~~ASCE/AWWA Draft American National Standard for Trial Use~~

NOTE: Please be advised that effective December 1, 2008, ANSI has eliminated Annex B: Draft American National Standards for Trial Use as an option for announcing documents through ANSI. As a result, this document is not considered an ANSI American National Standard for Trial Use. Please also note that the period for submitting comments on this document has expired. Comments may still be forwarded to either ASCE or AWWA as noted on the cover below.

Guidelines for the Physical Security of Water Utilities

December 2006

American Society of Civil Engineers

American Water Works Association

The Authoritative Resource on Safe Water®

Water Environment Federation®
Preserving & Enhancing the Global Water Environment

Publication of this draft standard for trial use and comment has been approved by the American Society of Civil Engineers and the American Water Works Association. Distribution of this draft standard for comment shall continue for no longer than six months from the date of publication. It is expected that following this public comment period, this draft standard, revised as necessary, will be submitted to the American National Standards Institute for approval as an American National Standard. A public review in accordance with established ANSI procedures is required at the end of the trial use period and before a draft standard for trial use may be submitted to ANSI for approval as an American National Standard. This draft standard is not an American National Standard. Comments should be directed to:

ASCE
1801 Alexander Bell Drive
Reston, VA 20191
Attn: Standards Department

Or email: wise@asce.org

AWWA
6666 W. Quincy Avenue
Denver, CO 80235
Attn: Standards Department

Or email: standards@awwa.org

Contents

Foreword ..... **v**
Purpose of the Guidelines v
Background of the Development v
Use of this Draft American National Standard for Trial Use vi
Special Issues vii
Disclaimer viii
Acknowledgements ..... **ix**
1.0 Application of Guidelines **1-1**
1.1 Introduction 1-1
1.2 Methodology for Applying These Guidelines 1-6
2.0 Raw Water Facilities **2-1**
2.1 Scope 2-1
2.2 Facility Mission 2-1
2.3 Philosophy of Security Approach 2-1
2.4 Benchmark Security Measures 2-2
3.0 Wells and Pumping Stations **3-1**
3.1 Scope 3-1
3.2 Facility Mission 3-1
3.3 Philosophy of Security Approach 3-2
3.4 Benchmark Security Measures 3-2
4.0 Water Treatment Plants **4-1**
4.1 Scope 4-1
4.2 Facility Mission 4-1
4.3 Philosophy of Security Approach 4-1
4.4 Benchmark Security Measures 4-2
5.0 Finished Water Storage Facilities **5-1**
5.1 Scope 5-1
5.2 Facility Mission 5-1
5.3 Philosophy of Security Approach 5-2
5.4 Benchmark Security Measures 5-2
6.0 Distribution Systems **6-1**
6.1 Scope 6-1
6.2 System Mission 6-1
6.3 Philosophy of Security Approach 6-1
6.4 Benchmark Security Measures 6-2
7.0 Water System Support Facilities **7-1**
7.1 Scope 7-1
7.2 Facility Mission 7-1
7.3 Philosophy of Security Approach 7-2
7.4 Benchmark Security Measures 7-2

Appendices

A Physical Security Elements A-1
1.0 Fencing and Perimeter Walls A-1
2.0 Gates A-4
3.0 Site Areas A-6
4.0 Facility Entrances A-7
5.0 Bollards and Other Vehicle Barriers A-8
6.0 Exterior Surfaces A-8
7.0 Outdoor Security Lighting A-9
8.0 Signage A-10
9.0 Electronic Security Systems A-11
10.0 Access Control Systems A-15
11.0 Closed Circuit Television (CCTV) Surveillance A-16
12.0 Security, Controls, and SCADA Wiring A-19
13.0 Building Elements A-19
14.0 Hatches/Vaults and Vents A-21
15.0 Online Water Quality Monitoring A-22
16.0 Operator Devices A-22
17.0 Chemical Fill-Line Locking Devices A-23
18.0 Hydrants A-23
19.0 Manholes A-23

B Glossary and Abbreviations B-1

C References C-1

Figures

1-1 Concept of Delay Calculation 1-4

1-2 Example Decision Tree 1-7

1-3 Typical Cost-to-Risk Reduction Curve 1-9

Tables

1-1 Design Basis Threat Capability Matrix 1-4

2-1 Benchmark Security Measures for Raw Water Facilities 2-4

3-1 Benchmark Security Measures for Wells and Pumping Stations 3-4

4-1 Benchmark Security Measures for Water Treatment Plants 4-4

5-1 Benchmark Security Measures for Finished Water Storage Facilities 5-4

6-1 Benchmark Security Measures for Distribution Systems 6-3

7-1 Benchmark Security Measures for Water System Support Facilities 7-4

Foreword

This Draft Standard for Trial Use (DSTU) has been 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. The consensus process includes balloting by a balanced standards committee and reviewing during a public comment period. This DSTU will be reviewed and considered for approval as an American National Standard upon completion of the six-month public comment and trial use period.

The provisions of these documents 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 parenthesis. This approach is in the best interest of ASCE, AWWA, and WEF at the time of development of this Draft American National Standard for Trial Use.

