencies (AMSA)].

NDWAC: National Drinking Water Advisory Council.

NETCSC: National Environmental Training Center for Small Communities.

NFPA: National Fire Protection Association.

NRWA: National Rural Water Association.

OD: Outside diameter.

PIR: Passive infrared.

PL: Public law.

PLC: Programmable logic controller.

Protection in Depth: The strategy of providing multiple layers of protective measures, thereby requiring an adversary to defeat a system, travel to the next protective layer and defeat that system, and so forth until reaching the target. An example of protection in depth is the application of layers of protective measures at the site boundary (perimeter fencing system), at the building envelope (exterior walls, doors, windows, grilles, and roof system), and at the target enclosure (the room in which the targeted asset is housed).

psi: Pounds per square inch.

PTZ: Pan, tilt, and zoom.

PVC: Polyvinyl chloride.

RAM-W: Risk Assessment Methodology for Water Utilities, available from the Sandia Corporation (Sandia National Laboratories).

Response: Actions taken to interrupt the adversary's task. Utility staff, the utility's security response force, or law enforcement may carry out response, depending on the threat and policy of the utility.

RF: Radio frequency.

RFI: Radio frequency interference.

Risk: The potential for realization of unwanted, adverse consequences to human life, health, property, or the environment. The quantitative or qualitative expression of possible loss that considers both the probability that a hazard will cause harm and the consequences of that event. Risk is usually expressed as a function of the probability that an adverse effect will occur and the criticality of the effect on the ability to fulfill a mission or function.

RTU: Remote terminal unit.

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 bent on damage or destruction of the utility's facilities or generating a lack of public confidence in the utility's ability to protect the public. See also Table 1-1.

SCADA: Supervisory Control and Data Acquisition (see full definition below).

SI: International System of Units.

Significant: Having or likely to have a major effect; important; fairly large in amount or quantity.

Supervisory Control and Data Acquisition (SCADA): The system that provides automatic or semi-automatic sensing of key parameters and control of key elements of the water or wastewater system. It generally provides for communications, notifications, and alarms, as well as for manual override of controls.

Surveillance: The placement of physical features, activities, vehicles, and people that maximize visibility by others during their normal activities. Surveillance may be natural or electronic, informal (office windows placed to facilitate surveillance of entry roads), or formal (continuous monitoring). Surveillance provides the link between detection (sensors activated due to the presence of an intruder) and assessment (confirming that the detection is valid and not a nuisance alarm).

SWAT: Special Weapons and Tactics.

Target: This term is used synonymously with asset throughout this document.

Terrorist: A radical who employs terror as a political weapon. With significantly enhanced tool and weapon capabilities, terrorists may be politically or doctrinally motivated to cause maximum human casualties, often without regard for the terrorist's personal survival.

UL: Underwriters Laboratory.

UPS: Uninterruptible power supply.

USEPA: U.S. Environmental Protection Agency.

VA: Vulnerability assessment (see full definition under **Vulnerability Assessment**).

Vandal: An individual acting alone or in a group, unarmed and using spray paint to deface property or using hand tools to inflict damage to utility assets. See also Table 1-1.

Vehicle Sallyport: Interlocking gates within a fenced area where incoming drivers pass through the first gate and stop at the second gate. Once both gates are closed and the vehicle is captured within the sallyport, a security guard may confirm the identity of the driver and, if necessary, search the vehicle to confirm the contents. Once the vehicle and driver are approved, the second gate opens and the vehicle may drive onto the facility.

VSAT: Vulnerability Self-Assessment Tool, available from NACWA.

Vulnerability: A characteristic of a critical infrastructure's design, implementation, or operation that renders the infrastructure susceptible to destruction or incapacitation by a threat. Vulnerabilities may consist of flaws in security procedures, software, internal system controls, or installation of infrastructure that may affect the integrity, confidentiality, accountability, or availability of data or services. Vulnerabilities also include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters. Vulnerability may be considered any weakness that can be exploited by an adversary or, in a nonterrorist threat environment, make an asset susceptible to hazard damage.

Vulnerability Assessment (VA): An assessment of the vulnerabilities of a water or wastewater system. The six common elements of vulnerability assessments identified by USEPA are: (1) characterization of the system, including its mission and objectives; (2) identification and prioritization of adverse consequences to avoid; (3) determination of critical assets that might be subject to malevolent acts that could result in undesired consequences; (4) assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries; (5) evaluation of existing countermeasures; and (6) analysis of current risk and development of a prioritized plan for risk

reduction. Two example approaches to VAs are the Risk Assessment Methodology for Water Utilities (**RAM-W**) and the Vulnerability Self-Assessment Tool (**VSAT**).

Water Research Foundation (WRF): Established in January, 2009; the former American Water Works Association Research Foundation (**AwwaRF**).

WEF: Water Environment Federation.

WISE: Water Infrastructure Security Enhancements.

WISE SC: Water Infrastructure Security Enhancements Standards Committee of the EWRI of ASCE.

WSWG: Water Security Working Group.

This page intentionally left blank

REFERENCES

For a comprehensive list of resources related to water and wastewater security, see the USEPA WISE Phase 1 documents developed by the American Society of Civil Engineers, the American Water Works Association, and the Water Environment Foundation (ASCE/AWWA/WEF 2004a, 2004b, 2004c). The initial Draft was developed for USEPA WISE Phase 3 and was titled the *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA/WEF 2006).

- American Concrete Institute (ACI). (1998). *371R-98: Guide for the analysis, design, and construction of concrete-pedestal water towers (reapproved 2003)*, ACI, Farmington Hills, Mich.: This ACI guide presents recommendations for materials, analysis, design, and construction of concrete-pedestal elevated water storage tanks. These structures are commonly referred to as composite-style elevated water tanks that consist of a steel water storage tank supported by a cylindrical reinforced concrete pedestal.
- American National Standards Institute/American Water Works Association (ANSI/AWWA). (2005). *C502-05: Dry-barrel fire hydrants and C503-05 Wet-barrel fire hydrants*, AWWA, Denver, Colo.: These standards establish flow standards for dry- and wet-barrel fire hydrants.
- American National Standards Institute/National Association of Architectural Metal Manufacturers/Hollow Metal Manufacturers Association (ANSI/NAAMM/HMMA). (2003). *ANSI/NAAMM/HMMA 862-03: Guide specifications for commercial security hollow metal doors and frames*, NAAMM, Chicago, Ill.: This document provides specifications for commercial security hollow metal doors and frames. Its focus is protection from vandalism, forced entry, theft, and firearms attack.
- American Society of Civil Engineers (ASCE). (2010). *Minimum design loads for buildings and other structures*, ASCE/SEI Standard 7-10, ASCE, Reston, Va.: This update to ASCE/SEI Standard 7-05 and its supplement provides requirements for general structural design, and includes means for determining dead, live, soil, flood, wind, snow, rain, atmospheric ice, and earthquake loads, and their combinations that are suitable for inclusion in building codes and other documents.
- American Society of Civil Engineers/American Water Works Association/Water Environment Federation (ASCE/AWWA/WEF). (2004a). *Interim voluntary guidelines for designing an online contaminant monitoring system*, ASCE, Reston, Va.: These guidelines are based on the USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004). Details are available at http://content.ewrinstitute.org/files/pdf/IVSGDOCMS_817R08007.pdf.
- ASCE/AWWA/WEF. (2004b). *Interim voluntary security guidance for wastewater/stormwater utilities*, ASCE, Reston, Va.: These USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at http://content.ewrinstitute.org/files/pdf/IVGWU_817R08006.pdf.
- ASCE/AWWA/WEF. (2004c). *Interim voluntary security guidance for water utilities*, ASCE, Reston, Va.: USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at http://content.ewrinstitute.org/files/pdf/IVGWU_817R08010.pdf.
- ASCE/AWWA/WEF. (2006). *Guidelines for the physical security of water utilities*. ASCE, Reston, Va.: These guidelines are based on the USEPA WISE ASCE/AWWA/WEF Phase 3 Documents (December 2006). Details are available at <http://content.ewrinstitute.org/files/pdf/4.pdf>.
- American Society of Industrial Security (ASIS). (2004). *Protection of assets*, ASIS, Alexandria, Va.: Although the availability of security literature is growing rapidly, with general and specialized texts, it has not been possible—until now—for a business manager or protection professional to find in one place, current, accurate, and practical treatment of the broad range of protection subjects, strategies, and solutions.
- American Water Works Association (AWWA). (1995). *D115-95: Circular prestressed concrete water tanks with circumferential tendons*, AWWA, Denver, Colo.: This standard includes current and recommended practice for the design, construction, and field observations of circular prestressed concrete tanks using tendons for circumferential prestressing.
- AWWA. (1998). *Steel water-storage tanks (M42)*, AWWA, Denver, Colo.: This manual provides information on the selection, design, construction, and maintenance of steel tanks for potable water storage.
- AWWA. (2002). *D120-02: Thermosetting fiberglass-reinforced plastic tanks*, AWWA, Denver, Colo.: This document discusses the composition, performance requirements, construction practices and workmanship, design, and methods of testing thermosetting fiberglass-reinforced plastic tanks for the storage of water and other liquids.
- AWWA. (2004). *D110-04: Wire- and strand-wound, circular, prestressed concrete water tanks*, AWWA, Denver, Colo.: This standard details recommended practice for the design, construction, inspection, and maintenance of these types of water tanks.
- AWWA. (2005). *D100-05: Welded carbon steel tanks for water storage*, AWWA, Denver, Colo.: This standard provides guidance to facilitate the design, manufacture, and procurement of welded steel tanks for the storage of water. This standard does not cover all details of design and construction because of the large variety of sizes and shapes of tanks.
- AWWA. (2006). *A100-06: Water wells*. AWWA, Denver, Colo.: This standard provides the minimum requirements for vertical water supply wells, including geologic/hydrologic conditions and water quality and well construction. USEPA WISE Phase 3 Draft (December 2006) is available at http://www.awwa.org/Resources/Content.cfm?ItemNumber=29824#P25_2507.
- American Water Works Association/American Society of Civil Engineers (AWWA/ASCE). (2005). *Water treatment plant design*, 4th ed., McGraw-Hill, New York.: This book is a reference for water treatment plant upgrades or new construction. Topics range from initial plans and permits, through design, construction, and startup.
- Association of State Drinking Water Administrators/National Rural Water Association (ASDWA/NRWA). (2002a). *Security vulnerability self-assessment guide for small drinking water systems*, ASDWA, Arlington, Va.: This guide is intended for water utilities that serve a population of less than 3,300. Its purpose is to help utilities identify critical assets and list appropriate security measures.
- Association of State Drinking Water Administrators/National Rural Water Association (ASDWA/NRWA). (2002b). *Security vulnerability self-assessment guide for small drinking water systems serving populations between 3,300 and 10,000*, ASDWA, Arlington, Va.: This guide is intended for water utilities that serve a population from 3,300 to 10,000. It was developed to help utilities meet the requirements of the U.S. Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107-188).
- ASTM International (ASTM). (2002). *F476-84(2002): Standard test methods for security of swinging door assemblies*, ASTM, West Conshohocken, Pa.: The standard test methods covered in this document are designed to measure the capability of a swinging door assembly to restrain or delay and to frustrate the commission of “break-in” crimes. Door assemblies of various materials and types of construction covered by these test methods also include individual components such as the hinge, lock, door, jamb/strike, and jamb/wall.
- ASTM. (2003). *F1910-98(2003): Standard specification for long barbed tape obstacles*, ASTM, West Conshohocken, Pa.: This specification covers barbed tape materials and configurations used for security barriers. Referenced in this document are ASTM specifications A764, F1379, A176, A666, A370, and A240.
- ASTM. (2004a). *A121-99(2004): Standard specification for metallic-coated carbon steel barbed wire*, ASTM, West Conshohocken, Pa.: This specification describes two-strand, metallic-coated, steel barbed wire fabricated of aluminum, zinc, and zinc-5% aluminum-mischmetal alloy coatings, with a number of coating weights, in a variety of designs.
- ASTM. (2004b). *A176-99(2004): Standard specification for stainless and heat-resisting chromium steel plate, sheet, and strip*, ASTM, West Conshohocken, Pa.: This specification covers stainless and heat-resisting chromium steel plate, sheet, and strip. A wide variety of surface finishes may be available for the steel plate, sheet, and strips described in this specification.
- ASTM. (2005a). *A666: Standard specification for annealed or cold-worked austenitic stainless steel sheet, strip, plate, and flat bar*, ASTM, West

- Conshohocken, Pa.: This specification covers the required annealed and cold-worked conditions for austenitic stainless steels in a variety of structural, architectural, pressure vessel, magnetic, cryogenic, and heat-resisting applications.
- ASTM. (2005b). *A853-04: Standard specification for steel wire, carbon, for general use*, ASTM, West Conshohocken, Pa.: This specification covers carbon steel wire that is intended for general use, and is supplied in coils and is hard drawn, annealed in process, or annealed at finish size.
- ASTM. (2005c). *F1043-06: Standard specification for strength and protective coatings on steel industrial chain link fence framework*, ASTM, West Conshohocken, Pa.: This specification covers the strength and protective coating requirements for industrial steel chain link fence frameworks. Details include the maximum allowable heights of framework, post spacing based the mesh size and gauges of the fence fabric, and specified wind loads. Also included are factors to consider when determining wind load, the cross-sectional shape, and approved fabrication methods for posts and rails.
- ASTM. (2005d). *F552-02: Standard terminology relating to chain link fencing*, ASTM, West Conshohocken, Pa.: This specification contains the standard terminology associated with aspects of chain-link fencing design and construction.
- ASTM. (2005e). *F567-00: Standard practice for installation of chain-link fence*, ASTM, West Conshohocken, Pa.: The standard of practice pertaining to the installation procedure for chain-link fence is described in this document. While this practice describes performance under varying conditions, weather, intended use, materials, etc., it does not address all of the safety problems associated with the installation of a chain-link fence.
- Garcia, M. L. (2001). *The design and evaluation of physical protection systems*, Butterworth-Heinemann, Burlington, Mass.: This book provides detailed information on the full process of security system design and integration, illustrating how the various physical and electronic elements work together to form a comprehensive system.
- Illumination Engineering Society of North America (IESNA). (2003). *Guideline for security lighting for people, property, and public spaces (G-1-03)*, IESNA, New York: This guideline covers basic security principles, illuminance requirements for various types of properties, protocols for evaluating current lighting levels for different security applications, and security survey and crime search methodology. This guideline includes exterior and interior security lighting practices for the reasonable protection of persons and property.
- Jones, G. M., Sanks, R. L., Tchobanoglous, G., and Bosserman, B.E., II, eds. (2005). *Pumping station design*, 3rd ed., Butterworth-Heinemann, Burlington, Mass.: This document provides detailed information needed to design, equip, and build efficient, reliable pumping stations that are easy to operate and maintain.
- Mays, L. R., ed. (2000). *Water distribution systems handbook*, McGraw-Hill, New York.: This handbook provides material to design, analyze, operate, maintain, and rehabilitate water distribution systems. Topics include hydraulic design for pipelines and tanks to water quality issues, computer models, and rehabilitation/replacement information.
- Murphy, B., Radder, L. L., and Kirmeyer, G. J. (2005). *Distribution systems security primer for water utilities*, Water Research Foundation, Denver, Colo.: This document provides tools to assess, prioritize, and address water distribution system vulnerabilities.
- National Association of Clean Water Agencies (NACWA). (2002). *Asset-based vulnerability checklist for wastewater utilities*, NACWA, Washington, D.C.: This document was developed to help wastewater utilities identify and evaluate the vulnerability of their assets, as well as the threats against them. This document was originally developed under NACWA's former name, Association of Metropolitan Sewerage Agencies (AMSA).
- NACWA. (2005). *Vulnerability Self Assessment Tool for Water & Wastewater Utilities* (version 3.2 update), NACWA, Washington, D.C.: Three versions of the Vulnerability Self Assessment Tool (VSAT) software—wastewater, water/wastewater/ and water—can be ordered from NACWA. This tool was originally developed under NACWA's former name, Association of Metropolitan Sewerage Agencies (AMSA).
- National Environmental Training Center for Small Communities (NETCSC). (2002). *Protecting your community's assets: A guide for small wastewater systems*, National Environmental Services Center, West Virginia University, Morgantown: This guide allows decision makers for small wastewater treatment systems to evaluate the security of their systems and to plan for emergencies. Tools provided in the guide include an Inventory of Critical Assets, Threat Assessment, Vulnerability Assessment Checklist, and Prioritization of Potential Corrective Actions.
- National Fire Protection Association (NFPA). (2002). *NFPA 101B: Code for means of egress for buildings and structures*, NFPA, Quincy, Mass.: This code includes the latest technologies, advances, and safety strategies in areas such as alarms, egress, emergency lighting, and special hazard protection. The contents are not meant as a standalone document, but for inclusion in a building code.
- NFPA. (2005). *National electrical code (NFPA 70) handbook*, NFPA, Quincy, Mass.: This code describes the safe installation and use of electrical equipment by consumers.
- NFPA. (2006). *NFPA 101: Life safety code*, NFPA, Quincy, Mass.: This code addresses those egress features necessary to minimize danger to life from fire and smoke, crowd pressures, and movement of individuals and groups. It provides minimum criteria for the design of egress facilities in order to permit prompt escape of occupants from buildings or, where desirable, into safe areas within buildings.
- Naval Construction Battalion Center (NCBC). (1990a). *Federal specification sheet: Fencing, wire and post, metal (chain-link fence gates)* (detail specification RR-F-191/2D), NCBC, Gulfport, Miss.: This document provides detailed requirements for chain-link fence gates and accessories.
- NCBC. (1990b). *Fencing, wire and post metal (and gates, chain-link fence fabric, and accessories)* (general specification RR-F-191/K), NCBC, Gulfport, Miss.: This specification covers general requirements for chain-link fencing and accessories, including classifications for various parts of fencing, wire and post metal, fencing fabric, gates, posts, top rails, braces, and accessories.
- NCBC. (1990c). *Fencing, wire and post, metal (chain-link fence accessories)* (detail specification RRF191/4D), NCBC, Gulfport, Miss.: This specification covers general requirements for chain-link fence accessories, including caps, rail sleeves, brace bands, rail and brace ends, wire ties and clips, tension wires, tension bars, truss rods, barbed wire, barbed wire support arms, and other miscellaneous accessories.
- Naval Facilities Engineering Service Center (NFESC). (1993a). *Design guidelines for physical security of facilities (MIL-HDBK-1013/1A)*, Washington Navy Yard, D.C.: This manual provides guidance to ensure that appropriate physical security considerations are included in the design of general facilities. Aspects considered in this manual include the predesign phase, the assessment of physical security threats, and an overview of the design phase. Specific technical sections in the manual also describe exterior site physical security, building physical security, ballistic attack hardening, standoff weapon hardening, and bomb blast hardening.
- NFESC. (1993b). *Design guidelines for security fencing, gates, barriers, and guard facilities (MIL-HDBK-1013/10)*, Washington Navy Yard, D.C.: This military handbook provides guidance and detailed criteria for the design, selection, and installation of new security fencing, gates, barriers, and guard facilities for perimeter boundaries of Navy and Marine Corps installations or separate activities, and designated restricted areas.
- NFESC. (1999). *Selection and application of vehicle barriers (MIL-HDBK-1013/14)*, Washington Navy Yard, D.C.: This handbook provides guidance to ensure that appropriate design, operational, environmental, cost, security, and safety considerations are included in the selection process for vehicle barrier systems. Topics covered in the handbook include vehicle barrier requirements, vehicle barrier installation and design, and descriptions and data on commercially available vehicle barriers and passive barriers that can be constructed on-site.
- Sandia Corporation. (2002). *Risk assessment methodology for water (RAM-W)*, Sandia Corporation, Albuquerque, N.M.: This document is a two-volume training guide used in RAM-W methodology workshops.
- U.S. Code. (2009). *42 U.S.C. §300(i)(1)*, Office of the Law Revision Counsel, Washington, D.C.: This is U.S. Code Title 42, Section 300i-1, "Tampering with Public Water Systems."
- U.S. Department of Defense (DoD). (2002). *Minimum antiterrorism standards for buildings. Unified Facilities Criteria UFC 4-010-01*, DoD, Washington, D.C.: The Unified Facilities Criteria (UFC) system is prescribed by *MIL-STD 3007* and provides planning, design, construction, sustainment, restoration, and modernization criteria.
- U.S. General Services Administration (GSA). (2005). *Facilities standards for the public buildings service*, GSA, Washington, D.C.: These design standards and criteria are to be used in the programming, design, and documentation of GSA buildings.