Purpose of the Guidelines

This Draft American National Standard for Trial Use (DSTU) applies 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. These VAs often recommended security improvements to reduce the risk of malevolent acts (which 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 is 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 2004, AWWA 2004a, and WEF 2004). 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 focuses solely on the development of physical security guidelines for water, wastewater, and stormwater facilities. These voluntary consensus guidelines are to be published as Draft American National Standards for Trial Use through ASCE's and AWWA's American National Standards Institute (ANSI)-accredited standards development process. The primary reviewers were within the ASCE WISE Standards Committee (SC), Water Supply Subcommittee, Wastewater and Stormwater Subcommittee, 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 (AwwaRF) 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 on Water Sector Security Findings to the National Drinking Water Advisory Council (NDWAC) on May 18, 2005 (WSWG 2005). Those findings include fourteen 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 this Draft American National Standard for Trial Use

Major points for the trial use of this document imply:

(1) It is the responsibility of the user of an ANSI 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 draft 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™), the Vulnerability Self-Assessment Tool (VSAT™), 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 facility's criticality within the 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 7.0, which, in conjunction with the Foreword, 1.1 Introduction and its subsections, and Appendices in this document, can be used as standalone documents.

(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 2004, AWWA 2004a, and WEF 2004).

(2) Added water security is beneficial for continuity of business, protection of water quality, provision of sufficient water quantity, 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 design basis threats. 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 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 this Draft American National Standard for Trial Use guidance document 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 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 DSTU is not intended to warrant that the information contained therein 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.

Acknowledgements

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

Clifford L. Bowen, PE

William C. Boyle, PhD, PE, DEE

Erica M. Brown

Jeanette A. Brown, PE, DEE

Jonathan W. Bulkley, PhD, PE

Ivan Burrowes

James B. Conboy, PE, DEE

Joseph W. Dellapenna, Esq.

Clyde R. Dugan

John H. Easton, PhD

Findlay G. Edwards, PhD, PE (Vice Chair)

Wayne Einfeld

Jorge A. Garcia, PhD, PE

Neil S. Grigg, PhD, PE

Yakir J. Hasit, PhD, PE

Todd Humphrey, PE

C. Dale Jacobson, PE, DEE

Jyung Seok Jeong

Conrad G. Keyes, Jr. ScD, PE, PS, D.WRE (Chair)

M. Patricia Lamb, CUSA

Thomas J. Lane, PE

Srinivasa Lingireddy, PhD, PE

Thomas J. Linville, PE

Daniel L. Lynch, PE, DEE

John W. McLaughlin, PE

Brian M. Murphy, PE

Irwin M. Pikus, PhD, Esq.

J. Alan Roberson, PE

Kyle E. Schilling, PE, DEE, D.WRE

Charles R. Stack, MPH

C. Wesley Strickland, Esq.

Lloyd V. Urban, PhD, PE

James Van Norman

Gregory J. Welter, PE, DEE

James F. Wheeler, PE

Harold F. Wiedeman, PE

Robert C. Williams, PE, DEE

Water Supply Subcommittee

Edward E. Baruth (AWWA)

Beth Behner (AWWA)

Clifford L. Bowen, PE

Scott Brooks

Erica M. Brown

Clyde R. Dugan

Neil S. Grigg, PhD, PE

Todd Humphrey, PE

M. Patricia Lamb, CUSA (Vice Chair)

Thomas J. Lane, PE

Thomas J. Linville, PE

John W. McLaughlin, PE (Chair)

Brian M. Murphy, PE

James A. Roberson, PE

Roy Robinson (Past Chair)

James S. Wailes, PE (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. They included:

L. Christian Hanson, CAE (ASCE; WISE Project Manager and Recording Secretary for the WISE SC)

Conrad G. Keyes Jr. ScD, PE, PS. D.WRE (WISE Standards Committee Chair)

Findlay G. Edwards, PhD, PE (WISE Standards Committee Vice Chair)

John W. Mc Laughlin, PE (Water Supply Subcommittee Chair)

M. Patricia Lamb, CUSA (Water Supply Subcommittee Vice Chair)

Irwin M. Pikus, PhD, Esq. (Methodology and Characteristics Subcommittee Chair)

Yakir J. Hasit, PhD, PE (Methodology and Characteristics Subcommittee Vice Chair)

Jeanette A. Brown, PE, DEE (Wastewater/Stormwater Subcommittee Chair)

William C. Boyle, PhD, PE, DEE (Wastewater/ Stormwater Subcommittee Vice Chair)

Stacy Passaro, PE, BCEE (WEF; WISE Project Manager)

James S. Wailes, PE (AWWA; WISE Project Manager)

CH2M HILL Team

Jason M. Assouline

Paul A. Berg, PE

Richard D. Brady, PE, DEE (Richard Brady and Associates, Inc.)

Dale D. Gabel, PE

Forrest M. Gist, PE

Kristine K. Hargreaves, AIA

Yakir J. Hasit, PhD, PE

Sam Irrinki, PE

Alan B. Ispass, PE, DEE

Jacqueline T. Kepke, PE

M. Jane Mailand

Lena Perkins

USEPA

Gregory Spraul

1.0 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 the design basis threats (DBTs), with specified motivation, 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 (AWWA 2004a): 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.

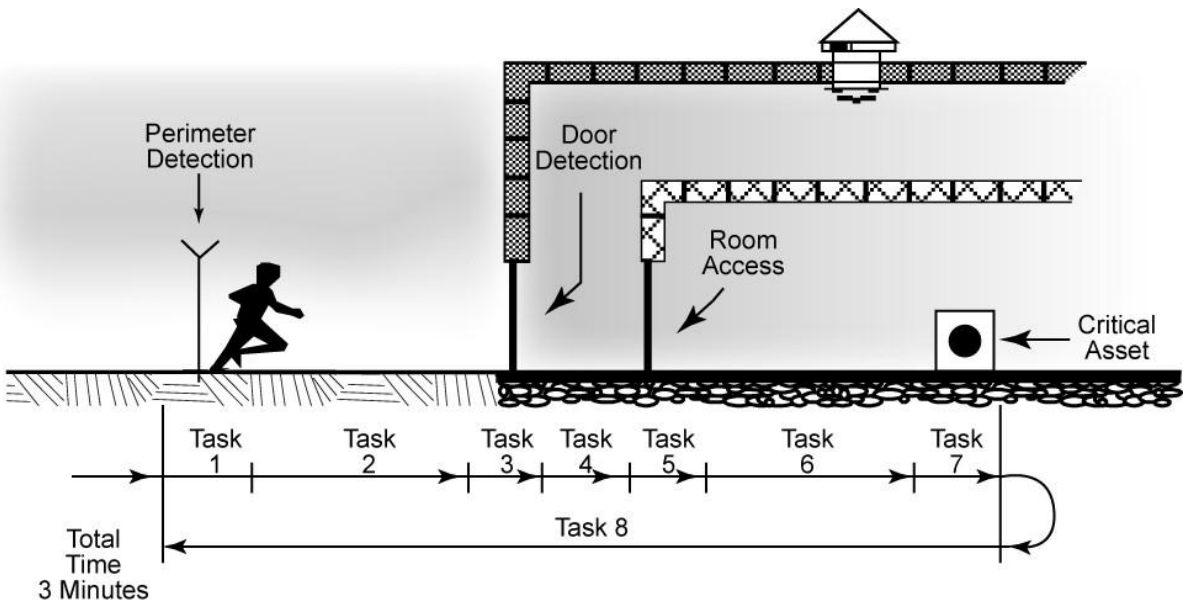
1.1.1.4 Response

(1) 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.

(2) 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.

(3) 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.



	Time Estimate				
Task	Task Time (minutes)	Cumulative Time (minutes)	Adversary Task Description	Response	
1	0.1		Climb over fence	1st Alarm	
2	0.3	0.4	Run 250 feet (76 m)		
3	0.8	1.2	Force door	2nd Alarm	Effective response time
4	0.4	1.6	Walk 150 feet (46 m)		
5	0.2	1.8	Cut door lock		
6	0.1	1.9	Walk to asset	Response Force Arrives	
7	0.2	2.1	Disable asset	Stop Adversary	
8	0.9	3.0	Escape		
	3.0		Total Time		

FIGURE 1-1
Concept of Delay Calculation (adapted from Garcia, 2001)

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

(1) 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.

(2) 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, that is, the repair or replacement of assets, than investing in expensive security systems and protective measures.

(3) An enhanced threat created by a more intense or invasive vandal (one consisting of a greater number of individuals that plan the activities or that has 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

(1) 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. Depending on the level of desperation or sophistication, criminals may be armed and willing to injure or kill to accomplish their objectives.

(2) Protective approaches against the base level of 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.

TABLE 1-1
Design Basis Threat Capability Matrix

Characteristic	Vandal		Criminal		Saboteur		Insider[1]	
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

[1]The 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.

(3) 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

(1) 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. 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.

(2) The difference between a base and enhanced level of threat from a saboteur is defined by the capabilities and methods. The base 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.

(3) 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

(1) 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.

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

(3) 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, "Methodology for Applying These Guidelines," 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, 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.

1.2.1.1 Step 1 – Vulnerability Assessment

(1) Complete a water system-wide VA and define the following:

(1) Critical assets to be protected

(2) DBT and its capabilities and motives

(3) Response force capabilities and response time

(4) Recommended security approach to reduce risk

(2) Several methodologies have been developed to assist utilities in completing vulnerability assessments. These include:

(1) Risk Assessment Methodology for Water Utilities (RAM-W™) developed by Sandia National Laboratories in partnership with the American Water Works Association Research Foundation (Sandia Corporation 2002)

(2) 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)

(3) "Asset Based Vulnerability Checklist for Wastewater Utilities," produced by AMSA (NACWA 2002)