Water Security Working Group (WSWG). (2005). *Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on water security practices, incentives, and measures*, WSWG, U.S. Environmental Protection Agency, Washington, D.C.: This report presents the consensus reached by WSWG on 18 findings which (1) establish the features of active and effective security programs; (2) identify ways government and others might encourage utilities to adopt and maintain active and effective programs; and (3) suggest utility-specific and national measures of water sector security progress.

Welter, G. J. (2003). *Actual and threatened security events at water utilities*, Water Research Foundation (WRF), Denver, Colo.: This report documents the security incidents, threats, and hoaxes that have involved or are of direct relevance to water systems. The report includes a review of 264 incidents, classifying them by geographic region, type of attacker, mode of attack, targeted asset, and other categorizations. The report reviews the incidents and discusses specific types of contaminants and the purported motivation of the attackers.

This page intentionally left blank

CONTENTS

	Page
FOREWORD	63
ACKNOWLEDGMENTS	65
 GUIDELINES FOR THE PHYSICAL SECURITY OF WASTEWATER/STORMWATER UTILITIES	
1 Application of Guidelines	67
1.1 Introduction	67
1.1.1 Elements of a Physical Protection System	67
1.1.1.1 Deterrence	67
1.1.1.2 Detection	67
1.1.1.3 Delay	67
1.1.1.4 Response	67
1.1.2 Design Basis Threat	67
1.1.2.1 Vandal	67
1.1.2.2 Criminal	67
1.1.2.3 Saboteur	68
1.1.2.4 Insider	68
1.2 Methodology for Applying These Guidelines	69
1.2.1 Instructions for Applying These Guidelines	69
1.2.1.1 Step 1: Complete Vulnerability Assessment	70
1.2.1.2 Step 2: Characterize the Design Basis Threat	70
1.2.1.3 Step 3: Identify Security Measures	71
1.2.1.4 Step 4: Consider Consequence Mitigation	71
1.2.2 Additional Information to Assist in Applying These Guidelines	71
1.2.2.1 New and Existing Facilities	71
1.2.2.2 Local Codes and Required Aesthetics	72
1.2.2.3 Assets Not Under Utility Control	72
1.2.2.4 Balance of the System	72
1.2.2.5 Value of the Asset	72
1.2.2.6 Levels of Security Measures	72
1.2.2.7 Response Time and Capabilities	72
2 Wastewater Treatment Plants	73
2.1 Scope	73
2.2 Facility Mission	73
2.3 Philosophy of Security Approach	73
2.4 Special Considerations for Critical Assets	73
2.5 Benchmark Security Measures	74
3 Collection Systems	79
3.1 Scope	79
3.2 System Mission	79
3.3 Philosophy of Security Approach	79
3.4 Benchmark Security Measures	79
4 Pumping Stations	83
4.1 Scope	83
4.2 Facility Mission	83
4.3 Philosophy of Security Approach	83
4.4 Benchmark Security Measures	83
5 Wastewater/Stormwater System Support Facilities	87
5.1 Scope	87
5.2 Facility Mission	87

5.3	Philosophy of Security Approach	87
5.4	Benchmark Security Measures	87
Appendix A Physical Security Elements		93
A.1.0	Fencing and Perimeter Walls	93
A.1.1	Chain-Link Fencing	93
A.1.2	Anti-Climb/Anti-Cut Fencing	93
A.1.3	Ornamental Fencing	93
A.1.4	Perimeter Wall	94
A.1.5	Fencing Topping	94
A.1.6	Perimeter Line	94
A.1.7	Fence Foundation Enhancements	94
A.2.0	Gates	94
A.2.1	Chain-Link Gates	94
A.2.2	Electronic Gate Opening	94
A.2.3	Electronic Gate Control System	95
A.3.0	Site Areas	95
A.3.1	Clear Zones	95
A.3.2	Site Utilities	95
A.4.0	Facility Entrances	95
A.4.1	Sallyport Entrances	95
A.4.2	Building Entrances	96
A.5.0	Bollards and Other Vehicle Barriers	96
A.6.0	Exterior Surfaces	96
A.7.0	Outdoor Security Lighting	96
A.8.0	Signage	96
A.8.1	Fence Signage	96
A.8.2	Primary Site Entrance Signage	96
A.8.3	Water Intake Delineation	97
A.9.0	Electronic Security Systems	97
A.9.1	Intrusion Detection Sensors: General	97
A.9.2	Exterior Intrusion Detection	97
A.9.2.1	Active Infrared Sensors	97
A.9.2.2	Microwave Sensors	97
A.9.2.3	Dual-Technology Sensors	97
A.9.2.4	Buried Line Sensors	97
A.9.2.5	Fence-Mounted Sensors	97
A.9.3	Interior Intrusion Detection	98
A.9.3.1	Dual-Technology Motion Sensors	98
A.9.3.2	Linear Beam Sensors	98
A.9.3.3	Glass-Break Sensors	98
A.9.4	Door and Hatch Contact Alarm Switches	98
A.9.5	Pipeline Vibration Detection	98
A.10.0	Access Control Systems	98
A.10.1	Access Control Systems: General	98
A.10.2	Locks and Padlocks	98
A.10.3	Numeric Keypad Locks	98
A.10.4	Card Reader Systems	98
A.11.0	Closed-Circuit Television (CCTV) Surveillance	99
A.11.1	General Considerations	99
A.11.2	Field of View	99
A.11.3	CCTV Housings and Mounts	99
A.11.4	Video Network Servers	99
A.11.5	Digital Video Recorders	99
A.11.6	CCTV Computer Application Software	100
A.12.0	Security, Controls, and SCADA Wiring	100
A.12.1	SCADA and Electrical Control Panel Enclosures	100
A.13.0	Building Elements	100
A.13.1	General	100
A.13.2	Doors	100
A.13.3	Security Grilles	100
A.13.4	Security Cages	100
A.14.0	Hatches/Vaults and Vents	100
A.14.1	Hatch, Vault, and Vent Alarms: General	100

A.14.2	Roof or Sidewalk Hatches	100
A.14.3	Roof Vents	101
A.14.4	Vault Hatch with Elevated Curb	101
A.14.5	Vault Door Hatch Set Flush with Top of a Structural Slab.	101
A.15.0	Online Water Quality Monitoring	101
A.16.0	Operator Devices	101
A.16.1	Man-Down Transmitter	101
A.17.0	Chemical Fill-Line Locking Devices	101
A.18.0	Hydrants	101
A.19.0	Manholes.	101
GLOSSARY AND ABBREVIATIONS		103
REFERENCES		107
INDEX		111

This page intentionally left blank

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 , and were published initially as a proposed draft, *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006). That consensus process included balloting by a balanced Standards Committee and reviewing during an ASCE 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 common U.S. 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 wastewater collection and treatment systems (also called sanitary sewer collection and treatment systems) and stormwater 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. These 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 through ASCE's and AWWA's American National Standards Institute (ANSI)-accredited standards development process and were published initially as *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006). The primary reviewers were members of the Wastewater and Stormwater 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 wastewater and stormwater 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 features, 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 these guidelines 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 wastewater or stormwater 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, with 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 5.0 (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 standalone documents. Most of the tables and figures of these guidelines were taken directly from ASCE/AWWA/WEF (2006) as cited herein.
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 otherwise 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 wastewater/stormwater 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 this guidance document, 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 intended to assist wastewater and stormwater 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 Wastewater/Stormwater 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., D.E.E.
Erica M. Brown
Jeanette A. Brown, P.E., B.C.E.E.
Jonathan W. Bulkley, Ph.D., P.E.
Ivan Burrowes
James 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. Mc Laughlin, 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, MPH
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.

Wastewater/Stormwater Subcommittee

William C. Boyle, Ph.D., P.E., B.C.E.E.,
Vice Chair
Jeanette A. Brown, P.E., B.C.E.E., Chair
Daniel D. Clark
James Conboy, P.E., B.C.E.E.
Findlay G. Edwards, Ph.D., P.E.
Dale D. Gabel, P.E.
C. Dale Jacobson, P.E., B.C.E.E.
Daniel L. Lynch, P.E., B.C.E.E.
Stacy Passaro, P.E., B.C.E.E. (WEF)
Jeffrey W. Talley, Ph.D.

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 WISE SC
Conrad G. Keyes Jr., ScD, 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. Mc Laughlin, 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., D.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

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

This page intentionally left blank

Guidelines for the Physical Security of Wastewater/Stormwater Utilities

Chapter 1 APPLICATION OF GUIDELINES

1.1 INTRODUCTION

These wastewater/stormwater utilities guidelines recommend physical and electronic security measures for physical protection systems to protect against identified adversaries, referred to as the 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 2004b): 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 also 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 similar plan.

Figure 1-1 illustrates the interaction of detection (at the perimeter fence and facility entrance door), delay (fence, exterior door, interior door), and 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 wastewater/stormwater treatment or collection processes, contaminate the wastewater, or trespass on the wastewater/stormwater 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 these guidelines. 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 the level of desperation or sophistication, criminals may be armed and willing to injure or kill to accomplish their objectives.

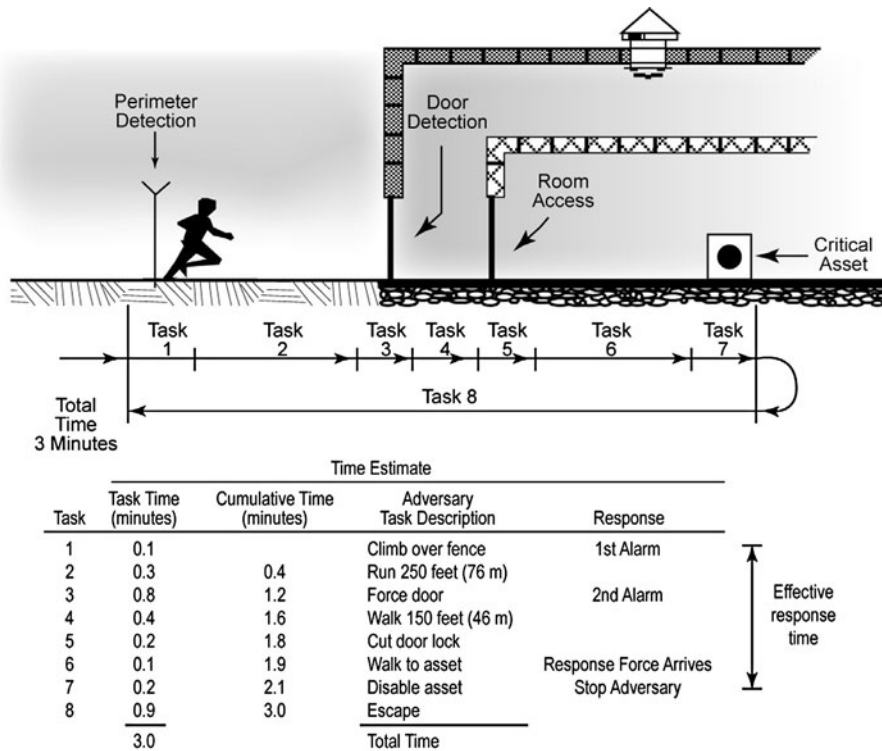


FIGURE 1-1. CONCEPT OF DELAY CALCULATION.
Source: Adapted from Garcia (2001), with permission. © Elsevier.

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 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 wastewater 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 wastewater 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 environment, 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

Table 1-1 Design Basis Threat Capability Matrix (ASCE/AWWA/WEF 2006)

Characteristic	Vandal		Criminal		Saboteur		Insider	
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	
	Base	Enhanced	Base	Enhanced	Base	Enhanced	Base	Enhanced
Planning/system knowledge	Little or none	Possible	Little, opportunistic	Definite	Definite	Definite	Limited access to equipment, facilities, SCADA, or computer 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-automatic weapons, 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, crowbars), 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.

(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 to ensure that 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 5.0 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 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.

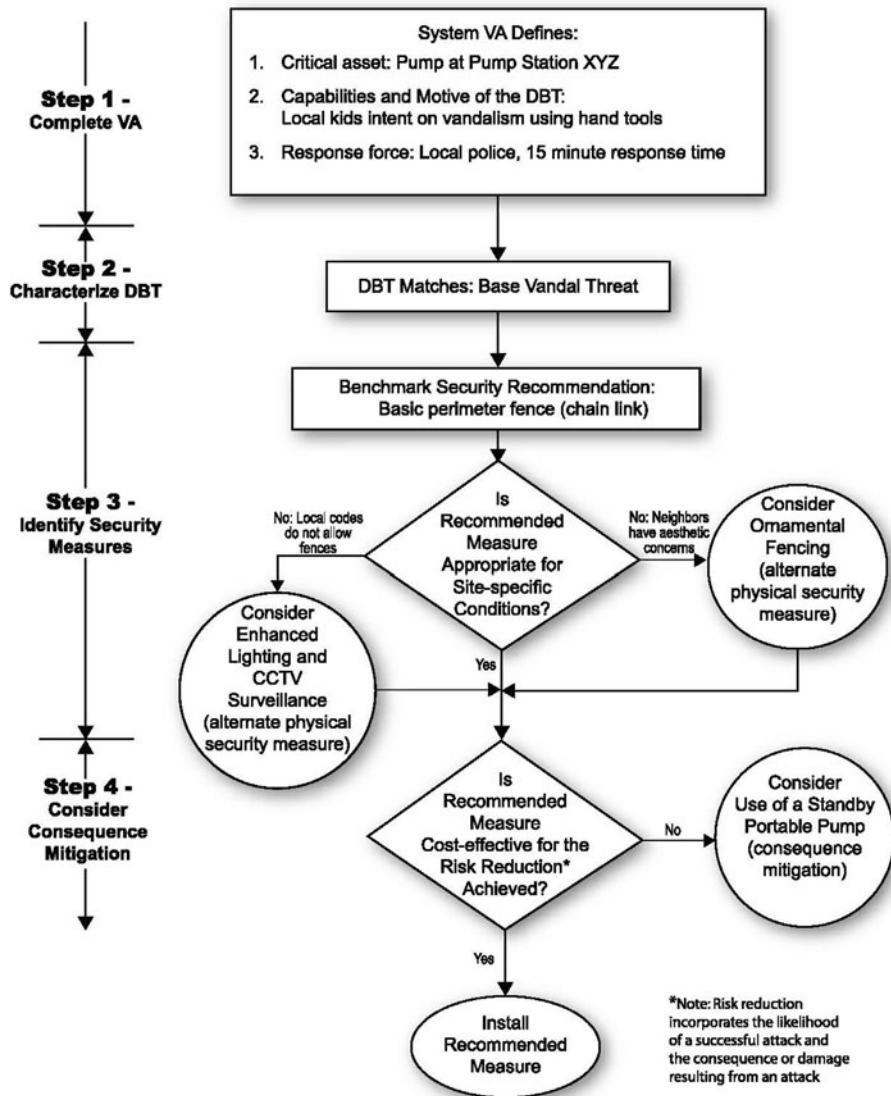


FIGURE 1-2. EXAMPLE DECISION TREE.
Source: ASCE/AWWA/WEF (2006).