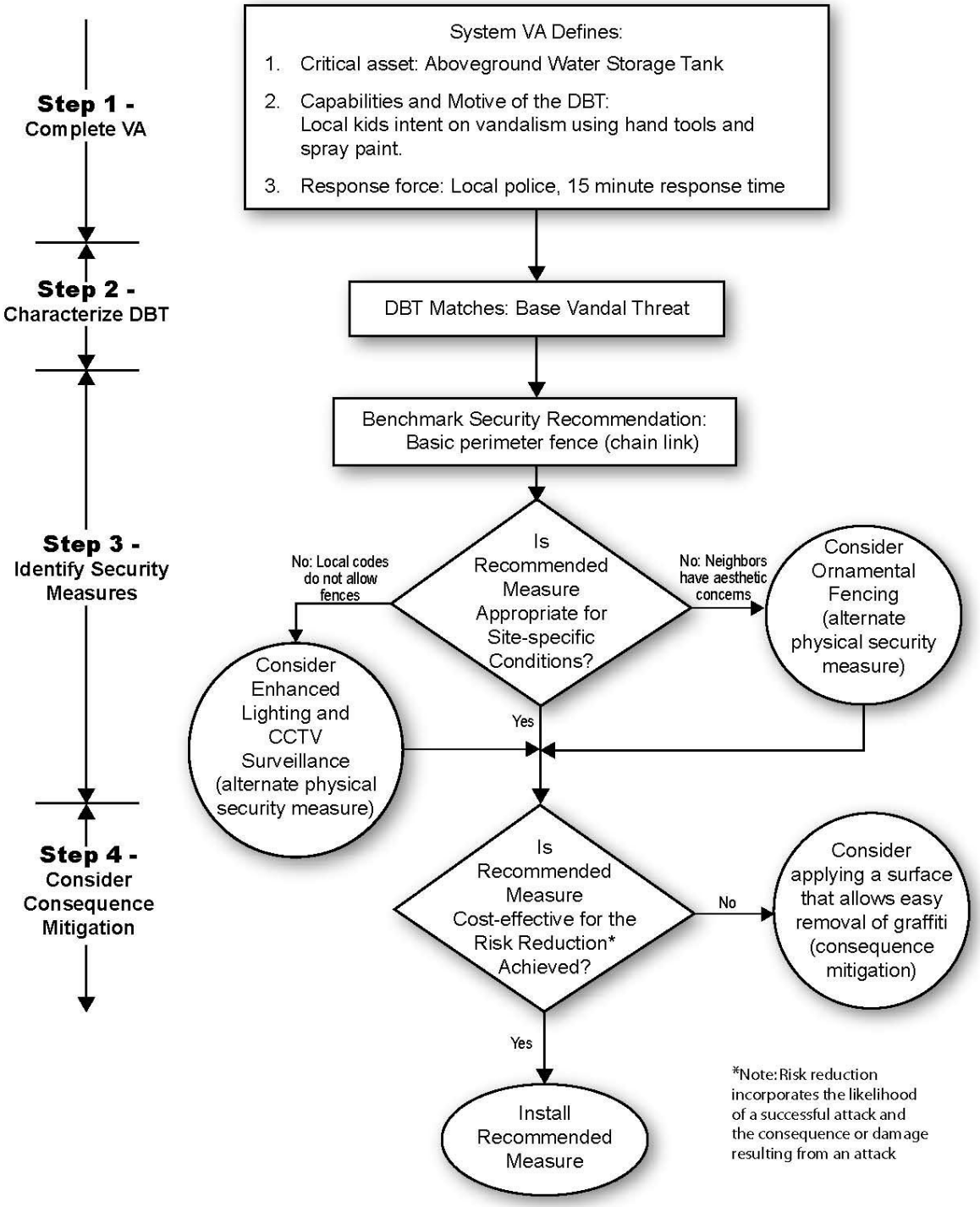


FIGURE 1-2
Example Decision Tree

(4) "Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems," prepared by the Association of State Drinking Water Administrators and National Rural Water Association (ASDWA 2002)

(5) "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 – Design Basis Threat

(1) Compare the DBT identified in the VA to the DBT levels described in 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 (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 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 similar objectives to the measure recommended in the table. Where certain measures may be less desirable (such as the 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, closed-circuit television 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 risk reduction associated with implementing additional security measures is marginal (WEF 2004). Management and operational measures to lower consequences are important elements of a utility or facility security plan that are not addressed in these guidelines.

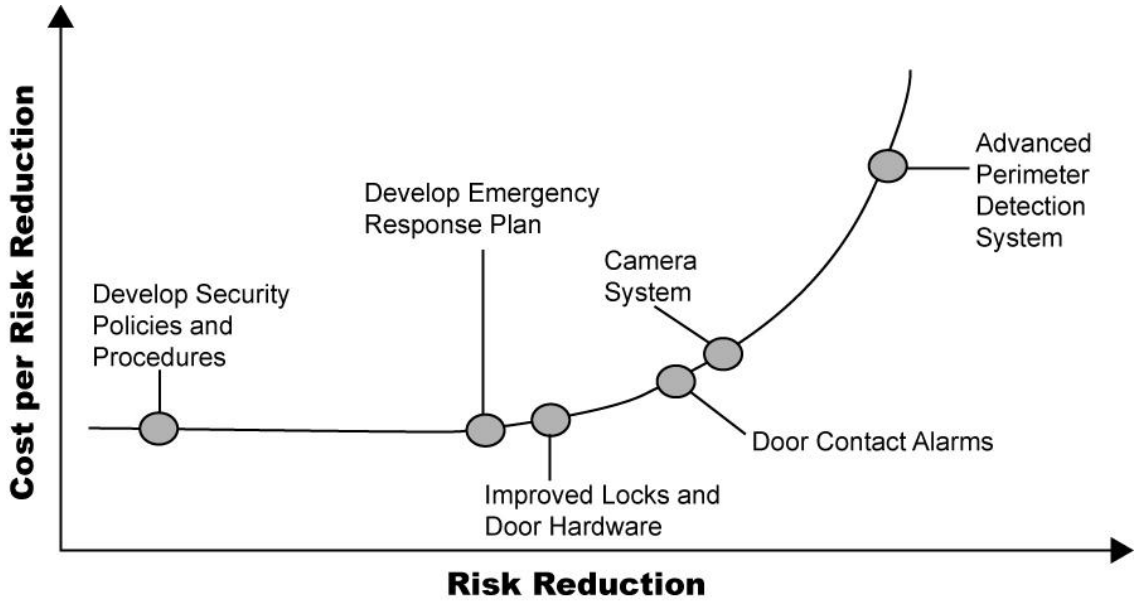


FIGURE 1-3
Typical Cost-to-Risk Reduction Curve (taken from Exhibit 1-13, WEF 2004)

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

(1) 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.

(2) 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 the owning parties.

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 high or if the response capability is low, additional security measures may be warranted.

2.0 Raw Water Facilities

2.1 Scope

(1) This section of this Draft American National Standard for Trial Use covers raw water facilities that are components of a municipal drinking water system and 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. It also does not include chemical feed facilities—these are addressed in the water treatment plant section (4.0).

(2) 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 or biological agent that contaminates the water supply.

(3) 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 design basis threats of 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 facility is to provide a supply of water to treatment plants. The facilities include storage reservoirs, basins, intakes, pipelines, and valve vaults. Generally, the facilities are not continuously staffed. They may be visited periodically by staff so that the staff can 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

(1) 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.

(2) 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.

(3) Benchmark security measures for deterrence, detection, and delay are provided in this guideline. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (AWWA 2004a) and are not addressed here.

2.4 Benchmark Security Measures

(1) 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

(2) 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 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).

(3) 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

TABLE 2-1
Benchmark Security Measures for Raw Water Facilities

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/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)

TABLE 2-1
Benchmark Security Measures for Raw Water Facilities

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	
Hardened site openings larger than 96 square inches (62,000 square millimeters) in area (e.g., grates on culverts)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3
"No Trespassing" signage (every 50 feet [15 meters])			✓	✓	✓	✓	✓	✓			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/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

TABLE 2-1
Benchmark Security Measures for Raw Water Facilities

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	
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	●			✓			✓	✓	✓		
Valve vault hatches – mechanically fastened or locked with shroud over lock	●		✓								10.2, 14.2

TABLE 2-1
Benchmark Security Measures for Raw Water Facilities

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	
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
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]	●							✓			

TABLE 2-1
Benchmark Security Measures for Raw Water Facilities

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 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 sq. in. (62,000 sq. mm)	●			✓	✓		✓				13.3
Grilles or other barriers with intrusion detection at skylights and louvers over 96 sq. in. (62,000 sq. mm)	●	●				✓		✓		✓	
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	●	●				✓		✓		✓	

TABLE 2-1
Benchmark Security Measures for Raw Water Facilities

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 (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

TABLE 2-1
Benchmark Security Measures for Raw Water Facilities

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	●							✓		✓	
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)

Notes:
[a] Many of the security measures identified in this table may also provide deterrence.
[b] Blast-resistant doors and glass are also bullet resistant.

3.0 Wells and Pumping Stations

3.1 Scope

This section of this Draft American National Standard for Trial Use covers water wells and pumping stations used within a water system. It establishes benchmark physical and electronic security features for protecting a well or 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

(1) 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 only periodically visit these facilities to perform maintenance 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.

(2) 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 a thousand gallons per day (3.8 cubic meters per day) to more than a million gallons per day (>3,800 cubic meters per day). Generally, operations and maintenance staff only periodically visit these facilities 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.

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

(4) More detailed information on wells can be found in AWWA Standard A100-06: Water Wells (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

(1) 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.

(2) 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.

(3) Benchmark security measures for deterrence, detection, and delay are provided in this section. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (AWWA 2004a) and are not addressed here.

3.4 Benchmark Security Measures

(1) 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

(2) 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

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 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 square inches (62,000 square millimeters) in area (e.g., grates on culverts)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3

TABLE 3-1
Benchmark Security Measures for Wells and Pumping Stations

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	
"No Trespassing" signage (every 50 feet [15 meters])			✓	✓	✓	✓	✓	✓			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

TABLE 3-1
Benchmark Security Measures for Wells and Pumping Stations

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 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	●		✓	✓			✓	✓			

TABLE 3-1
Benchmark Security Measures for Wells and Pumping Stations

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	
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

TABLE 3-1
Benchmark Security Measures for Wells and Pumping Stations

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, 13.2
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]	●							✓			
Glass-break detection at windows		●		✓		✓	✓	✓			9.3
Interior motion detection		●				✓		✓	✓	✓	9.3

TABLE 3-1
Benchmark Security Measures for Wells and Pumping Stations

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	
Grilles or other barriers at skylights and louvers over 96 sq. in. (62,000 sq. mm)	●			✓	✓		✓				13.3
Grilles or other barriers with intrusion detection at skylights and louvers over 96 sq. in. (62,000 sq. mm)	●	●				✓		✓		✓	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

TABLE 3-1
Benchmark Security Measures for Wells and Pumping Stations

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 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 3-1
Benchmark Security Measures for Wells and Pumping Stations

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)

Notes:
[a] Many of the security measures identified in this table may also provide deterrence.
[b] Blast-resistant doors and glass are also bullet resistant.

4.0 Water Treatment Plants

4.1 Scope

This section of the Draft American National Standard for Trial Use 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 or biological agent that contaminates the drinking water supply. 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 may be additional concerns requiring security features.

4.2 Facility Mission

(1) The mission of this facility is to treat source water to drinking water standards. Water treatment plants may produce from one hundred thousand gallons (380 cubic meters) to one hundred million gallons (1,140,000 cubic meters) 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.

(2) More detailed information on specific functions and treatment processes is contained in the *Water Treatment Plant Design – 4th Edition*, (AWWA/ASCE 2005a).

4.3 Philosophy of Security Approach

(1) 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.

(2) 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.

(3) Benchmark security measures for deterrence, detection, and delay are provided in this guideline. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (AWWA 2004a) and are not addressed here.

4.4 Benchmark Security Measures

(1) 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

(2) 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 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).