1.2.1.1 Step 1: Complete Vulnerability Assessment

1. Complete a wastewater/stormwater 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
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

tion 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 the 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

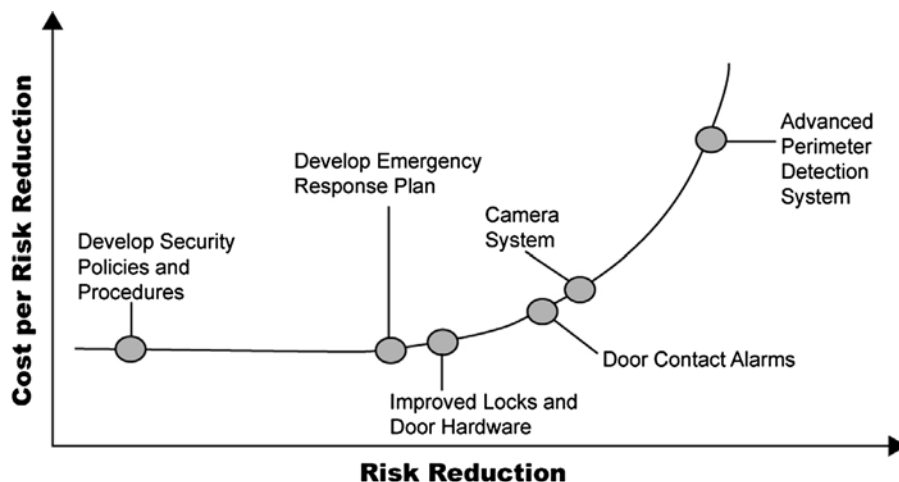


FIGURE 1-3. TYPICAL COST-TO-RISK REDUCTION CURVE.
Source: ASCE/AWWA/WEF (2004b).

category (more than one may be selected): vandal, criminal, saboteur, or insider.

2. Within each of these DBT categories (see 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 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 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 risk reduction associated with implementing additional security measures is marginal. Management and operational measures to lower consequences are important elements of a utility or facility security plan (ASCE/AWWA/WEF 2004b) 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; locating redundant critical assets in nonadjacent areas; and replacing large-diameter pipes with multiple smaller-diameter pipes that are too small for an individual to enter and that together can carry the entire design flow.

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

WASTEWATER TREATMENT PLANTS

2.1 SCOPE

This guideline covers wastewater treatment plants used within a municipal wastewater system. It establishes benchmark physical and electronic security features for protecting a wastewater 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 contaminant that severely impedes wastewater treatment or renders the facilities unusable. A wastewater treatment plant that cannot provide adequate capacity or performance due to a malevolent activity could discharge an effluent with significantly impaired quality that may create a public health hazard or cause environmental damage of the downstream receiving water or receiving environment. Employee safety and public health concerns can be caused by the intentional release of hazardous chemicals or toxic gasses, or by damaging ventilation and other life-safety control features. The potential for malevolent individuals to create intentional fire and explosive hazards are additional concerns that may require security features.

2.2 FACILITY MISSION

The mission of this type of facility is to treat the incoming wastewater to an environmentally and public health-acceptable level before discharging to a receiving body of water or other system. Wastewater treatment plants typically include below-grade, ground level, and elevated structures, tankage, and buildings with typical throughput capacities ranging from 1,000 gal/day (3.8 m³/day) to more than 1 billion gal/day (>3,800,000 m³/day). Large wastewater treatment plants are routinely staffed on a continuous basis; small facilities are likely to be staffed by operations and maintenance personnel only periodically to perform maintenance activities, conduct process monitoring, collect environment samples, or 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 the WEF Manual of Practice No. 8: *Design of Municipal Wastewater Treatment Plants*, 4th Ed., [WEF 1998; this is the same as ASCE Manuals and Reports on Engineering Practice No. 76 (ASCE 1998)], and WEF Manual of Practice 11: *Operation of Municipal Wastewater Treatment Plants*, 6th Ed. (WEF 2005).

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 Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2004b) and are not addressed here.

2.4 SPECIAL CONSIDERATIONS FOR CRITICAL ASSETS

Special considerations should be provided for security of the extremely critical or hazardous assets or facilities identified in the VA. These assets may be the target of a DBT that is more capable than the DBT for the remainder of the wastewater treatment plant, thus the 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. Typical critical assets of wastewater treatment plants that should be considered for more robust or enhanced security measures include:

- *Toxic gas storage facilities* such as chlorine, sulfur dioxide, and ozone
- *Facilities for storage and use of combustible/flammable materials* such as methane, gasoline, propane, methanol, and oxygen storage facilities and natural gas metering and connections
- *Power equipment and systems* such as electrical switchgear, transformers, substations, generators, and motor control centers
- *Major mechanical systems* such as influent, effluent, and in-plant pumping stations, and blowers
- *SCADA, security and communication systems* such as network, supervisory control and data acquisition (SCADA), and security servers, and radio, microwave, and telephone communications

2.5 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
- 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
- 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 wastewater 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. Appendix A provides additional details on security measures (specific sections are referenced in Table 2-1 where applicable).

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER 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
Intercom and remotely controlled electronic gate lock for visitors	●	●		✓		✓		✓		✓	2.2, 2.3
Vehicle sally port gate entrance for delivery vehicles	●	●				✓	✓	✓			4.1
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 feet [15 meters])			✓	✓	✓	✓	✓	✓			8.1
Site (area between perimeter and facilities)											
Motion-activated lighting		●		✓		✓	✓	✓			7.0 (9)
Perimeter minimum clear zone distance	●	●		✓		✓	✓	✓			3.0

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER 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 feet (9 meters away)	•							✓			
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	•			✓		✓	✓	✓			
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)—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	•		✓	✓					✓		19.0
Manholes—intrusion detection on lock	•	•		✓				✓		✓	
Minimize exterior signage indicating the presence or locations of assets	•		✓	✓			✓	✓			
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

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER 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	
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, 13.1
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)	•	•						✓			
Visitor waiting area	•	•				✓		✓			14.2
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
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	•						✓	✓	✓		13.4
Generator (indoor)—locked protective barrier or cage	•					✓	✓	✓	✓		13.4
Switchgear/motor control center (indoor)—locked protective cage	•						✓	✓	✓		13.4
Chemical fill lines at building exterior—locked access	•			✓	✓		✓	✓	✓		17.0
Chemical fill lines at building exterior—locked access with intrusion detection	•	•				✓		✓		✓	17.0
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

TABLE 2-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER 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	
Water Quality Monitoring											
Online 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)
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.

This page intentionally left blank

Chapter 3

COLLECTION SYSTEMS

3.1 SCOPE

This guideline covers the collection and conveyance components of wastewater and stormwater systems. This section establishes benchmark physical and electronic security features for protecting these systems from vandal, criminal, saboteur, and insider threats. Threats and malevolent acts of concern include damage or destruction of individual facilities or equipment, release of untreated wastewater into the environment, or use of the collection system as a conduit to reach buildings or other targets of malevolent action.

3.2 SYSTEM MISSION

The mission of these facilities is to collect and convey wastewater from its origins in the community to wastewater treatment facilities or to convey stormwater to treatment or to discharge points. They include pipelines, culverts, conveyance tunnels, manholes, isolation and control valves, air release valves, combined sewer structures, stormwater inlets, and catch basins, stormwater outfall structures, stormwater retention/detention basins, and related items. These facilities are distributed throughout the community that is served by the utility and rarely have defined individual facility perimeters. Most pipelines and valves are buried and therefore are out of sight of the public. However, every customer has a direct connection to the wastewater system through their service line, and manholes that provide access to the wastewater and stormwater systems are prevalent throughout the community.

More detailed information on specific functions and features of wastewater and stormwater collection systems is contained in the following documents:

- *Gravity Sanitary Sewer Design and Construction*, WEF Manual of Practice No. FD-5 and ASCE Manuals and Reports on Engineering Practice No. 60 (WEF 2007; ASCE 2007)
- *Wastewater Collection Systems Management*, Manual of Practice No. 7, 5th Ed. (WEF 1999)
- *Design and Construction of Urban Stormwater Management Systems*, WEF Manual of Practice No. FD-20 and ASCE Manuals and Reports on Engineering Practice No. 77 (WEF 1992; ASCE 1992)
- *Standard Guidelines for the Design, Installation, Maintenance and Operation of Urban Stormwater Systems*, ASCE/EWRI 45-05, 46-05, 47-05 (ASCE 2006)

3.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for collection systems 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. For a saboteur DBT, an enhanced response force with superior numbers and weapons would typically be required.

DBTs considered in this guideline include vandals, criminals, saboteurs, and insiders. Characteristics and capabilities of the two levels of DBT 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 Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2004b) 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:

- System Structures
- Water Quality Monitoring
- Closed-Circuit Television—Alarm Assessment (fixed 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 collection systems. Systems 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).

Collection systems present challenges in developing adequate detection and delay approaches, as many facilities are not constructed with defined perimeters or site areas where access can be controlled and are frequently open to the public. Section 2.0, Wastewater Treatment Plants, and Section 4.0, Pumping Stations, provide guidelines for protecting facilities

with defined perimeters and site areas. For the elements of the collection systems without defined perimeters and site areas, a utility may elect to selectively apply the recommended security measures on a subset of their assets, the most critical assets, based on the results of their VA or similar risk assessment evaluation.

TABLE 3-1 BENCHMARK SECURITY MEASURES FOR COLLECTION SYSTEMS (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	
System 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
Exposed pipelines and forcemains: provide fence barrier to limit access to appurtenances	•			✓							
Exposed pipelines and forcemains: bury or install in hardened carrier pipes for double-wall protection	•						✓				
Exposed pipelines and forcemains: bury or install in hardened carrier pipes and vibration/motion detection	•	•						✓		✓	
Route sewers such that they are not located under critical infrastructure or potential targets						✓		✓		✓	
Locking covers for control, air relief, and other valves	•			✓			✓		✓		
Locking covers with intrusion detection for control, air relief, and other valves	•	•				✓		✓		✓	
Pan-type manhole cover locks	•		✓						✓		19.0
Bolt-type manhole cover locks	•			✓			✓		✓		19.0
Tack-weld manhole covers with motion detection	•	•						✓		✓	19.0
In existing system, mount bar screens or horizontal bars on catch basins, curb inlets, and pipe inlets and outlets	•		✓								
Mount bolt-type locking devices on catch basins, curb inlets, and pipe inlets and outlets	•			✓			✓		✓		

TABLE 3-1 BENCHMARK SECURITY MEASURES FOR COLLECTION SYSTEMS (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	
Weld screen and bars on catch basins, curb inlets, and pipe inlets and outlets and install motion detection	•	•						✓		✓	
Hardened key locked accessways for deep tunnels	•		✓		✓		✓		✓		
Electronic access-controlled for deep tunnel accessways	•	•		✓		✓		✓		✓	
Motion detection or intrusion alarms for deep tunnel accessways		•		✓		✓		✓		✓	
Thermal imaging devices in access shafts and tunnels		•						✓		✓	
Water Quality Monitoring											
On-line water quality monitoring		•					✓	✓		✓	15.0
Closed Circuit Television—Alarm Assessment (fixed cameras)											
CCTV—Hatches, vaults, structure doors		•		✓		✓	✓	✓		✓	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) connections	•							✓		✓	
SCADA—Physical Security											
Locked PLC/RTU enclosure(s)	•		✓	✓	✓	✓	✓	✓	✓		13.1
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.

This page intentionally left blank

Chapter 4

PUMPING STATIONS

4.1 SCOPE

This guideline covers pumping stations used within a wastewater collection system (often called a sanitary sewer or sewerage system) or within a stormwater system. It establishes benchmark physical and electronic security features for protecting a pumping station (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 the pumping station equipment that causes an uncontrolled release of the wastewater or stormwater creating a public health hazard or environmental damage. Additional threats include introduction of a chemical, radiological, or biological contaminant that severely impedes or damages downstream sewer lines and treatment processes that may ultimately contaminate the water or environmental system receiving the treatment plant’s discharge.

4.2 FACILITY MISSION

The mission of this facility is to pump raw wastewater or stormwater to a treatment facility, another pumping station, or to a sewer line at a higher elevation. Pumping stations typically comprise both below-grade and at-grade facilities with capacities ranging from 1,000 gal/day (3.8 m³/day) to more than 1 million gal/day (>3,800 m³/day). Although larger pumping stations may be routinely staffed on a continuous or part-time basis, more frequently operations and maintenance staff only visit these facilities periodically to perform maintenance activities or to respond to failure alarms. Although typically isolated from the general public, these facilities can be located in residential, park-like settings, or in the midst of denser populated urban areas. Due to safety concerns, the public generally has no direct access.

More detailed information on pumping station functions and features is contained in the *Design of Wastewater and Stormwater Pumping Stations*, WEF Manual of Practice No. FD-4 (WEF 1993).

4.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for 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. For a saboteur DBT, an enhanced response force with superior numbers and weapons would typically be required.

DBTs considered in this section include vandals, criminals, saboteurs, and insiders. Characteristics and capabilities of the two levels of DBT 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 Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2004b) 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 pumping stations. Pumping stations 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 4-1 where applicable).

TABLE 4-1 BENCHMARK SECURITY MEASURES FOR 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
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 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- 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	●			✓		✓	✓	✓			
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

TABLE 4-1 BENCHMARK SECURITY MEASURES FOR 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	
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 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, 13.1
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
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
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	•						✓	✓	✓		13.4

TABLE 4-1 BENCHMARK SECURITY MEASURES FOR 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	
Generator (indoor)—locked protective barrier or cage	•					✓	✓	✓	✓		13.4
Switchgear/motor control center (indoor)—locked protective cage	•						✓	✓	✓		13.4
Chemical fill lines at building exterior—locked access	•			✓	✓		✓		✓		17.0
Chemical fill lines at building exterior—locked access with intrusion detection	•	•				✓		✓		✓	17.0
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											
Online 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)
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

WASTEWATER/STORMWATER SYSTEM SUPPORT FACILITIES

5.1 SCOPE

This guideline presents guidance for security for support facilities that are part of wastewater and stormwater systems. It establishes benchmark physical and electronic security features for protecting support facilities from vandal, criminal, saboteur, and insider threats. Threats and malevolent acts of concern include damage or destruction of individual facilities or critical assets within facilities.

5.2 FACILITY MISSION

Wastewater/stormwater system support facilities include administrative buildings, maintenance yards, sites for material and vehicle storage, laboratories, and septage disposal facilities. The common element linking these facilities is that they are not in direct contact with the wastewater or stormwater. If a facility such as a laboratory or storage yard is located at the wastewater treatment plant, then the security guideline for wastewater treatment plants (Section 2) should be referenced. This guideline applies to those facilities that are not located at a treatment plant, or pumping station, or otherwise in direct contact with the wastewater or stormwater. Because support facilities are located apart from the water flow, they have a low risk for being avenues of intentional contamination of the wastewater or stormwater.

Support facilities may also have the following common factors that are often different from other system facilities:

- Large number of people entering and leaving the facility, including the public
- High vehicle traffic
- Fuel tanks to supply utility fleet
- In the case of laboratories, may house chemicals or even pathogens that are used in tests
- May be symbolic of the utility's image, such as a headquarters facility
- May provide storage for utility vehicles, which as moving assets, present unique challenges
- May be combined with other government facilities, such as an administrative facility within the city hall or a maintenance yard combined with other city maintenance functions

The assets in a support facility may include maps, supervisory control and data acquisition (SCADA)/controls, reports, cash, business systems, heavy and mobile equipment, and tools.

5.3 PHILOSOPHY OF SECURITY APPROACH

An effective security approach for support 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 Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2004b) 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 (✓). 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
- 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 wastewater/stormwater support 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 5-1 where applicable).

Special considerations should be provided for security of extremely critical assets or facilities such as SCADA, security equipment, and network computer servers, hubs and related systems, and dangerous chemicals and pathogens located in analytical laboratories.

**TABLE 5-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER/STORMWATER SYSTEM SUPPORT 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- 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
Minimize vehicle access points and/or number of entrance gates	●	●			✓	✓	✓	✓			
Key-locked entrance gate	●		✓		✓		✓		✓		2.1, 10.2
Electronic access-controlled entrance gate	●	●		✓		✓		✓		✓	2.2, 2.3, 10.3, 10.4
Intercom and remotely controlled electronic gate lock for visitors	●	●		✓		✓		✓		✓	2.2, 2.3
Vehicle sallyport gate entrance for delivery vehicles	●	●				✓	✓	✓			4.1
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
Locate public or visitor parking as far away from the facility as practical, but at least 30 ft (9 m) away	●							✓			
Eliminate parking underneath facilities	●							✓			
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		●					✓	✓		✓	1.6, 3.0, 7.0, 9.1, 9.2, 11.0
Foundation enhancements for second layer of fencing	●						✓	✓			1.7

**TABLE 5-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER/STORMWATER SYSTEM SUPPORT 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 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
Fuel storage tanks located at least 100 feet (30 meters) from all buildings and away from perimeter fence lines	•						✓	✓			
Landscaping that does not obscure building or other assets		•	✓	✓	✓	✓	✓	✓	✓	✓	1.6, 3.0 (3)
Minimize exterior signage indicating the presence or locations of assets	•		✓	✓			✓	✓			
Facility Structures											
Industrial-type, tamper-resistant door hinges	•			✓	✓	✓	✓	✓			
Key-locked entrance door	•		✓		✓				✓		10.1, 10.2, 13.2 (6)(c)
Exterior doors with status switch contact alarmed to security		•		✓		✓	✓	✓	✓	✓	9.4, 13.2
Electronic access-controlled entrance door	•	•		✓		✓	✓	✓	✓	✓	9.4, 10.4, 13.2
Automatic locking critical interior doors with access control	•	•				✓	✓	✓	✓	✓	10.1, 10.3, 10.4, 13.2
Blast-resistant exterior doors ^b	•							✓			
Double entry system or secured lobby entry (mantrap)	•	•						✓			
Visitor waiting area	•	•				✓		✓			14.2
Provide dedicated meeting room located outside secured interior for meetings with visitors or vendors	•					✓		✓			

**TABLE 5-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER/STORMWATER SYSTEM SUPPORT 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	
Design building circulation to provide unobstructed views of people approaching controlled areas or critical assets		•		✓		✓		✓			
Bollards or vehicle barriers protecting vehicle and personnel doors	•					✓		✓			5.0
Break-resistant glass	•		✓	✓	✓	✓	✓				
Blast-resistant windows ^b	•							✓			
Interior motion detection		•				✓	✓	✓	✓	✓	9.3
Do not locate windows next to doors so that intruders could unlock the doors through them	•		✓	✓	✓	✓	✓	✓			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	•						✓	✓	✓		13.4
Generator (indoor)—locked protective barrier or cage	•					✓	✓	✓	✓		13.4
Switchgear/motor control center (indoor)—locked protective cage	•						✓	✓	✓		13.4
Chemical fill lines at building exterior—locked access	•	•		✓	✓		✓		✓		
Chemical fill lines at building exterior—locked access with intrusion detection	•	•				✓		✓		✓	
Chemical storage (indoor)—locked access	•						✓		✓		13.1
Chemical storage (indoor)—locked with intrusion detection	•	•				✓		✓		✓	10.1, 10.3, 10.4, 13.1
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

**TABLE 5-1 BENCHMARK SECURITY MEASURES FOR WASTEWATER/STORMWATER SYSTEM SUPPORT 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	
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	•							✓		✓	
Incoming site utilities—harden power, gas, water, waste and their facility entry points.	•							✓			
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.

This page intentionally left blank

Appendix A

PHYSICAL SECURITY ELEMENTS

The design of any security measure must always take safety and maintenance considerations into account.

This guideline applies 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.

A.1.0 FENCING AND PERIMETER WALLS

The primary goals of fencing and perimeter walls are to establish a legal demarcation by defining the perimeter boundaries of a facility; to present a barrier that causes an intruder to make an overt action to penetrate that demonstrates intent; and to create a delay barrier against unauthorized access.

Secondary goals may include screening the facility against visual observation; establishing a clear zone that enhances lighting and surveillance; and providing a means to install intrusion detection sensors.

A.1.1 Chain-Link Fencing. For terms related to chain-link fencing systems, refer to ASTM F552, *Standard Terminology Relating to Chain Link Fencing* (ASTM 2005d). For detailed specifications and design information related to chain-link fencing and posts, refer to *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b), and *Federal Specification RR-F-191/2D, Fencing, Wire and Post, Metal (Chain-Link Fence Gates) (Detail Specification)* (NCBC 1990a). Both documents have been approved for public release and are available online. Aluminum fabric, poles, or accessories are not recommended for security applications.

The base-level fence guideline is galvanized steel chain-link fence post with a 6-ft (1.8-m) or greater fabric height. The enhanced-level fence guideline is galvanized steel chain-link fence post with an 8-ft (2.4-m) or greater fabric height.

Fence fabric should be one piece and should be coated with zinc or polyvinyl chloride (PVC). PVC over zinc-coated steel is recommended in harsh, corrosive environments.

The base-level fabric wire gauge should be a minimum standard No. 9 wire gauge and mesh pattern of 2-in. (50-mm) diamond mesh or smaller.

Enhanced-level chain-link fencing should comply with the requirements for the base-level guideline chain-link fencing, except using No. 6 or No. 8 gauge fencing fabric in place of No. 9 gauge, and mesh patterns 1 in. (25 mm) or less across.

Post strength and stiffness for base-level and enhanced-level chain-link fences should meet ASTM F1043, *Standard Specification for Strength and Protective Coatings on Steel Industrial Chain Link Fence Framework*, Group 1A requirements (ASTM 2005c) for heavy industrial fences. Follow the manufacturer's standard with allowance for minimum embedment below finished grade.

The average distance between line posts for chain link fences is recommended to be no more than 10 ft (3 m) when measured center-to-center between posts and parallel to the fence grade

(ASIS 2004, Chapter 3—Chain Link Fencing). For additional guidance on installing chain-link fencing, refer to *RR-F-191K/GEN, Fencing, Wire, and Post Metal (and Gates, Chain-Link Fence Fabric, and Accessories) (General Specification)* (NCBC 1990b); ASTM F567, *Standard Practice for Installation of Chain-Link Fence* (ASTM 2005e); and *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b) for guidelines on connection of fencing mesh to posts for security applications.

The American Society of Industrial Security (ASIS) *Protection of Assets* manual (ASIS 2004) further identifies that post hole depths be a minimum of 24 in. (610 mm), plus an additional 3 in. (76 mm) for each 1-ft (0.3-m) increase in fence height over 4 ft (1.2 m), such that an 8-ft (2.4-m) fence requires a 36-in. (910-mm) depth for post holes. The hole should be backfilled with concrete into the excavation hole [2,500 lb/in.² (psi) (17,000 kPa)] and the concrete extended 2 in. (50 mm) above grade, with a crowned surface to shed water.

Where fences cross a stream, culvert, swale, depression, or other openings that fencing does not enclose, where the opening size is 96 in.² (62,000 mm²) or larger, these openings should be protected by additional grilles, fencing, or other barriers against penetration. Refer to Section 13.3 of this Appendix and to *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b), for recommendations and construction of grilles.

A.1.2 Anti-Climb/Anti-Cut Fencing. If the DBT warrants, a specialized anti-climb/anti-cut fence such as wire-panel mesh fencing should be considered.

Wire-panel mesh fabric wire gauge should be a minimum of No. 8 wire gauge.

Wire-panel mesh pattern should be non-climbable, with a 0.5-in. by 3-in. (13-mm by 76-mm) mesh pattern, welded at each intersection.

Fabric wire should conform to ASTM A853-04, *Standard Specification for Steel Wire, Carbon, for General Use*, Grade AISI 1006 as specified by the American Iron and Steel Institute (AISI) (ASTM 2005b). After welding, the fabric is hot-dipped and galvanized with a zinc coating followed by a PVC coating.

A.1.3 Ornamental Fencing. Site conditions and local codes may dictate the use of aesthetically pleasing fence materials. In such cases, ornamental fences of steel, aluminum, or wrought iron should be considered.

As an example of aluminum fencing meeting the requirements, base-level ornamental fence should be a picket fence, 8-ft (2.4-m) picket height or greater, constructed of HS-35 aluminum alloy. Nominal picket spacing should be 5 in. (130 mm) on center or less. Pickets may include spiked tops, depending on the DBT.

Suggested minimum sizes for fence pickets are 1 in. (25 mm) square by 0.062 in. (1.6 mm) thick, while suggested minimum fence rail dimensions are 1.625 in. (41 mm) by 0.070 in.

(1.8 mm) thick top walls, and 1.625 in. (41 mm) by 0.100 in. (2.54 mm) thick side walls.

Line posts for aluminum ornamental fences should be constructed of HS-35 aluminum alloy, with suggested dimensions of 2.5 in. (64 mm) square by 0.075 in. (1.9 mm) thick. Follow the manufacturer's standard with allowance for minimum embedment below finished grade.

Gate posts for aluminum ornamental fences should be constructed of HS-35 aluminum alloy of minimum dimensions 6 in. (150 mm) square by 0.125 in. (3.2 mm) thick. Follow the manufacturer's standard with allowance for minimum embedment below finished grade.

Fencing should have a powder-coated finish or other appropriate protective finish.

A.1.4 Perimeter Wall. The need for solid perimeter walls, such as concrete masonry walls, may be dictated by the DBT, hardening needs, aesthetics, or the desire to fully screen a facility or asset from outside view. In those instances where hardening and aesthetics are both objectives, hardened (or crash-resistant) ornamental fencing is available.

A base-level concrete masonry unit (CMU) wall height should be 6 ft (1.8 m) or greater. An enhanced-level CMU wall height should be 8 ft (2.4 m) or greater. Wall thickness should be 8 in. (200 mm) as a suggested minimum, with additional thickness as required to meet hardened designs.

Intermediate wall columns should be spaced per design criteria and site conditions.

Corner columns should be positioned where directional changes in wall alignment occur.

Wall foundation and reinforcement should be provided per local design criteria and geotechnical conditions.

A sheer exterior surface should have no protruding, climbable edges.

A.1.5 Fencing Topping. Fence topping may include barbed-wire topping or concertina barbed-wire tape topping, or a combination of both.

For base-level barbed-wire topping, attach a three-strand of barbed wire, conforming to ASTM A176, *Standard Specification for Stainless and Heat-Resisting Chromium Steel Plate, Sheet, and Strip* (ASTM 2004b) and ASTM A666, *Standard Specification for Annealed or Cold-Worked Austenitic Stainless Steel Sheet, Strip, Plate, and Flat Bar* (ASTM 2005a) for a 1-ft (0.3-m)-high single outrigger; for enhanced-level climb resistance, use double Y-style outriggers with three-strand barbed wire.

For concertina-wire topping, attach 12-gauge stainless steel wires to 2-ft (0.6 m)-high double Y-style outriggers. Concertina wire should conform to ASTM F1910, *Standard Specification for Long Barbed Tape Obstacles* (ASTM 2003), and should be 24-in. to 30-in. (610 to 760 mm)-diameter double-coil concertina type. Each concertina loop should consist of 43 ± 2 clusters of needle-sharp barbs on 4-in. (100-mm) centers, each barb measuring a minimum of 1.2 in. (30 mm) in length.

Refer to ASTM A121, *Standard Specification For Metallic-Coated Carbon Steel Barbed Wire* (ASTM 2004a) and *Federal Specification RR-F-191/4D, Fencing, Wire, and Post, Metal (Chain-Link Fence Accessories)* (NCBC 1990c) for installation guidance.

Ornamental fencing with angled "pikes" can be provided as a fence topping to discourage or prevent access to a facility by climbing.

A.1.6 Perimeter Line. Periodic treatment of the perimeter line is recommended to prevent vegetation growth.

Provide a 1-ft (0.3-m)-wide vegetation-free zone with the fence or wall placed in the center of zone, using a 2-in. (50-mm)-thick layer of 0.375-in. to 0.75-in. (10-mm to 19-mm) aggregates, and treat with herbicide.

A.1.7 Fence Foundation Enhancements. To prevent stretching of the fence fabric to allow an adversary to move under the fence, it may be appropriate to anchor the bottom fabric of the fence to create a delay similar to that of solid fencing. For anchorage of fabric, the bottom of the fence fabric should be secured to a bottom rail and securely anchored at the midpoint between the fence posts along the fence line. For the base-level threat guideline, the bottom rail may be anchored to an eyebolt embedded in a "deadman" anchor, a concrete cube 3 ft by 3 ft (0.9 m by 0.9 m) as described in *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b); the deadman should be buried in the soil below the fence rail. As an alternative, 12-in. (300-mm)-deep rows of metal bars or pickets may be embedded at 12-in. (300-mm) intervals along the base of the fencing.

For the enhanced-level guideline to prevent tunneling under fences, provide a continuous concrete curb at the base of the fence 8 in. (200 mm) wide by 24 in. (610 mm) deep. The maximum clearance between the bottom rail and the top of the grade strip should be no more than 2 in. (50 mm) maximum clearance, with the bottom rail of the fencing secured to the concrete strip at the mid-point between the posts and at intervals of 10 ft (3 m) or less.

A.2.0 GATES

Personnel gates should be of similar construction guidelines as fences, or stronger, while vehicle gates will need additional strength due to the weight of the gate assembly, and to prevent vehicle incursion, if dictated by the DBT. Where the DBT justifies additional layered security, hardened (or crash-resistant) gates are available.

A.2.1 Chain-Link Gates. For detail specifications on chain-link gates, refer to *Military Handbook MIL-HDBK-1013/1A, Design Guidelines for Physical Security of Facilities*, Table 6—Common Chain Link Fence Materials (NFESC 1993a), and *Federal Specification RR-F-191/2D, Fencing, Wire and Post, Metal (Chain-Link Fence Gates)* (NCBC 1990a).

Entry gates using perimeter fence double-swing gates should have maximum 2.5-in. (64-mm) clearance between the bottom rail and the finished grade.

Entry gates should have a reinforced steel latch with hardened steel padlock protection.

Posts for swing gates with fabric height up to 8 ft (2.4 m) should have nominal minimum dimensions of 2.875-in. (73-mm) outside diameter (OD) to 8.625-in. (219-mm) OD, depending upon the gate leaf width.

Posts for swing gates with fabric height of 9 to 10 ft (2.7 to 3 m) should have nominal minimum dimensions of 3.5-in. (89-mm) OD to 8.625-in. (219-mm) OD, depending upon the gate leaf width.

A.2.2 Electronic Gate Opening. Electronic gate operators should be Underwriters Laboratory (UL)-listed, heavy-duty, high-frequency electronic models designed to open and close sliding or other types of gates as selected for specific applications. Gates should have maximum 2.5-in. (64-mm) clearance between the bottom tension bar and finished grade.

Electric motors should be sized appropriately for the gate size, duty rating, and frequency of operation. Provide industrial-

quality motor overload protection with manual reset. Gate operators and other electrical appurtenances should be positioned within the fenced perimeter to avoid vandalism and tampering.

Recommended gate travel speed is a minimum 1 ft (0.3 m) per sec. A speed-adjusting feature that provides a range of appropriate speeds for slide gate operation is recommended.

Provide positive limit switches that sense the position of the gate and provide control to prevent damage to the gate operator.

Provide a manual operation feature or disconnect for operation during power failure, malfunction, or emergency. The manual gate operator should be secured inside a locked weather-resistant cabinet, with an attached key box as required. Gate operators should be located so they cannot be reached or tampered with from outside the fence. A variety of types of manual and automatic gate operators, from simple push-button-type operators to complex electronic operating systems, as well as associated hardware and safety devices, are available from gate manufacturers. Gate storage, housing for operators, and site-specific operating systems, warning devices, or signage should also be considered to ensure safe operation when authorized.

Component parts of the gate operator, including attachments, should be constructed with materials or plated, coated, or finished as necessary to provide reliable service in an all-weather environment.

A.2.3 Electronic Gate Control System. A push-button or card-reading sensor in a weatherproof enclosure should be mounted on a steel tube post or concrete bollard anchored to a concrete foundation outside the gate as required.

Consider providing loop, beam, or other vehicle detectors a minimum of 4 ft (1.2 m) away from each side of the gate for safety.

A communication interface should enable remote monitoring of the gate position from a central location, such as a central security office. The suggested operation sequence is:

1. *Entry:* The gate opens when activated by a valid card presented to a card-reading sensor. The gate closes after a sensing loop/sensing beam has determined that the vehicle has passed through the gate.
2. *Exit:* The gate opens when activated by a detector loop in the pavement or a push button inside the gate. The gate closes as for entry.

Other options for automated gate access control systems include radio-controlled, remote-operated (from a control room or operations center), guard-operated, key-switched, and others. Each type will have specific features to consider with respect to the overall access control system.

A.3.0 SITE AREAS

A.3.1 Clear Zones. The purpose of a clear zone is for intrusion detection surveillance and assessment using visual observation or cameras, and to provide an unobstructed area in which placed devices can be readily observed or detected. Clear zone regions are typically established:

- On both sides of a perimeter security fence to allow unobstructed surveillance of the fence area
- Between a perimeter fence and structures, buildings, or other critical assets enclosed within the fence to maintain a clear area for detection of intruders or placed devices
- Around the perimeter of a building to prevent areas of concealment of intruders or placed devices.

For additional information regarding clear zones, see *Minimum Antiterrorism Standards for Buildings, Unified Facilities Criteria (UFC) 4-010-01* (DoD 2002).

Effective clear zone distances should be in accordance with the DBT, but a suggested minimum distance is 20 ft (6 m) or more between the outer perimeter fence and interior structures per *UFC 4-010-01* (DoD 2002).

Within the clear zone, prune or trim vegetation to a height of 4 in. (100 mm) or less, and remove large obstacles or rocks that can shield intruders from view. Avoid locating equipment within clear zones or in spaces below which devices can be readily concealed.

A.3.2 Site Utilities. Wherever possible, incoming site utilities need to be protected from accidental or deliberate damage that might affect operations. It is recommended that the core site utility connections entering the site and facility be hardened. Hardening techniques may include burying, protecting within conduit, security cages, or grilles, or by adding redundant service feeds. The following utilities should be examined and protected to the extent possible:

- Electrical power
- Natural gas
- Incoming water
- Wastewater
- Fire water main(s)
- Communications (phone, data, etc.)

Exposed pipelines should be protected, where possible, using fence barriers to limit access. Alternatively, exposed pipelines could be run within carrier pipes to enable double-wall protection.

Redundant utility connection sources should be provided if available. Dual electrical systems that feed off separate circuits, or incoming water supplies from different source mains, should be utilized where available.

Electrical lines should be placed underground where applicable.

A.4.0 FACILITY ENTRANCES

A.4.1 Sallyport Entrances. A sallyport is a combination of electrically operated gates or portals that are interlocked to prevent more than one gate from opening at a time. The sallyport provides a means for secured, controlled entry through the fence perimeter of the facility. Entry processing, paperwork review, and driver/load identification or verification occur within the sallyport. Sallyports may also be used to enable searching the interior and undercarriage of vehicles for explosives.