(3) 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, for example, chlorine or ammonia gas. The 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, 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. 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-foot (30-meter), 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. Closed-circuit television cameras (CCTVs) 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

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 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 sally port gate entrance for delivery vehicles	●	●				✓	✓	✓			4.0
Guardhouse and manned entrance gate to control site access	●	●						✓			
Perimeter site lighting		●	✓	✓	✓	✓	✓	✓			7.0

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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	
Gate entrance lighting		●		✓		✓	✓	✓			7.0 (4), (5), (6)
Hardened site openings larger than 96 square inches (62,000 square millimeters) 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
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/cut resistant	●							✓			1.2,
Intrusion detection at second layer of fencing		●					✓	✓		✓	3.0, 7.0, 9.1, 9.2, 11.0

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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	
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)

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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	
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
Clearwell hatch/manway – hardened lock with shroud or mechanically fastened	●		✓								8
Clearwell hatch/manway – double layer doors with shrouded lock	●			✓			✓		✓		8

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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 – 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

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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	
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	●	●				✓		✓			
Blast-resistant exterior doors[b]	●							✓			

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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 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 sq. in. (62,000 sq. mm)	●			✓	✓		✓				13.3
Grilles or other barriers with intrusion detection at skylights and louvers over 96 sq. in. (62,000 sq. mm)	●	●				✓		✓		✓	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	●	●				✓		✓		✓	

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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 (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

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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 – 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	●							✓		✓	

TABLE 4-1
Benchmark Security Measures for Water Treatment Plants

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)

Notes:
[a] Many of the security measures identified in this table may also provide deterrence.
[b] Blast-resistant doors and glass are also bullet resistant.

5.0 Finished Water Storage Facilities

5.1 Scope

This section of the Draft American National Standard for Trial Use 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

(1) 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.

(2) 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 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.

(3) AWWA Manual M-42, *Steel Water-Storage Tanks,* (1998) and *D100-05: Welded Carbon Steel Tanks for Water Storage* (2005b) provide additional information on the design and function of steel water storage tanks. Concrete tank standards and information are provided in AWWA's D110-04 (2004b), D115-95 (1995) and American Concrete Institute's (ACI) 371R-98

Guide for the Analysis, Design, and Construction of Concrete-Pedestal Water Towers. FRP tanks are covered in AWWA standard D120-02 (2002).

5.3 Philosophy of Security Approach

(1) An effective security approach for water storage facilities includes equipment or systems to deter, detect, delay, and respond to a threat prior to achieving his/her 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.

(2) 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.

(3) Benchmark security measures for deterrence, detection, and delay are provided in this section. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (AWWA 2004a) and are not addressed here.

5.4 Benchmark Security Measures

(1) 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

(2) 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

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 sq. inches (62,000 sq. mm.) in area (e.g., grates on vents)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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	
"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
Locate public or visitor parking as far away from 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/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

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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 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

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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	
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

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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	
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
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

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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	
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

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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 (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

TABLE 5-1
Benchmark Security Measures for Finished Water Storage Facilities

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)

Notes:
[a] Many of the security measures identified in this table may also provide deterrence.

6.0 Distribution Systems

6.1 Scope

This section of the Draft American National Standard for Trial Use 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, out of sight of the public. However, 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 (see Section 4.0 for chemical facilities).

6.3 Philosophy of Security Approach

(1) 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.

(2) 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.

(3) Benchmark security measures for deterrence, detection, and delay 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* (AWWA 2004a) and are not addressed here.

(4) 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.

(5) 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 2004) and to regular updates on the EPA web site for information on the topic of online contaminant monitoring.

6.4 Benchmark Security Measures

(1) 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

(2) 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 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).

(3) 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. 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 distribution system security can be found in Murphy et al. (2005).

TABLE 6-1
Benchmark Security Measures for Distribution Systems

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 uni-directional customer meters to reduce backflow potential	●						✓	✓			
Exposed pipelines: provide fence barrier to limit access to appurtenances	●			✓			✓				

TABLE 6-1
Benchmark Security Measures for Distribution Systems

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	
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 locking mechanisms	●			✓				✓			
Backflow prevention valves or tamper switches installed on connections to multi-family residential connections and commercial facilities (e.g., motels)	●							✓			
Backflow valves to limit potential for reverse flow at interconnections to neighboring water systems, wholesale customers, or customer connections to industrial facilities	●						✓	✓			

TABLE 6-1
Benchmark Security Measures for Distribution Systems

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
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)

Notes:
[a] Many of the security measures identified in this table may also provide deterrence.

7.0 Water System Support Facilities

7.1 Scope

This section of this Draft American National Standard for Trial Use presents guidelines 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 the 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, or 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 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, Supervisory Control and Data Acquisition (SCADA)/controls, reports, cash, business systems, heavy and mobile equipment, laboratory equipment and chemicals, and tools.

7.3 Philosophy of Security Approach

(1) 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.

(2) 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.

(3) Benchmark security measures for deterrence, detection, and delay are provided in this guideline. Approaches for consequence mitigation are presented in the *Interim Voluntary Security Guidance for Water Utilities* (AWWA 2004a) and are not addressed here.

7.4 Benchmark Security Measures

(1) 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

(2) 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).