Typical vehicle sallyport dimensions are in the range of 75 ft (23 m) long by 20 ft (6 m) wide, and should be sized to accommodate the largest delivery vehicle. The sallyport should be enclosed by fenced sides of height, construction, and configuration consistent with the site perimeter fencing. Vehicle gates should be consistent with the gate guidelines provided in Section A.2.0, Gates, of this Appendix.

Sallyport gates should be equipped with an interlocking system to ensure that the inner and outer gates are not capable of being opened at the same time. However, a keyed manual override switch should be provided that allows the gates to be opened simultaneously. This override switch must be protected and covered such that the possibility of accidental operation is eliminated.

Gate controls should be located in an area such that the person operating the controls maintains a constant visual observation of

the sallyport area. The controls should be protected and covered so that unauthorized use is eliminated.

A.4.2 Building Entrances. Building entrances should provide a space for screening visitors. The area should provide enough space for visitors to wait, queue, and be logged-in prior to entering the interior secure spaces. If frequent visitor entry is anticipated, vandal-resistant furniture may be provided within the visitor waiting area.

Visitor management software can facilitate the log-in and registration of incoming visitors. Some systems permit preregistration prior to entry and notification upon visitor arrival.

If the DBT warrants, x-ray screening of incoming personnel and visitors may be considered. Additionally, explosive screening may be considered for incoming mail and packages.

A.5.0 BOLLARDS AND OTHER VEHICLE BARRIERS

Bollards, jersey barriers, decorative planters, or other vehicle barriers, where applied, should be capable of stopping a 4,000-lb (1,800-kg) vehicle traveling at 30 mph (48 km/h) within 3 ft (0.9 m) or less.

Refer to Department of Defense Handbook *MIL-HDBK-1013/14, Selection and Application of Vehicle Barriers* (NFESC 1999) for detailed descriptions, attributes, and stopping capabilities of several barrier types. This document has been approved for public release and is available online.

A.6.0 EXTERIOR SURFACES

At surfaces subject to vandalism, incorporate glazed concrete masonry units, glazed ceramic tiles, or fiberglass coatings to resist vandalism attempts.

Apply nonstick, unmarkable, polyurethane-based paints and coatings for external surfaces subject to vandalism.

A.7.0 OUTDOOR SECURITY LIGHTING

Depending on the DBT and the local site environment, the amount of recommended illumination may vary. Consult with local code officials for additional restrictions that may apply to lighting levels.

In addition to the suggested illumination levels provided below, refer to the Illumination Engineering Society of North America (IESNA) handbook, *Guideline on Security Lighting for People, Property, and Public Spaces (G-1-03)* (IESNA 2003).

General perimeter roadways and parking areas should be illuminated to 1 to 2 horizontal foot-candles (fch) [11 to 22 lumens/square meter (lux)] on average.

Vehicle gate areas should be illuminated to 3 to 5 fch (32 to 54 lux), average, measured horizontally. If this area will receive CCTV camera coverage, a recommendation is that the illumination levels be 5 to 10 vertical foot-candles (fcv) (54 to 108 lux), measured vertically at the subject height.

- Horizontal illumination measures the lighting at a horizontal surface or plane, such as the ground surface.
- Vertical illumination measures the illumination received on a vertical plane, such as a person's face or the license plate of a vehicle.

If a gatehouse or sallyport entrance is used, an illumination level of 10 to 30 fcv (110 to 320 lux) is the goal.

Building exterior door areas should be illuminated to 3 to 5 fch (32 to 54 lux), on average, for a radius of 15 ft (4.5 m) beyond the exterior door.

General outdoor areas should be illuminated to 0.5 fch (5 lux), average.

Provide a minimum light-to-dark illumination ratio of maximum 6:1, preferably 4:1. Preferably, a lighting engineering study should be performed using point-by-point lighting calculations with a point spacing not more than 25 ft (7.6 m) on center.

Where applicable, incorporate motion-activated lighting to provide instant-on lighting upon motion alarm activation. Such a system will raise the illumination from 0.5 fch (5 lux) to 2 to 3 fch (22 to 32 lux). If motion-activated lighting is included, make sure that the lamp re-strike time is quick enough to support instant-on activation.

When CCTV cameras are used, these additional lighting considerations should be taken (ASIS 2004, *Protection of Assets*, Chapter 19—Security and Protective Lighting):

- *Color Rendering Index:* Choose an appropriate lamp that has accurate color reproduction.
- *Reflectance of Materials:* Consider the material that will be illuminated, and its ability to reflect and transmit light.
- *Direction of Reflected Lighting:* Identify whether reflected lighting will assist or interfere with camera operation.

A.8.0 SIGNAGE

A.8.1 Fence Signage. Post “No Trespassing” signs at 50-ft (15-m) intervals in multiple languages as is consistent with the local population. From a general legal standpoint, the fence and signage establishes a boundary that intruders must cross for violation.

Include appropriate federal, state, and local laws prohibiting trespassing. For example, U.S. Code Title 42, Section 300i-1, titled, “Tampering with Public Water Systems,” states the following (U.S. Code 2009):

1. *Tampering:* Any person who tampers with a public water system shall be imprisoned for not more than 20 years, or fined in accordance with Title 18 “Crimes and Criminal Procedure,” or both.
2. *Attempt or Threat:* Any person who attempts to tamper, or makes a threat to tamper, with a public drinking water system be imprisoned for not more than 10 years, or fined in accordance with Title 18, or both.
3. *Civil Penalty:* The Administrator may bring a civil action in the appropriate United States district court (as determined under the provisions of Title 28 “Judiciary and Judicial Procedure”) against any person who tampers, attempts to tamper, or makes a threat to tamper with a public water system. The court may impose on such person a civil penalty of not more than \$1,000,000 for such tampering or not more than \$100,000 for such attempt or threat.
4. *“Tamper” Defined:* For purposes of this section, the term “tamper” means:
 - a. To introduce a contaminant into a public water system with the intention of harming persons; or
 - b. To otherwise interfere with the operation of a public water system with the intention of harming persons.

A.8.2 Primary Site Entrance Signage. At the primary entrance to the site, post the address of the site so that first responder crews (such as police and fire departments) can confirm the address location.

A.8.3 Water Intake Delineation. At lake or river intakes, provide buoys or float lines with appropriate signage to delineate no-entry zones.

A.9.0 ELECTRONIC SECURITY SYSTEMS

A.9.1 Intrusion Detection Sensors: General. The intrusion detection system should be capable of detecting an individual [weighing 75 lb (34 kg) or more] crossing the detection zone walking, crawling, jumping, running, or rolling [at speeds between 0.5 and 15 ft (0.2 and 4.6 m) per sec], or climbing the fence, if applicable.

Perimeter intrusion detection systems should provide average false alarm rates of not more than one false alarm per week, per sensor, while maintaining proper detection sensitivity.

Interior intrusion detection should provide false alarm rates of not more than one false alarm every three months, per sensor system.

Detection probability should be at a 95% confidence level. When calculating the detection probability for multiple sensor systems, detection is assumed if any of the sensors detects the intrusion.

Intrusion detection systems should cover the entire length of the perimeter of a detection area, including gates.

Intrusion detection sensors should be provided with a redundant power source for a period of not less than 4 h.

Detection sensors should be monitored for alarm and fault conditions by an attendant security monitoring system (an electronic system that monitors security alarms).

A.9.2 Exterior Intrusion Detection. Prevalent sensor technologies include active infrared, microwave, dual-technology, buried-line, fence-mounted sensors, and video motion detection.

Appropriate detection technology should be selected based on factors such as facility environment, location, climate, and ambient temperature conditions, and on the DBT.

A.9.2.1 Active Infrared Sensors. Active infrared sensors transmit infrared signals to a receiver. Interruption of the signal indicates that an intruder or object has blocked the path.

Active infrared sensors require a line of sight; the signal must be projected over a clear path where the line of sight remains unblocked.

Transmitters and receivers should be installed where they will not be misaligned due to Earth tremors, objects hitting the unit (such as falling rocks, branches, or falling trees), or freezing and thawing of the ground.

Active infrared sensors do not work well in areas with heavy snowfall because drifts or snow mounds cover sensors and block transmission and reception paths. Weather conditions such as fog, heavy rain, or severe sand or dust will affect the reliable detecting range.

Nuisance alarm sources for active infrared sensors include animals and wind-blown debris. Fencing can minimize animal false alarms. Vegetation can also pose a problem if it is allowed to grow to a size where its movement will generate an alarm.

A.9.2.2 Microwave Sensors. Microwave sensors transmit or flood a designated area with an electronic field. A movement in the area disturbs the field and sets off an alarm.

The detection area should be free of bushes and obstructions. Close proximity to other high-frequency signals can adversely affect the detection reliability of microwave sensors. Areas that contain strong emitters of electric fields (such as radio transmitters) or magnetic fields (such as large electric motors

or generators) can affect the ability of the microwave sensors to function properly and should be avoided.

Grass should be cut to less than 3 in. (76 mm). A gravel surface prepared for water drainage is better than a grass surface. Avoid dead spots or areas of no detection created by metal objects such as Dumpsters, shipping crates, trash cans, and electrical boxes. These dead spots create areas for intrusion attempts.

Nuisance alarm sources for microwave sensors include wind creating wave action on puddles or moving nearby fences or vegetation, or movement adjacent to, but outside of, the protected area because the signal can easily pass through standard walls, fences, glass, sheet rock, and wood.

A.9.2.3 Dual-Technology Sensors. Dual-technology sensors use both microwave and passive infrared (PIR) sensor circuitry within the same housing. PIR sensors pick up heat signatures from intruders by comparing infrared receptions to typical background infrared levels. Typically, activation differentials are 3 °F (1.7 °C).

Dual-technology sensors generate an alarm condition if either the microwave or PIR sensor detects an intruder.

Dual-technology sensors can be installed along a perimeter line, a fence, or a buffer zone, or as a defense against intruders approaching a door or wall.

Nuisance alarms for microwave sensors are described in Section A.9.2.2. Nuisance alarms for PIR sensors include reflected light and radiated heat.

In some dual-technology sensors, alarm settings may be adjusted to require that both the microwave and the PIR unit detect an intruder before an alarm condition is generated. With two independent means of detection, false alarms are reduced.

A.9.2.4 Buried Line Sensors. There are several types of buried line sensors, including fiber-optic cable, ported cable, and ported co-axial cable.

The two principal advantages of buried cable are that it is covert and it follows the terrain.

Buried line systems do not work well with shrubbery or trees that require landscaping and maintenance.

It is important that the cable be buried to a uniform depth. Changes in soil conductivity can affect the sensor readings.

Nuisance alarms can be caused by the ground shifting due to standing or puddling water, or erosion. Tree roots can also cause nuisance alarms when windy conditions aboveground cause movement in the roots. Large animals passing over the detection zone can also generate alarms.

A.9.2.5 Fence-Mounted Sensors. Fence-mounted sensors detect vibrations on fence fabric associated with sawing, cutting, climbing, or lifting the fence fabric.

Fence-mounted sensors are not reliable in areas where high vibrations are likely to be encountered, such as in close proximity to roadway activity or construction. Do not use in areas with high wind or numerous animal interactions with the fence line.

Fence-mounted sensors perform best when mounted directly to the fence fabric. Each sensor is connected in series along the fence with a common cable to form a single zone of protection.

Sensor zone lengths have a typical recommended range of 300 ft (90 m), although some systems permit longer sensing zones.

Install these sensors on high-quality fencing. Poor-quality fences with loose fabric can create too much background activity due to flexing, sagging, or swaying.

Nuisance alarms can be generated from shrubbery and tree branches as well as animals and severe weather that contacts the fence, causing it to vibrate.

A.9.3 Interior Intrusion Detection. Provide appropriate interior intrusion detection according to the DBT and the building environment.

Applicable technologies include dual-technology (passive infrared and microwave), linear beam, and glass-break sensors.

Select products that are consistent with the ambient temperature, environment, and moisture content of the structure to be protected.

A.9.3.1 Dual-Technology Motion Sensors. Dual-technology motion sensors use passive infrared and microwave technology to detect motion. Described in Section A.9.2.3, these sensors are applicable for both interior and exterior applications.

Do not use dual-technology sensors in areas where the PIR sensor can be exposed to sudden changes in temperature, such as near an exterior door.

Nuisance alarms can be generated from heat-radiating objects such as heat system registers or other warm objects (including things as innocuous as a mop bucket with hot water in it).

A.9.3.2 Linear Beam Sensors. Linear beam sensors transmit a beam of infrared light to a remote receiver, creating an “electronic fence.” Once the beam is broken, an alarm signal is generated. It has a high probability of detection and a low false alarm rate.

This type of sensor is often used to cover openings such as doorways or hallways, acting essentially as a trip wire. The infrared beam is unaffected by changes in thermal radiation, fluorescent lights, electronic frequency interference (EFI), or radio frequency interference (RFI).

The transmitter and receiver can be up to 1,000 ft (300 m) apart.

Nuisance alarms can be created by any objects that may break the beam, such as paper blowing off of a shelf or desk.

A.9.3.3 Glass-Break Sensors. There are three basic types of glass-break sensors: acoustic sensors (listen for an acoustic sound wave that matches the frequency of broken glass), shock sensors (feel the shock wave when glass is broken), and dual-technology sensors (sense acoustic and shock vibrations).

Using dual-technology sensors significantly reduces false alarms from background noise such as RFI and frequency noise created by office machines.

Glass-break sensors provide intrusion detection for windows and doors with glass panes. They are mounted on a window, window frame, wall, or ceiling. If mounted on a wall or ceiling (this is the preferred placement), place it opposite the window. If mounted on glass, place it in the corner, approximately 2 in. (50 mm) from the edge of the frame.

Use mounting adhesive specified to withstand long exposure to summer heat, winter cold, or condensation.

Regardless of the type of sensor, coverage typically does not exceed 100 ft² (9 m²) of glass surface.

Nuisance alarms can be caused by improper calibration or installation. In addition, RFI, sharp impact noises, and background noise such as office, industrial, and cleaning machinery can cause false alarms.

A.9.4 Door and Hatch Contact Alarm Switches. Door and hatch contact alarm switches should interface with a security monitoring system in addition to the SCADA system.

Magnetic door contact switches should be installed at all building exterior doors to monitor for door-ajar and door-forced-open conditions.

Exposed exterior locations, such as exterior hatches or vaults, should utilize high-security balanced magnetic switches.

Industrial doors, gates, and roll-up doors should use high-security, rugged-duty, sealed, wide-gap magnetic switches.

A.9.5 Pipeline Vibration Detection. Emerging technologies are being developed that provide vibration detection within pipeline sections. Incorporating this technology can detect attempts at sabotage such as cutting, hammering, or detonation of the pipeline, and a response can be initiated. Such detection systems might be considered for critical pipeline sections that do not have redundancy. The detection systems monitor vibration within the pipeline section. If the vibration level exceeds a threshold amount, then an alarm could be transmitted back to a central monitoring station. Such systems are relatively new technology but are currently in operation for critical utility (oil, natural gas) pipelines within the United States.

A.10.0 ACCESS CONTROL SYSTEMS

A.10.1 Access Control Systems: General. A means of providing access control should be incorporated into all security systems. Access control measures should consist of one or more of the following systems; key locks and/or padlocks, numeric keypad locks, or card reader systems.

A.10.2 Locks and Padlocks. Padlocks should be weather-resistant with a hardened-steel shackle.

Padlock pulling resistance should be 4,500 lb (20,000 N) at minimum.

Padlock pressure resistance to bolt cutters should be 10,000 lb (44,000 N) at minimum.

Key locks should use hardened steel inserts protecting the plug face, shell, and sidebar from drilling attack.

Provide an access guard of channel steel or other material against bolt-cutter or torch access to padlocks.

Whenever possible, avoid using “daisy chains” of padlocks. Instead, use a programmable lock that allows for authorized entry by multiple individuals using unique codes.

A.10.3 Numeric Keypad Locks. Numeric keypad locks are locking systems that include a programmable keypad in addition to the door latch or deadbolt and lever handle. A user must enter a code at a keypad before the door will unlock and allow access. New codes can be added or changed at the keypad.

Models are available that require both a credential and a code. This dual method can provide an additional layer of protection.

Models are available to mount on various door thicknesses and doors with narrow stiles.

A.10.4 Card Reader Systems. Card reader systems should incorporate:

1. *Alarm Display and Programming:* A computer server or workstation that displays alarm conditions and allows programming of the system.
2. *Badge Creation:* A badge station, allowing creation and programming of badges.
3. *Local Control:* Local control panels that control the doors, card reader units, and access cards.
4. *Printer Unit:* A printer unit that can print a report for each event and alarm condition.

Under normal operation, the system should grant access at doors with card readers by comparing the time and location of any attempted entry with information stored in local (at the door controller) memory.

Access is granted only when the security card used has a valid entry code at the card reader for the designated time frame.

The access card should be a standard credit-card-size passive component with an integral coding technology, such as coding contained within a chip in the card.

Electrical locking means should be electric strike, magnetic lock, or other approved means. Great care should be taken in designing access control for doors used for egress to ensure that free egress is permitted at all times.

Refer to NFPA 101, *Life Safety Code* (NFPA 2006) and NFPA 101B, *Code for Means for Egress for Buildings and Structures* (NFPA 2002) for code guidance on egress and ingress doors.

A.11.0 CLOSED-CIRCUIT TELEVISION (CCTV) SURVEILLANCE

A.11.1 General Considerations. CCTV cameras can be analog or Internet Protocol (IP)-network cameras, depending on factors such as the suitability to the installation, site conditions, and availability of local area networks.