(3) 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 7-1
Benchmark Security Measures for Water System Support Facilities

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 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 sally port gate entrance for delivery vehicles	●	●				✓	✓	✓			4.0
Guardhouse and manned entrance gate to control site access	●	●						✓			

TABLE 7-1
Benchmark Security Measures for Water System Support Facilities

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 site lighting		●	✓	✓	✓	✓	✓	✓			7.0
Gate entrance lighting		●		✓		✓	✓	✓			7.0 (4), (5), (6)
Hardened site openings larger than 96 square inches (62,000 square millimeters) in area (e.g., grates on culverts)	●		✓	✓	✓	✓	✓	✓			1.1, 13.2, 14.3
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
Public or visitor parking located as far away from the facility as practical, but at least 30 feet (9 meters) away	●							✓			
Eliminate parking underneath facilities	●							✓			
Second layer of basic fencing	●						✓			✓	1.0, 1.1

TABLE 7-1
Benchmark Security Measures for Water System Support Facilities

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	
Enhanced second layer of fencing that is climb/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
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 7-1
Benchmark Security Measures for Water System Support Facilities

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	●	●				✓		✓		✓	
Fuel storage tanks – locate 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	●		✓		✓				✓		
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

TABLE 7-1
Benchmark Security Measures for Water System Support Facilities

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	
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	●					✓		✓			
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	●		✓	✓	✓	✓	✓	✓			

TABLE 7-1
Benchmark Security Measures for Water System Support Facilities

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	
Grilles or other barriers at skylights and louvers over 96 sq. in. (62,000 sq. mm)	●			✓	✓		✓				13.3
Grilles or other barriers with intrusion detection at skylights and louvers over 96 sq. in. (62,000 sq. mm)	●	●				✓		✓		✓	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	●	●		✓	✓		✓		✓		

TABLE 7-1
Benchmark Security Measures for Water System Support Facilities

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 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
CCTV – Interior protected areas		●					✓	✓	✓	✓	11.0, 11.1, 11.2

TABLE 7-1
Benchmark Security Measures for Water System Support Facilities

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	●							✓		✓	
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)

Notes:
[a] Many of the security measures identified in this table may also provide deterrence.
[b] Blast-resistant doors and glass are also bullet resistant.

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 the owning parties.

1.0 Fencing and Perimeter Walls

(1) 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.

(2) Secondary goals may include screening the facility against visual observation, establishing a clear zone enhancing lighting and surveillance, and providing a means to install intrusion detection sensors.

1.1 Chain-Link Fencing

(1) For terms related to chain-link fencing systems, refer to American Society for Testing and Materials (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)" (Naval Construction Battalion Center 1990a). Both documents have been approved for public release and are available online. Aluminum fabric, poles, or accessories are not recommended for security applications.

(2) Base-level fence guideline is galvanized steel chain-link fence post with a 6-foot (1.8-meter [m]) or greater fabric height. Enhanced-level fence guideline is galvanized steel chain-link fence post with an 8-foot (2.4-m) or greater fabric height.

(3) 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.

(4) Base-level fabric wire gauge should be a minimum standard wire gauge of No. 9 and mesh pattern of 2-inch (50-millimeter [mm]) diamond mesh or smaller.

(5) Enhanced-level chain-link fencing should comply with the requirements for the base-level guideline chain-link fencing, except use No. 6 or No. 8 gauge fencing fabric in place of No. 9 gauge and select mesh patterns less than 2-inches (50 mm) across.

(6) 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 manufacturer's standard with allowance for minimum embedment below finished grade.

(7) The average dimension between line posts for chain link fences is recommended to be no more than 10 feet (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)" (Naval Construction Battalion Center 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.

(8) The ASIS "Protection of Assets" manual (ASIS 2004) further identifies that post hole depth be a minimum of 24 inches (610 mm), plus an additional 3 inches (76 mm) for each 1-foot (0.3-m) increase in fence height over 4 feet (1.2 m), such that an 8-foot (2.4-m) fence requires 36-inch (910-mm) depth for post holes. The hole should be backfilled with concrete]into the excavation hole (2500 pounds per square inch [psi] [17,000 kilopascals]) and the concrete extended 2 inches (50 mm) above grade, with a crowned surface to shed water.

(9) Where fences cross a stream, culvert, swale, depression or other openings that fencing does not enclose, where opening size is 96 square inches (62,000 square mm) or larger, these openings should be protected by additional grilles, fencing, or other barriers against penetration. Refer to 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.

1.2 Anti-Climb/Anti-Cut Fencing

(1) If the design basis threat (DBT) warrants, a specialized anti-climb/anti-cut fence such as wire-panel mesh fencing should be considered.

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

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

(4) 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 polyvinyl chloride (PVC) coating.

1.3 Ornamental Fencing

(1) 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.

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

(3) Suggested minimum sizes for fence pickets are 1-inch (25-mm) square by 0.062-inch (1.6-mm) thick, while suggested minimum fence rail dimensions are 1.625-inch (41-mm) by 0.070-inch (1.8-mm) thick top walls, and 1.625-inch (41-mm) by 0.100-inch (2.54-mm) thick side walls.

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

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

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

1.4 Perimeter Wall

(1) 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.

(2) Base-level concrete masonry unit (CMU) wall height should be 6-feet (1.8-m) high or greater. Enhanced-level CMU wall height should be 8-feet (2.4-m) high or greater. Wall thickness should be 8 inches (200 mm) as a suggested minimum with additional thickness as required to meet hardening designs.

(3) Immediate wall columns should be spaced per design criteria and site conditions.

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

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

1.5 Fencing Topping

(1) Fence topping may include barbed-wire topping or concertina barbed-wire tape topping, or a combination of both.

(2) For base-level barbed-wire topping guideline, 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 A 666, "Standard Specification for Annealed or Cold-Worked Austenitic Stainless Steel Sheet, Strip, Plate, and Flat Bar" (ASTM 2005a) to a 2-foot (0.6-m) high single outrigger; for enhanced-level climb resistance, use double Y-style outriggers with 3-strand barbed wire.