The ASIS publication *Protection of Assets*, Chapter 38—Television in Security (ASIS 2004), identifies the following specification items to consider when specifying CCTV cameras:

- **Imager:** The size of the image-sensing device within the camera.
- **Resolution:** The measure of detail that the camera can distinguish, usually measured in horizontal TV lines per in. (25 mm). The larger the number, the sharper the image and the better the camera.
- **Sensitivity:** Typically, the minimum lighting illumination level required for full video. The lower the required illumination level, the more sensitive the camera.
- **Signal-to-Noise Ratio:** The ratio of the peak value of the video signal to the peak value of the noise or electromagnetic interference, measured in decibels. The greater the ratio, the sharper and better the picture image.
- **Automatic Light Compensation:** The process whereby the amount of illumination on the image sensor is automatically adjusted to the scene brightness. A high ratio indicates that the camera can automatically adjust to wide variations in scene illumination without noticeable distortion in the transmitted image.
- **Backlight Compensation:** A feature available in many cameras that automatically reduces contrast and silhouetting between near and far objects.
- **Video Output:** A measurement, stated in volts peak-to-peak, between the darkest black to brightest light levels of the signal. A typical value is 1.0 V peak-to-peak.
- **Synchronization:** A means of controlling the image scanning so that the camera image will not roll when switched between video monitors. Better cameras allow for synchronization adjustment to accommodate multiphase power supplies.
- **Environment:** Upper and lower temperature and humidity limits for the cameras. It is important to specify a camera that works in the intended environment, including weather.

- **Dimensions:** The outside measurements of the camera case.
- **Weight:** The weight of the camera within its case.

Because camera technology is improving so rapidly, detailed performance specifications are not provided here; it is recommended that utilities consult with a security engineer for current camera hardware standards and sensitivity ratings.

A.11.2 Field of View. Provide fixed-position or pan/tilt/zoom (PTZ) cameras depending upon the desired field of view and the intended application.

Provide appropriate camera lenses corresponding to the camera application and field of view requirements.

The CCTV surveillance system should be capable of viewing prescribed objects within the field of view as follows, considering a screen height of 480 pixels to be full-screen (100% = 480 pixels).

- For intrusion detection purposes, the object should occupy a minimum of 10% of the screen height or be 48 pixels tall.
- For recognizing a person's face, the body of the person should be a minimum of 50% of the screen height or 240 pixels tall.
- To identify a license plate, the plate height should be a minimum of 5% of the screen height or 24 pixels tall.

In some cases, the field of view of a camera may include public areas or private residential areas that should not be monitored by video surveillance. In these cases, to minimize liability issues, a current capability of modern CCTV systems allows masking of these areas or views so that they cannot be seen by the attendant staff.

A.11.3 CCTV Housings and Mounts. CCTV housings should be adequate for the intended application and site location.

Incorporate heater/blower units, wipers, or other elements as necessary to accommodate site environmental conditions.

Incorporate pole-mount, building-mount, or other mounting means so that the camera obtains a clear field of view of the intended target.

Specify and locate the housing and camera mount such that tampering or vandalism of the camera units is prevented.

A.11.4 Video Network Servers. The video network server should be a high-performance IP network-compatible video system.

The network server should be capable of streaming images at a frame rate of 30 frames per sec.

The video communication system should be capable of transmitting live video across communication networks and enable video cameras to be remotely monitored and controlled over the network, provided password authentication requirements are met.

The desired camera view should be selectable by designated camera name and IP address.

A.11.5 Digital Video Recorders. As a minimum, it is recommended to provide adequate digital recording capacity for all cameras for 30 days of continuous storage at 5 frames per sec.

Provide a means for archiving video to digital video disc (DVD) or other long-term storage format.

Specify the physical location of the recorder unit based on environmental considerations, location, network, and bandwidth availability.

Identify appropriate video compression technology to conserve network bandwidth and storage needs.

A.11.6 CCTV Computer Application Software. CCTV application software should be full management software to monitor and manage single or multiple sites.

The software should allow monitoring and recording of images from multiple simultaneous cameras at frame rates up to 30 frames per sec.

The system should enable customized layouts for intuitive and interactive ways of representing the camera network.

The software should provide flexible live and recording settings per individual camera input.

The software should allow connectivity to other systems, via application programming interface (API) alarm and pre-alarm recordings, and enable support for external joysticks to perform pan and tilt operations.

A.12.0 SECURITY, CONTROLS, AND SCADA WIRING

All security, controls, and SCADA wiring should be protected within conduit.

All interconnecting wiring between security components should be monitored for integrity so that an abnormal condition (e.g., wire-to-wire short, wire break, or wire ground-fault condition) is automatically indicated to the user upon arming the system.

The security wiring configuration at the end device should be a four-state configuration using an end-of-line (EOL) resistor network where neither the alarm nor the normal condition are 0 ohms or open-circuit.

Conceal security conduits, telephone lines, and other critical utility connections from view and access, or locate them in the interior of buildings.

Provide a backup power source (4-h minimum) to security components and SCADA and other crucial control systems. Backup power sources may include battery units, auxiliary power supplies, uninterruptible power supplies (UPSs), or generators.

Refer to NFPA 70, *National Electrical Code* (NFPA 2005), for code guidance on electrical wiring requirements.

A.12.1 SCADA and Electrical Control Panel Enclosures. Provide a tamper switch at all security and SCADA control panel enclosures. Upon enclosure door opening, an alarm condition should be logged by the system.

Though panels should be locked, the electrical disconnect should never be locked.

A.13.0 BUILDING ELEMENTS

A.13.1 General. When new buildings are being designed, discuss with the building architect and structural engineers the opportunity to incorporate design elements that prevent progressive collapse of the facility in the event of explosion within or adjacent to the building. Progressive collapse is defined by ASCE and the Structural Engineering Institute (SEI) in *Minimum Design Loads for Buildings and Other Structures* (ASCE/SEI 2010) as “The spread of an initial local failure from element to element eventually resulting in the collapse of an entire structure or a disproportionate large part of it.”

A.13.2 Doors. Exterior doors should be heavy-duty, steel-metal doors conforming to ASTM F476-84(2002) Grade 40 high-security-level door (ASTM 2002), prepped for security door hardware. Doors should comply with ANSI/NAAMM/HMMA 862-03 *Guide Specifications for Commercial Security Hollow Metal Doors and Frames* (ANSI/NAAMM/HMMA 2003).

Doors should have a maximum window opening of 96 in.² (62,000 mm²) or nominal 4-in. by 16-in. (100-mm by 400-mm) size with a minimum side panel size.

The door frame should be heavy-duty with concrete fill.

Hinge pins should be on the secure side or be nonremovable or tamper-resistant to eliminate door compromise by removing hinge pins.

Consider electronic door status monitoring for door-forced and door-ajar conditions.

The following door recommendations are provided for example purposes from the U.S. General Services Administration publication *Facilities Standards for the Public Buildings Service*, Section 3.5—Building Elements (GSA 2005).

- Glazed exterior doors and frames should be steel and meet the requirements of SDI Grade III with a G-90 galvanic zinc coating.
- Hinges, hinge pins, and hasps must be secured against unauthorized removal by using spot welds or peened mounting bolts.
- All exterior doors must have automatic closers.
- The exterior side of the door should have a lock guard or astragal to prevent jimmying of the latch hardware.
- Doors used for egress only should not have any operable exterior hardware.

A.13.3 Security Grilles. Base-level security grilles (for windows, louver openings, roof hatches, culverts, etc.) should be woven No. 10 wire gauge steel, 1.5-in. (38-mm) diamond mesh, or welded No. 10 wire gauge, 2-in. (50-mm) square welded mesh screens.

The grilles should be hot-galvanized with a hot-powdered-coat finish.

Use tamper-resistant and tamper-proof fasteners for mounting window grilles.

For enhanced-level threat protection, refer to *Military Handbook MIL-HDBK-1013/10, Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities* (NFESC 1993b) for security grilles.

A.13.4 Security Cages. Caged partitions (for critical equipment, pumps, motor control centers, and so on) should be No. 10 wire gauge steel with 2-in. (50-mm) welded openings in 1.25-in. by 1.25-in. by 0.125-in. (32-mm by 32-mm by 3-mm) angle iron framework.

Ensure that the partitions include framework supports, access gates, locks, and other accessories.

A.14.0 HATCHES/VAULTS AND VENTS

A.14.1 Hatch, Vault, and Vent Alarms: General. Hatch, vault, and vent alarms should use similar alarm contact hardware, such as magnetic door contact switches, depending on the final hatch or vault design.

Interconnect the alarm contacts to a security monitoring system.

Note that curb and sidewalk devices may become a tripping or safety hazard. Consider the location and application carefully when designing the system.

Provide locking covers for valve operators.

A.14.2 Roof or Sidewalk Hatches. Provide a lock on a manufacturer's metal door system that is set into concrete curb with a gutter and drain.

Consider an additional protected keyed bar lock across a door that is mounted directly to a structural curb, especially for large, publicly accessible pumping stations.

Consider an elevated upper structure cover surrounding a sidewalk door, especially for large, publicly accessible pumping stations. This cover is to prevent drilling through the doorplate and adding liquids to the contents, as well as to delay access to the sidewalk door hatch. This additional layer delays someone attempting to gain access to water to introduce a contaminant.

Alarm the upper structure using exterior-rated, balanced magnetic door contacts.

A.14.3 Roof Vents. Provide metal roof vents with numerous small openings rather than vents with fewer, larger openings [96 in.² (62,000 mm²) is considered a person-passable opening]. Contaminants can be introduced through much smaller vents; prevent direct passage of contaminants through a vent by using traps.

Position or barricade vent openings to prevent spray of a contaminant liquid into a vent opening.

Provide a metal structure cover surrounding the vent to delay access to the vent structure, with adequate standoff [nominally 8 in. (200 mm) or more] from the vent to limit drilling attempts into the vent assembly.

Provide protected dual locks on a metal vent cover system set on a concrete curb.

Alarm the protective cover using exterior-rated magnetic door contacts.

A.14.4 Vault Hatch with Elevated Curb. Provide a lock on a manufacturer's door system. Alarm the vault hatch using exterior-rated magnetic door contacts.

Consider an additional protected key bar lock across a door that is mounted directly to a structural curb.

A.14.5 Vault Door Hatch Set Flush with Top of a Structural Slab. Provide a lock on a manufacturer's door system. Alarm the vault hatch using exterior-rated magnetic door contacts.

Consider an interior keyed bar lock system or secondary horizontal structure immediately below the vault sidewalk door hatch to block access.

A.15.0 ONLINE WATER QUALITY MONITORING

A suite of online instruments to monitor certain surrogate water quality parameters should be installed. Among the parameters to monitor in water distribution systems are pH, chlorine residue (either total or free, depending on the type of residue maintained in the system), specific conductance, turbidity, and total organic carbon.

Among the parameters that could be considered for monitoring wastewater collection systems are pH and volatile organic carbon.

Periodic readings from the online instruments should be compared with baseline water quality values to determine whether there is potential contamination.

The placement of the sampling location for the instruments depends on the type of asset. For example, in water storage tanks the sampling location should be from the outlet pipe near the tank, ideally between the tank and the isolation valve. If there is a common inlet outlet pipe, the sampling location should be installed on the common pipe near the tank, ideally between the tank and the isolation valve.

A.16.0 OPERATOR DEVICES

A.16.1 Man-Down Transmitter. A man-down transmitter is worn by personnel for automatic man-down signaling. The unit

should be portable, lightweight, and supplied with a belt clip or holster for mounting.

Built-in tilt switches should automatically activate the man-down transmitter when the user is knocked down.

A pull cord should activate the alarm or emergency signal when an attempt is made to remove the unit from a belt.

The transmission mode should integrate both radio frequency (RF) and infrared (IR) signaling for redundant communications.

Power should be provided by a long-life lithium battery.

A.17.0 CHEMICAL FILL-LINE LOCKING DEVICES

Connections for filling chemical tanks should be locked to restrict access to authorized personnel only. Chemical fill lines usually are fitted with quick-connect, cam-arm actuated couplings for ease of use by the chemical vendor. Locking devices for the contractor's temporary connections are recommended.

Lockable dust caps or dust plugs with hardened key locks should be installed on the individual couplings.

Where multiple fill lines are co-located, a hardened box or port integrated into the building masonry, complete with a shrouded and hardened lock, can be used in lieu of individual coupling locks.

A.18.0 HYDRANTS

Provide tamper seals on hydrants. Tamper seals reduce the possibility of tampering or unauthorized operation of the hydrant.

Provide a one-way check valve minimizing the possibility of accidental or intentional contamination of drinking water via the hydrant. The device should not hinder or slow response time to firefighters or reduce flow below the flows referred to by standards ANSI/AWWA C502-05 and ANSI/AWWA C503-05 (ANSI/AWWA 2005). The check valve must be capable of being tested without being removed from the hydrant to ensure a leak-proof seal.

Provide locking mechanisms on hydrants. Hydrant locking systems should be designed so that the hydrants can be operated using a special keyed wrench without the need to remove the lock.

- If locking mechanisms are used on hydrants, it is important that training on unlocking the mechanisms be provided to all local firefighting personnel and any other fire departments with which there are mutual aid agreements in place, who would respond in an emergency.
- Provide the specialized wrenches in sufficient quantity to the fire department and other authorized persons so they can operate the hydrants as needed. These wrenches are typically only sold to fire authorities and water utilities.

A.19.0 MANHOLES

Securing manholes can be accomplished in three ways: tack welding, bolt locks, and pan locks.

1. *Tack Welding:* Provides a fast method of securing manholes. It is economical and effective for manholes not frequently accessed. The disadvantage is that the tack weld must be removed or broken before utility staff can access the manhole.

2. *Bolt Locks:* Anchor the manhole to the manhole frame. They have a specialized bolt head that requires a specialized tool to unbolt or unlock the manhole. To remove or access the manhole, the bolt locks must be removed. This system of locking manholes is more flexible than the tack welding method, but more expensive to install. There are some challenges with noise and rattling on locking manhole covers.
3. *Pan Locks:* Prevent entry into the manhole, as well as eliminating dumping into the collection system. The pan unit is installed into the manhole, with the edge of the pan resting within the manhole opening. The manhole is then locked into place in the pan unit. This system of locking manholes is more flexible than the tack welding and bolt locking methods, but more expensive to install.

GLOSSARY AND ABBREVIATIONS

Access Control: The physical guidance of vehicles and/or people going to and coming from a space through judicious placement of entrances, exits, landscaping, lighting, and controlling devices (such as guard stations, turnstiles, etc.)

ACI: American Concrete Institute.

Agent: Any physical, chemical, or biological entity that can be harmful to an organism.

AISI: American Iron and Steel Institute.

AMSA: Association of Metropolitan Sewerage Agencies [now National Association of Clean Water Agencies (NACWA)].

ANSI: American National Standards Institute.

API: Application programming interface.

ASCE: American Society of Civil Engineers.

ASDWA: Association of State Drinking Water Administrators.

Asset: Anything of value (such as people, information, hardware, software, facilities, equipment, reputation, activities, or operations) that may be a target of the design basis threat (DBT) adversary. Assets are what an organization needs to get the job done—to carry out the mission. The more critical the asset is to an organization accomplishing its mission, the greater the effect of its damage or destruction.

ASTM: ASTM International (formerly the American Society for Testing and Materials).

AWWA: American Water Works Association.

AwwaRF: The former American Water Works Association Research Foundation, now called the **Water Research Foundation**.

Base: Minimum recommended.

Bollard: One of a series of posts preventing vehicles from entering an area.

CCTV: Closed-circuit television.

Check Valve: A valve that allows fluid to flow through it in one direction but prevents flow in the opposite direction.

Clear Zone: An area surrounding the perimeter of a facility that is free of shrubs and trees, and features well-maintained landscaping that does not provide hiding places for an adversary.

CMU: Concrete masonry unit.

Contaminant: Any physical, chemical, biological, or radiological substance or matter that has an adverse effect on air, water, or soil.

Contamination: Introduction of microorganisms, chemicals, toxic substances, wastes, or wastewater into water, air, and soil in a concentration that makes the medium unfit for its intended use.

Countermeasure: A reaction to or a defense against a hostile action to deal with a threatening situation.

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 for the adversary to obtain the asset. See also Table 1-1.

Cross Connection: Any temporary or permanent connection between a public water system for consumer's potable (i.e., drinking) water system and any source or system containing or which may contain nonpotable water or other substances.

Daisy Chain: Groups of padlocks connected and hooked to a common chain in such a way as to allow access through a key that can unlock any one of the padlocks.

Delay Features: Security objects such as physical barriers designed to occupy or limit an adversary until a response force can interrupt accomplishment of the adversary's objectives. Delay features consist primarily of physical hardening features and are often employed in multiple layers to provide protection in depth. Delay features are only effective when placed within a layer of detection.

Design Basis Threat (DBT): The adversary against which a utility must be protected. Determining the DBT requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence.

Detection: The point at which a potential attack is discovered, assessed, and determined to be an attack in progress rather than a false alarm.

Detection Features: Security items such as sensors that are intended to detect the presence of an intruder. A complete detection system generally includes 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 also include lighting systems, motion detectors, monitoring cameras, access control equipment, or other devices.

Deterrence: Security measures such as lighting or the presence of closed-circuit television or people in the area that may discourage an adversary from attacking the 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.

DoD: U.S. Department of Defense.

DVD: Digital versatile disc, digital video disc.

EFI: Electronic frequency interference.

Enhanced: Augmented with improved, advanced, or sophisticated features.

EOC: Emergency operation center.

EOL: End-of-line.

EWRI: Environmental and Water Resources Institute of the ASCE.

Foot-Candle: A unit of light intensity defined as the amount of light measured on a surface one foot from a uniform point source of light equal to the light of one candle. A foot-candle is equal to one lumen per square foot.

FRP: Fiberglass-reinforced plastic.

GSA: U.S. General Services Administration.

Harden: To improve the physical strength of a protective measure.

IESNA: Illuminated Engineering Society of North America.

Improvised Explosive Device (IED): An apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, harass, or distract through high-speed projectiles and overpressure.

Improvised Incendiary Device (IID): An apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, harass, or distract by creating intense heat and fire.

Insider: An individual who is granted normal access to a facility. This may be an employee, a contractor, a custodial worker, or an authorized visitor. See also Table 1-1.

Intrusion: Entrance by force or without permission or authorization, either physically or via electronic methods.

IP: Internet Protocol.

IR: Infrared.

Key Card Reader/Access: Entry to a facility via a device used by an individual(s).

lb: Pound.

Lumen: The SI unit of measuring the power of light being produced by a light source or received by a surface.

Lux: The SI unit of light intensity defined as the amount of light equal to one lumen per square meter.

m: Meter.

mm: Millimeter.

Mantrap: Secured entry system that prevents an individual from gaining access to an area by holding them first in an assessment area.

NACWA: National Association of Clean Water Agencies [formerly Association of Metropolitan Sewerage Agencies (AMSA)].

NDWAC: National Drinking Water Advisory Council.

NETCSC: National Environmental Training Center for Small Communities.

NFPA: National Fire Protection Association.

NRWA: National Rural Water Association.

OD: Outside diameter.

PIR: Passive infrared.

PL: Public law.

PLC: Programmable logic controller.

Protection in Depth: The strategy of providing multiple layers of protective measures, thereby requiring an adversary to defeat a system, travel to the next protective layer and defeat that system, and so forth until reaching the target. An example of protection in depth is the application of layers of protective measures at the site boundary (perimeter fencing system), at the building envelope (exterior walls, doors, windows, grilles, and roof system), and at the target enclosure (the room in which the targeted asset is housed).

psi: Pounds per square inch.

PTZ: Pan, tilt, and zoom.

PVC: Polyvinyl chloride.

RAM-W: Risk Assessment Methodology for Water Utilities, available from the Sandia Corporation (Sandia National Laboratories).

Response: Actions taken to interrupt the adversary's task. Utility staff, the utility's security response force, or law enforcement may carry out response, depending on the threat and policy of the utility.

RF: Radio frequency.

RFI: Radio frequency interference.

Risk: The potential for realization of unwanted, adverse consequences to human life, health, property, or the environment. The quantitative or qualitative expression of possible loss that considers both the probability that a hazard will cause harm and the consequences of that event. Risk is usually expressed as a function of the probability that an adverse effect will occur and the criticality of the effect on the ability to fulfill a mission or function.

RTU: Remote terminal unit.

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 bent on damage or destruction of the utility's facilities or generating a lack of public confidence in the utility's ability to protect the public. See also Table 1-1.

SCADA: Supervisory Control and Data Acquisition (see full definition below).

SI: International System of Units.

Significant: Having or likely to have a major effect; important; fairly large in amount or quantity.

Supervisory Control and Data Acquisition (SCADA): The system that provides automatic or semi-automatic sensing of key parameters and control of key elements of the water or wastewater system. It generally provides for communications, notifications, and alarms, as well as for manual override of controls.

Surveillance: The placement of physical features, activities, vehicles, and people that maximize visibility by others during their normal activities. Surveillance may be natural or electronic, informal (office windows placed to facilitate surveillance of entry roads), or formal (continuous monitoring). Surveillance provides the link between detection (sensors activated due to the presence of an intruder) and assessment (confirming that the detection is valid and not a nuisance alarm).

SWAT: Special Weapons and Tactics.

Target: This term is used synonymously with asset throughout this document.

Terrorist: A radical who employs terror as a political weapon. With significantly enhanced tool and weapon capabilities, terrorists may be politically or doctrinally motivated to cause maximum human casualties, often without regard for the terrorist's personal survival.

UL: Underwriters Laboratory.

UPS: Uninterruptible power supply.

USEPA: U.S. Environmental Protection Agency.

VA: Vulnerability assessment (see full definition under **Vulnerability Assessment**).

Vandal: An individual acting alone or in a group, unarmed and using spray paint to deface property or using hand tools to inflict damage to utility assets. See also Table 1-1.

Vehicle Sallyport: Interlocking gates within a fenced area where incoming drivers pass through the first gate and stop at the second gate. Once both gates are closed and the vehicle is captured within the sallyport, a security guard may confirm the identity of the driver and, if necessary, search the vehicle to confirm the contents. Once the vehicle and driver are approved, the second gate opens and the vehicle may drive onto the facility.

VSAT: Vulnerability Self-Assessment Tool, available from NACWA.

Vulnerability: A characteristic of a critical infrastructure's design, implementation, or operation that renders the infrastructure susceptible to destruction or incapacitation by a threat. Vulnerabilities may consist of flaws in security procedures, software, internal system controls, or installation of infrastructure that may affect the integrity, confidentiality, accountability, or availability of data or services. Vulnerabilities also include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters. Vulnerability may be considered any weakness that can be exploited by an adversary or, in a nonterrorist threat environment, make an asset susceptible to hazard damage.

Vulnerability Assessment (VA): An assessment of the vulnerabilities of a water or wastewater system. The six common elements of vulnerability assessments identified by USEPA are: (1) characterization of the system, including its mission and objectives; (2) identification and prioritization of adverse consequences to avoid; (3) determination of critical assets that might be subject to malevolent acts that could result in undesired consequences; (4) assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries; (5) evaluation of existing countermeasures; and (6) analysis of current risk and development of a prioritized plan for risk

reduction. Two example approaches to VAs are the Risk Assessment Methodology for Water Utilities (RAM-W) and the Vulnerability Self-Assessment Tool (VSAT).

Water Research Foundation (WRF): Established in January, 2009; the former American Water Works Association Research Foundation (**AwwaRF**).

WEF: Water Environment Federation.

WISE: Water Infrastructure Security Enhancements.

WISE SC: Water Infrastructure Security Enhancements Standards Committee of the EWRI of ASCE.

WSWG: Water Security Working Group.

This page intentionally left blank

REFERENCES

For a comprehensive list of resources related to water and wastewater security, see the USEPA WISE Phase 1 documents developed by the American Society of Civil Engineers, the American Water Works Association, and the Water Environment Foundation (ASCE/AWWA/WEF 2004a, 2004b, 2004c). The initial Draft was developed for USEPA WISE Phase 3 and was titled the *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006).

American National Standards Institute/American Water Works Association (ANSI/AWWA). (2005). *C502-05: Dry-barrel fire hydrants and C503-05 Wet-barrel fire hydrants*, AWWA, Denver, Colo.: These standards establish flow standards for dry- and wet-barrel fire hydrants.

American National Standards Institute/National Association of Architectural Metal Manufacturers/Hollow Metal Manufacturers Association (ANSI/NAAMM/HMMA). (2003). *ANSI/NAAMM/HMMA 862-03: Guide specifications for commercial security hollow metal doors and frames*, NAAMM, Chicago, Ill.: This document provides specifications for commercial security hollow metal doors and frames. Its focus is protection from vandalism, forced entry, theft, and firearms attack.

American Society of Civil Engineers (ASCE). (1992). *Design and construction of urban stormwater management systems*, ASCE Manuals and Reports on Engineering Practice No. 77, ASCE, Reston, Va.: This manual is an update of relevant portions of the ASCE/WPCF Manuals and Reports on Engineering Practice No. 37, *Design and Construction of Sanitary and Storm Sewers*, to include the new developments in the field of stormwater management. The manual describes currently accepted procedures for financial services, regulations, surveys and investigations, design concepts and master planning, hydrology and water quality, storm drainage hydraulics, and computer modeling.

ASCE. (1998). *Design of municipal wastewater treatment plants*, ASCE Manuals and Reports on Engineering Practice No. 76, 4th ed., ASCE, Reston, Va.: The focus of this manual is current practice in the design of municipal wastewater treatment plants. Its intended audience is design professionals knowledgeable in the areas related to wastewater treatment, including plant operations and regulations.

ASCE. (2006). *Standard guidelines for the design, installation, maintenance and operation of urban stormwater systems*, ASCE/EWRI Standards 45-05, 46-05, and 47-05, ASCE, Reston, Va.: This set of guidelines provides for the design of urban stormwater systems, covering topics such as site analysis, system configuration, hydrology, hydraulic design, nonstructural considerations, structural design, and materials (ASCE/EWRI Standard 45-05); guidelines for the installation of urban stormwater systems and discusses subjects such as contract documents, preconstruction site inspection, construction, and inspection (ASCE/EWRI Standard 46-05); and guidelines for the operation and maintenance of urban stormwater systems, including operation and maintenance plans, water quality, periodic inspection, and maintenance (ASCE/EWRI Standard 47-05).

ASCE. (2007). *Gravity sanitary sewer design and construction*, ASCE Manuals and Reports on Engineering Practice No. 60, ASCE, Reston, Va.: This manual is the second revision of the relevant portions of the ASCE/WPCF Manual of Practice No. 37, *Design and Construction of Sanitary and Storm Sewers* and presents the current practice in the field of sanitary sewer design and construction. Its intended audience is design professionals knowledgeable in the areas of gravity sewers.

ASCE. (2010). *Minimum design loads for buildings and other structures*, ASCE/SEI Standard 7-10, ASCE, Reston, Va.: This update to ASCE/SEI Standard 7-05 and its supplement provides requirements for general structural design, and includes means for determining dead, live, soil, flood, wind, snow, rain, atmospheric ice, and earthquake loads, and their combinations that are suitable for inclusion in building codes and other documents.

American Society of Civil Engineers/American Water Works Association/Water Environment Federation (ASCE/AWWA/WEF). (2004a). *Interim voluntary guidelines for designing an online contaminant monitoring system*, ASCE, Reston, Va.: These guidelines are based on the USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004). Details are available at http://content.ewrinstitute.org/files/pdf/IVSGDOCMS_817R08007.pdf.

ASCE/AWWA/WEF. (2004b). *Interim voluntary security guidance for wastewater/stormwater utilities*, ASCE, Reston, Va.: These USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at http://content.ewrinstitute.org/files/pdf/IVGWU_817R08006.pdf.

ASCE/AWWA/WEF. (2004c). *Interim voluntary security guidance for water utilities*, ASCE, Reston, Va.: USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at http://content.ewrinstitute.org/files/pdf/IVGWU_817R08010.pdf.

ASCE/AWWA/WEF. (2006). *Guidelines for the physical security of wastewater/stormwater utilities*. ASCE Press, Reston, Va.: These guidelines are based on the USEPA WISE ASCE/AWWA/WEF Phase 3 Documents (December 2006). Details are available at <http://content.ewrinstitute.org/files/pdf/5.pdf>.

American Society of Industrial Security (ASIS). (2004). *Protection of assets*, ASIS, Alexandria, Va.: Although the availability of security literature is growing rapidly, with general and specialized texts, it has not been possible—until now—for a business manager or protection professional to find in one place, current, accurate, and practical treatment of the broad range of protection subjects, strategies, and solutions.

Association of State Drinking Water Administrators/National Rural Water Association (ASDWA/NRWA). (2002a). *Security vulnerability self-assessment guide for small drinking water systems*, ASDWA, Arlington, Va.: This guide is intended for water utilities that serve a population of less than 3,300. Its purpose is to help utilities identify critical assets and list appropriate security measures.

ASDWA/NRWA. (2002b). *Security vulnerability self-assessment guide for small drinking water systems serving populations between 3,300 and 10,000*, ASDWA, Arlington, Va.: This guide is intended for water utilities that serve a population from 3,300 to 10,000. It was developed to help utilities meet the requirements of the U.S. Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107-188).

ASTM International (ASTM). (2002). *F476-84(2002): Standard test methods for security of swinging door assemblies*, ASTM, West Conshohocken, Pa.: The standard test methods covered in this document are designed to measure the capability of a swinging door assembly to restrain or delay and to frustrate the commission of “break-in” crimes. Door assemblies of various materials and types of construction covered by these test methods also include individual components such as the hinge, lock, door, jamb/strike, and jamb/wall.

ASTM. (2003). *F1910-98(2003): Standard specification for long barbed tape obstacles*, ASTM, West Conshohocken, Pa.: This specification covers barbed tape materials and configurations used for security barriers. Referenced in this document are ASTM specifications A764, F1379, A176, A666, A370, and A240.

ASTM. (2004a). *A121-99(2004): Standard specification for metallic-coated carbon steel barbed wire*, ASTM, West Conshohocken, Pa.: This specification describes two-strand, metallic-coated, steel barbed wire fabricated of aluminum, zinc, and zinc-5% aluminum-mischmetal alloy coatings, with a number of coating weights, in a variety of designs.

ASTM. (2004b). *A176-99(2004): Standard specification for stainless and heat-resisting chromium steel plate, sheet, and strip*, ASTM, West Conshohocken, Pa.: This specification covers stainless and heat-resisting chromium steel plate, sheet, and strip. A wide variety of surface finishes may be available for the steel plate, sheet, and strips described in this specification.

ASTM. (2005a). *A666: Standard specification for annealed or cold-worked austenitic stainless steel sheet, strip, plate, and flat bar*, ASTM, West Conshohocken, Pa.: This specification covers the required annealed and cold-worked conditions for austenitic stainless steels in a variety of structural, architectural, pressure vessel, magnetic, cryogenic, and heat-resisting applications.

ASTM. (2005b). *A853-04: Standard specification for steel wire, carbon, for general use*, ASTM, West Conshohocken, Pa.: This specification covers carbon steel wire that is intended for general use, and is supplied in coils and is hard-drawn, annealed in process, or annealed at finish size.

ASTM. (2005c). *F1043-06: Standard specification for strength and protective coatings on steel industrial chain link fence framework*, ASTM, West Conshohocken, Pa.: This specification covers the strength and protective

- coating requirements for industrial steel chain link fence frameworks. Details include the maximum allowable heights of framework, post spacing based the mesh size and gauges of the fence fabric, and specified wind loads. Also included are factors to consider when determining wind load, the cross-sectional shape, and approved fabrication methods for posts and rails.
- ASTM. (2005d). *F552-02: Standard terminology relating to chain link fencing*, ASTM, West Conshohocken, Pa.: This specification contains the standard terminology associated with aspects of chain-link fencing design and construction.
- ASTM. (2005e). *F567-00: Standard practice for installation of chain-link fence*, ASTM, West Conshohocken, Pa.: The standard of practice pertaining to the installation procedure for chain-link fence is described in this document. While this practice describes performance under varying conditions, weather, intended use, materials, etc., it does not address all of the safety problems associated with the installation of a chain-link fence.
- Garcia, M. L. (2001). *The design and evaluation of physical protection systems*, Butterworth-Heinemann, Burlington, Mass.: This book provides detailed information on the full process of security system design and integration, illustrating how the various physical and electronic elements work together to form a comprehensive system.
- Illumination Engineering Society of North America (IESNA). (2003). *Guideline for security lighting for people, property, and public spaces (G-1-03)*, IESNA, New York.: This guideline covers basic security principles, illuminance requirements for various types of properties, protocols for evaluating current lighting levels for different security applications, and security survey and crime search methodology. This guideline includes exterior and interior security lighting practices for the reasonable protection of persons and property.
- National Association of Clean Water Agencies (NACWA). (2002). *Asset-based vulnerability checklist for wastewater utilities*, NACWA, Washington, D.C.: This document was developed to help wastewater utilities identify and evaluate the vulnerability of their assets, as well as the threats against them. This document was originally developed under NACWA's former name, Association of Metropolitan Sewerage Agencies (AMSA).
- NACWA. (2005). *Vulnerability Self Assessment Tool for Water & Wastewater Utilities* (version 3.2 update), NACWA, Washington, D.C.: Three versions of the Vulnerability Self Assessment Tool (VSAT) software—wastewater, water/wastewater/ and water—can be ordered from NACWA. This tool was originally developed under NACWA's former name, Association of Metropolitan Sewerage Agencies (AMSA).
- National Environmental Training Center for Small Communities (NETCSC). (2002). *Protecting your community's assets: A guide for small wastewater systems*, National Environmental Services Center, West Virginia University, Morgantown: This guide allows decision makers for small wastewater treatment systems to evaluate the security of their systems and to plan for emergencies. Tools provided in the guide include an Inventory of Critical Assets, Threat Assessment, Vulnerability Assessment Checklist, and Prioritization of Potential Corrective Actions.
- National Fire Protection Association (NFPA). (2002). *NFPA 101B: Code for means of egress for buildings and structures*, NFPA, Quincy, Mass.: This code includes the latest technologies, advances, and safety strategies in areas such as alarms, egress, emergency lighting, and special hazard protection. The contents are not meant as a standalone document, but for inclusion in a building code.
- NFPA. (2005). *National electrical code (NFPA 70) handbook*, NFPA, Quincy, Mass.: This code describes the safe installation and use of electrical equipment by consumers.
- NFPA. (2006). *NFPA 101: Life safety code*, NFPA, Quincy, Mass.: This code addresses those egress features necessary to minimize danger to life from fire and smoke, crowd pressures, and movement of individuals and groups. It provides minimum criteria for the design of egress facilities in order to permit prompt escape of occupants from buildings or, where desirable, into safe areas within buildings.
- Naval Construction Battalion Center (NCBC). (1990a). *Federal specification sheet: Fencing, wire and post, metal (chain-link fence gates)* (detail specification RR-F-191/2D), NCBC, Gulfport, Miss.: This document provides detailed requirements for chain-link fence gates and accessories.
- NCBC. (1990b). *Fencing, wire and post metal (and gates, chain-link fence fabric, and accessories)* (general specification RR-F-191/K), NCBC, Gulfport, Miss.: This specification covers general requirements for chain-link fencing and accessories, including classifications for various parts of fencing, wire and post metal, fencing fabric, gates, posts, top rails, braces, and accessories.
- NCBC. (1990c). *Fencing, wire and post, metal (chain-link fence accessories)* (detail specification RRF191/4D), NCBC, Gulfport, Miss.: This specification covers general requirements for chain-link fence accessories, including caps, rail sleeves, brace bands, rail and brace ends, wire ties and clips, tension wires, tension bars, truss rods, barbed wire, barbed wire support arms, and other miscellaneous accessories.
- Naval Facilities Engineering Service Center (NFESC). (1993a). *Design guidelines for physical security of facilities (MIL-HDBK-1013/1A)*, Washington Navy Yard, D.C.: This manual provides guidance to ensure that appropriate physical security considerations are included in the design of general facilities. Aspects considered in this manual include the predesign phase, the assessment of physical security threats, and an overview of the design phase. Specific technical sections in the manual also describe exterior site physical security, building physical security, ballistic attack hardening, standoff weapon hardening, and bomb blast hardening.
- NFESC. (1993b). *Design guidelines for security fencing, gates, barriers, and guard facilities (MIL-HDBK-1013/10)*, Washington Navy Yard, D.C.: This military handbook provides guidance and detailed criteria for the design, selection, and installation of new security fencing, gates, barriers, and guard facilities for perimeter boundaries of Navy and Marine Corps installations or separate activities, and designated restricted areas.
- NFESC. (1999). *Selection and application of vehicle barriers (MIL-HDBK-1013/14)*, Washington Navy Yard, D.C.: This handbook provides guidance to ensure that appropriate design, operational, environmental, cost, security, and safety considerations are included in the selection process for vehicle barrier systems. Topics covered in the handbook include vehicle barrier requirements, vehicle barrier installation and design, and descriptions and data on commercially available vehicle barriers and passive barriers that can be constructed on-site.
- Sandia Corporation. (2002). *Risk assessment methodology for water (RAM-W)*, Sandia Corporation (Sandia National Laboratories), Albuquerque, N.M.: This document is a two-volume training guide used in RAM-W methodology workshops.
- U.S. Code. (2009). 42 U.S.C. §300(i)(1), Office of the Law Revision Counsel, Washington, D.C.: This is U.S. Code Title 42, Section 300i-1, "Tampering with Public Water Systems."
- U.S. Department of Defense (DoD). (2002). *Minimum antiterrorism standards for buildings. Unified Facilities Criteria UFC 4-010-01*, DoD, Washington, D.C.: The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.
- U.S. General Services Administration (GSA). (2005). *Facilities standards for the public buildings service*, GSA, Washington, D.C.: These design standards and criteria are to be used in the programming, design, and documentation of GSA buildings.
- Water Environment Federation (WEF). (1992). *Design and construction of urban stormwater management*, Manual of Practice No. FD-20, WEF, Alexandria, Va.: This document provides design and construction best practices for urban stormwater management.
- WEF. (1993). *Design of wastewater and stormwater pumping stations*, Manual of Practice No. FD-4, WEF, Alexandria, Va.: This manual focuses on the design of wastewater and stormwater pumping stations.
- WEF. (1998). *Design of municipal wastewater treatment plants*, Manual of Practice No. 8, 4th ed., WEF, Alexandria, Va.: This is the industry standard for wastewater design. This is also ASCE Manuals and Reports of Engineering Practice No. 76.
- WEF. (1999). *Wastewater collection systems management*, Manual of Practice No. 7, 5th ed., WEF, Alexandria, Va.: Manual of Practice No. 7 is a reference for the operation and maintenance of a wastewater collection system.
- WEF. (2005). *Operation of municipal wastewater treatment plants*, Manual of Practice No. 11, 6th ed. (electronic version), WEF, Alexandria, Va.: This three-volume Manual of Practice covers the operation of municipal wastewater treatment plants. Volume I, Management and Support Systems, covers plant management, support systems, plant operations, safety and health, and chemical application systems. Volume II, Liquid Processes, addresses characterization and sampling of municipal wastewater, select biological processes, and other related topics. Volume III, Solids Processes, includes sludge thickening, aerobic and anaerobic digestion, sludge and lime stabilization, disposal of biosolids, and related topics.
- WEF. (2007). *Gravity sanitary sewer design and construction*, Manual of Practice No. FD-5, WEF, Alexandria, Va.: This manual is the second revision of the relevant portions of the ASCE/WPCF Manual of Practice No. 37, *Design and Construction of Sanitary and Storm Sewers* and presents

the current practice in the field of sanitary sewer design and construction. Its intended audience is design professionals knowledgeable in the areas of gravity sewers.

Water Security Working Group (WSWG). (2005). *Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on water security practices, incentives, and measures*. WSWG, U.S. Environmental Protection Agency, Washington, D.C.: This report presents the consensus reached by WSWG on 18 findings which (1) establish the features of active and effective security programs; (2) identify ways government and others might encourage utilities to adopt

and maintain active and effective programs; and (3) suggest utility-specific and national measures of water sector security progress.

Welter, G. J. (2003). *Actual and threatened security events at water utilities*. Water Research Foundation (WRF), Denver, Colo.: This report documents the security incidents, threats, and hoaxes that have involved or are of direct relevance to water systems. The report includes a review of 264 incidents, classifying them by geographic region, type of attacker, mode of attack, targeted asset, and other categorizations. The report reviews the incidents and discusses specific types of contaminants and the purported motivation of the attackers.

This page intentionally left blank

INDEX

- access control systems, 68
 - card reader systems, 46–47, 98–99
 - locks and padlocks, 46, 98
 - numeric keypad locks, 46, 98
- access rules, 2
- active infrared sensors, 45, 97
- aesthetic requirements, for security measures, 6, 72
- anti-climb/anti-cut fencing, 41, 93
- Asset-Based Vulnerability Checklist for Wastewater Utilities*, 5, 70
- background checks, 2, 4
- badge creation, 46, 98
- barbed-wire fence topping, 42, 94
- benchmark security measures
 - collection systems, 79–80, 80t–81t
 - pumping stations, 83, 84t–86t
 - raw water facilities, 7–8, 8t–11t
 - wastewater treatment plants, 74, 74t–77t
 - water distribution systems, 31–32, 32t–33t
 - water storage facilities, 25–26, 26t–29t
 - water system support facilities, 35–36, 36t–39t
 - water treatment plants, 19–20, 20t–24t
 - wells and pumping stations, 13, 14t–17t
- bollards, 44, 96
- bolt locks, for manholes, 50, 102
- building elements, 48, 100
- building entrances, 96
- buried line sensors, 45
- card reader systems, 46–47, 68, 98–99
- CCTV. *see* closed-circuit television (CCTV) surveillance
- chain-link fencing, 41, 93
- chain-link gates, 42, 94
- chemical fill-line locking devices, 49, 101
- chemical injection facilities, 19
- Circular Prestressed Concrete Water Tanks with Circumferential Tendons*, 25
- civil action warnings, 44, 96
- clear zones, 43, 95
- closed-circuit television (CCTV) surveillance
 - computer application software, 48, 100
 - digital video recorders, 47, 99
 - field of view, 47, 99
 - housings and mounts, 47, 99
 - video network servers, 47, 99
- Code for Means for Egress for Buildings and Structures*, 99
- codes, local, 6, 72
- collection systems
 - benchmark security measures, 79–80, 80t–81t
 - scope, 79
 - security approach philosophy, 79
 - system mission, 79
- color rendering index, 44, 96
- combustible materials, storage and use of, 73
- concertina-wire topping, 42, 94
- concrete masonry unit (CMU) wall height, 42
- concrete water storage tanks, 25
- consequence mitigation, 4, 5–6, 71
- cost-to-risk reduction curve, 5t, 71f
- criminals, 1–2, 67–68
- dams, 7, 8
- decision tree (example), 70f
- decorative planters, 44
- delay, 1, 67
- Design and Construction of Urban Stormwater Management*, 79
- design basis threats (DBTs), 1, 67
 - capability matrix, 3t, 69t
 - characterizing, 5, 70–71
- Design Guidelines for Fencing, Gates, Barriers, and Guard Facilities*, 100
- Design of Municipal Wastewater Treatment Plants*, 73
- Design of Wastewater and Stormwater Pumping Stations*, 83
- detection, 1, 67
- deterrence, 1, 67
- digital video recorders, 47, 99
- disinfection systems, 20
- door contact alarm switches, 46, 98
- doors, exterior, 48, 100
- drinking water standards, 19
- dual-technology sensors, 45
- electrical control panel enclosures, 100
- electronic gates, 42–43, 94–95
- electronic security systems
 - active infrared sensors, 45, 97
 - buried line sensors, 45, 97
 - door and hatch contact alarm switches, 46, 98
 - dual-technology sensors, 45, 46, 97, 98
 - exterior intrusion detection, 45, 97
 - fence-mounted sensors, 45–46, 97–98
 - glass-break sensors, 46, 98
 - interior intrusion detection, 46, 98
 - intrusion detection sensors, general, 45, 97
 - linear beam sensors, 46, 98
 - microwave sensors, 45, 97
 - pipeline vibration detection, 46, 98
- emergency generators, 20
- employee safety, and water treatment plants, 19
- entrances
 - building entrances, 44, 96
 - primary site entrance signage, 44
 - sallyport entrances, 43–44, 95–96
- equipment, protection of, 2
- exterior doors, 48
- exterior intrusion detection, 45, 97
- exterior surfaces, 44, 96
- Facilities Standards for the Public Buildings Service*, 100
- facility entrances
 - building entrances, 44, 96
 - primary site entrance signage, 44
 - sallyport entrances, 43–44

- fencing
 - anti-climb/anti-cut fencing, 41, 93
 - chain-link, 41, 93
 - fence-mounted sensors, 45–46
 - foundation enhancements, 42, 94
 - ornamental, 41–42, 93–94
 - signage, 44, 96
 - topping, 42, 94
- flammable materials, storage and use of, 73
- Garcia, Mary Lynn, 1
- gatehouses, 44
- gates
 - chain-link, 42, 94
 - electronic control system, 43, 95
 - electronic opening, 42–43, 94–95
- glass-break sensors, 46, 98
- Gravity Sanitary Sewer Design and Construction*, 79
- Guide for the Analysis, Design, and Construction of Concrete-Pedestal Water Towers*, 25
- guidelines, application of, 4–6, 67–72
- Guide Specifications for Commercial Security Hollow Metal Doors and Frames*, 100
- hatch contact alarm switches, 46, 98
- hatches
 - alarms, 48, 100
 - roof or sidewalk, 48–49, 100–101
 - vault door hatch set flush with top of structural slab, 49, 101
 - vault hatch with elevated curb, 49, 101
- hazardous chemical storage, 20
- hydrants, 49, 101
- improvised explosive devices (IEDs), 2
- improvised incendiary devices (IIDs), 2
- infrared sensors, 45, 97
- in-plant pumping stations, 20
- insider threats, 2, 4, 68–69
- Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*, 31
- Interim Voluntary Security Guidance for Wastewater/Stormwater Utilities*, 73
- Interim Voluntary Security Guidance for Water Utilities*, 7
- interior intrusion detection, 46, 98
- intrusion detection sensors, 45, 97
 - exterior, 45, 97
 - interior, 46, 98
- jersey barriers, 44
- Life Safety Code*, 99
- lighting
 - motion sensors and, 44
 - outdoor security, 44, 96
 - reflected, 96
- linear beam sensors, 46, 98
- locks, 46, 98
- main electrical switchgear, 20
- man-down transmitter, 49, 101
- manholes, 49–50, 101–102
- mechanical systems, special considerations for, 73
- microwave sensors, 45, 97
- Minimum Design Loads for Buildings and Other Structures*, 100
- motion sensors. *see also* intrusion detection sensors
 - dual-technology, 45, 97
 - lighting and, 44
- National Electrical Code*, 100
- numeric keypad locks, 46, 98
- online water control monitoring, 49
- online water quality monitoring, 101
- operator devices, 49, 101
- ordinances, 6, 72
- ornamental fencing, 41–42, 93–94
- outdoor security lighting, 44, 96
- padlocks, 46, 98
- pan locks, for manholes, 50, 102
- perimeter line, 42, 94
- perimeter walls, 42, 94
- personnel gates, 42–43
- physical security elements
 - access control systems, 46–47, 98
 - bollards and other vehicle barriers, 44, 96
 - building elements, 48, 100
 - CCTV surveillance, 47–48, 99–100
 - chemical fill-line locking devices, 49, 101
 - electronic security systems, 45–46, 97–98
 - exterior surfaces, 44, 96
 - facility entrances, 43–44, 95–96
 - fencing and perimeter walls, 41–42, 93–94
 - gates, 42–43, 94–95
 - hatches, vaults, and vents, 48–49, 100–101
 - hydrants, 49, 101
 - manholes, 49–50, 101–102
 - online water control monitoring, 49, 101
 - operator devices, 49, 101
 - outdoor security lighting, 44, 96
 - security, controls, and SCADA wiring, 48, 100
 - signage, 44–45, 96–97
 - site areas, 43, 95
- “pike” fence topping, 42
- pipelines
 - vibration detection, 46, 98
 - in water distribution systems, 31
- planters, decorative, 44
- power equipment and systems, 73
- primary site entrance signage, 44
- Protecting Your Community’s Assets: A Guide for Small Drinking Water Systems*, 70
- Protecting Your Community’s Assets: A Guide for Small Wastewater Systems*, 5
- protection-in-depth principles, 20
- Protection of Assets Manual* (ASIS), 41
- public health concerns, with water treatment plants, 19
- Pumping Station Design* (Jones), 13
- pumping stations, 20
 - benchmark security measures, 13, 14t–17t, 83, 84t–86t
 - facility mission, 13, 83
 - scope, 13, 83
 - security approach philosophy, 13, 83
- raw water facilities
 - benchmark security measures, 7–8, 8t–11t
 - facility mission, 7
 - scope, 7
 - security approach philosophy, 7

- reflected lighting, 44, 96
- reservoir dams, 7
- response, 1, 67
 - delay calculation concept, 2f, 68f
- response time and capabilities, 6, 72
- restrictive covenants, 6, 72
- Risk Assessment Methodology for Water Utilities (RAM-W), 5
- risk reduction, 5f
- roof hatches, 48–49, 100
- roof vents, 49, 101
- saboteurs, 2, 68
- sallyport entrances, 43–44, 95–96
- SCADA
 - access, 2, 68–69
 - control panel enclosures, 100
 - enhanced security measures for, 73
 - special security considerations for, 20
 - wiring, 48, 100
- security cages, 48, 100
- security grilles, 48, 100
- security lighting, 44, 96
- security measures
 - guidelines for new and existing facilities, 6, 71–72
 - identifying, 5, 71
 - levels of, 6, 72
- security systems, electronic. *see* electronic security systems
- Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*, 5, 70
- sensors, 1. *see also* electronic security systems; specific type of sensor
- sidewalk hatches, 48–49, 100
- signage
 - fence signage, 44, 96
 - primary site entrance signage, 44, 96
 - water intake delineation, 45
- site areas
 - clear zones, 43, 95
 - site utilities, 43, 95
- site utilities, 43, 95
- Special Weapons and Tactics (SWAT) team, 2
- Standard Guidelines for the Design, Installation, Maintenance and Operation of Urban Stormwater Systems*, 79
- steel water storage tanks, 25
- Steel Water-Storage Tanks*, 25
- storage facilities, 25–29
- stormwater utilities guideline applications, 67–72
- supervisory control and data acquisition (SCADA). *see* SCADA
- support facilities, 35–39
- SWAT team, 2
- tack welding, for manholes, 49, 101
- tampering, 44, 96
- Thermosetting Fiberglass-Reinforced Plastic Tanks*, 25
- tiered access strategies, 2
- toxic chemical storage, 20
- toxic gas storage facilities, 73
- vandals, 1, 67
- vaults, 100
- vehicle barriers, 44, 96
- vents, 101
 - alarms, 100
 - roof, 49, 101
- video network servers, 47, 99
- visual barriers, 1
- vulnerability assessment, 4–5, 67, 70
- Vulnerability Self-Assessment Tool (VSAT), 5
- Wastewater Collection Systems Management*, 79
- wastewater/stormwater system support facilities
 - benchmark security measures, 87, 88t–91t
 - facility mission, 87
 - scope, 87
 - security approach philosophy, 87
- wastewater treatment plants
 - benchmark security measures, 74, 74t–77t
 - facility mission, 73
 - scope, 73
 - security approach philosophy, 73
 - special considerations for critical assets, 73
- wastewater utilities guideline applications, 67–72
- water distribution systems
 - benchmark security measures, 31–32, 32t–33t
 - scope, 31
 - security approach philosophy, 31
 - system mission, 31
- water intake delineation, 97
- water storage facilities, 25–29
 - benchmark security measures, 25–26, 26t–29t
 - facility mission, 25
 - scope, 25
 - security approach philosophy, 25
- water system support facilities
 - benchmark security measures, 35–36, 36t–39t
 - facility mission, 35
 - scope, 35
 - security approach philosophy, 35
- Water Treatment Plant Design*, 19
- water treatment plants
 - benchmark security measures, 19–20, 20t–24t
 - facility mission, 19
 - scope, 19
 - security approach philosophy, 19
- water utilities
 - application of security guidelines, 1–6
 - distribution systems, 31–33
 - finished water storage facilities, 25–29
 - physical security elements, 41–50
 - raw water facilities, 7–11
 - support facilities, 35–39
 - water treatment plants, 19–24
 - wells and pumping stations, 13–17
- Water Wells*, 13
- Welded Carbon Steel Tanks for Water Storage*, 25
- wells
 - benchmark security measures, 13, 14t–17t
 - facility mission, 13
 - scope, 13
 - security approach philosophy, 13
- Wire- and Strand-Wound, Circular, Prestressed Concrete Water Tanks*, 25
- wiring, in security components, 48, 100