(3) For concertina-wire topping, attach 12-gauge stainless steel wires to 2-foot (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-inch to 30-inch (610 to 760 mm) diameter double coil concertina type. Each concertina loop should consist of 43 +/- 2 clusters of needle-sharp barbs on 4-inch (100-mm) centers, each barb measuring a minimum of 1.2 inches (30 mm) in length.

(4) 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)" (Naval Construction Battalion Center 1990c) for installation guidance.

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

1.6 Perimeter Line

(1) Periodic treatment of the perimeter line is recommended to prevent vegetation growth.

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

1.7 Fence Foundation Enhancements

(1) 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 similar delay to that of fencing. For anchorage of fabric, the bottom 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 guideline, the bottom rail may be anchored to an eyebolt embedded in a "deadman" anchor, a concrete cube 3 feet by 3 feet (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-inch (300 mm) deep rows of metal bars or pickets may be embedded at 12-inch (300 mm) intervals along the base of the fencing.

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

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.

2.1 Chain-Link Gates

(1) 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)" (Naval Construction Battalion Center 1990a).

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

(3) Entry gates should have reinforced steel latch with hardened steel padlock protection.

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

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

2.2 Electronic Gate Opening

(1) Electrical gate operators should be Underwriters Laboratory (UL)-listed, heavy-duty, high-frequency electrical models designed to open and close sliding or other types of gates as selected for specific applications. Gates should have maximum 2.5-inch (64 mm) clearance between bottom tension bar and finished grade.

(2) Electrical motors should be sized appropriately for 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.

(3) Recommended gate travel speed is a minimum 1 foot (0.3 m) per second. Speed adjusting feature that provides range of appropriate speeds for slide gate operation is recommended.

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

(5) Provide 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.

(6) Component parts of 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.

2.3 Electronic Gate Control System

(1) Pushbutton or card-reading sensor in weatherproof enclosure should be mounted on steel tube post or concrete bollard anchored to concrete foundation outside gate as required.

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

(3) Communication interface should enable remote monitoring of gate position from central location, such as central security office.

(4) Suggested operation sequence:

> (a) Entry: Gate opens when activated by valid card presented to card-reading sensor. Gate closes after sensing loop / sensing beam has determined that vehicle has passed through gate.
>
> (b) Exit: Gate opens when activated by detector loop in pavement or push button inside gate. Gate closes as for entry.

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

3.0 Site Areas

3.1 Clear Zones

(1) The purpose of a clear zone is such that intrusion detection surveillance and assessment using visual observation or cameras can be applied and to provide an unobstructed area in which placed devices can be readily observed/detected. Clear zone regions are typically established:

> (a) On both sides of a perimeter security fence to allow unobstructed surveillance of the fence area
>
> (b) 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
>
> (c) 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).

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

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

3.2 Site Utilities

(1) 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:

(a) Electrical Power

(b) Natural Gas

(c) Incoming Water

(d) Wastewater

(e) Fire Water Main(s)

(2) Exposed pipelines should be protected, where possible, using fence barriers to limit access.

(3) Alternatively, exposed pipelines could be run within carrier pipes to enable double-wall protection.

(4) Redundant utility connection sources should be provided if available. Dual electrical that feeds off separate circuits or incoming water supply from different source mains should be utilized where available.

(5) Electrical lines should be placed underground where applicable.

4.0 Facility Entrances

4.1 Sallyport Entrances

(1) 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.

(2) Typical vehicle sallyport dimensions are in the range of 75-feet (23-m) long by 20-feet (6-m) wide (and should be sized to accommodate the largest delivery vehicle), 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 2.0, Gates, of this Appendix.

(3) 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.

(4) Gate controls should be located in an area so that the person operating the controls maintains a constant visual observation of the sallyport area. The controls should be protected and covered so that non-authorized use is eliminated.

(5) A keyed manual override switch should be provided that allows the gates to be opened simultaneously. However, this override switch must be protected and covered such that the possibility of accidental operation is eliminated.

4.2 Building Entrances

(1) 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, anti-vandal furniture may be provided within the visitor waiting area.

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

(3) 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.

5.0 Bollards and Other Vehicle Barriers

(1) Bollards, jersey barriers, decorative planters, or other vehicle barriers, where applied, should be capable of stopping a 4,000-pound (1,800 kilogram [kg]) vehicle traveling at 30 miles per hour (48 kilometers per hour) within 3 feet (0.9 m) or less.

(2) 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.

6.0 Exterior Surfaces

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

(2) Apply non-stick, non-mark, polyurethane-based paints and coatings for external surfaces subject to vandalism.

7.0 Outdoor Security Lighting

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

(2) 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).

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

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

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

(5) If a gatehouse or sallyport entrance is used, an illumination level of 10 to 30 vertical foot-candles (110 to 320 luces) is the goal.

(6) Building exterior door areas should be illuminated to 3 to 5 horizontal foot-candles (32 to 54 luces), on average, for a radius of 15 feet (4.5 m) beyond the exterior door.

(7) General outdoor areas should be illuminated to 0.5 horizontal foot-candles (5 luces), average.

(8) 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 feet (7.6 m) on center.

(9) 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 foot-candles (5 luces) to 2 to 3 foot-candles (22 to 32 luces). If motion-activated lighting is included, make sure that lamp re-strike time is quick enough to support instant-on activation.

(10) When CCTV cameras are used, these additional lighting considerations should be taken (ASIS 2004, Chapter 19 – Security and Protective Lighting):

> (a) Color Rendering Index: Choose an appropriate lamp that has accurate color reproduction.

(b) Reflectance of Materials: Consider the material that will be illuminated, and its ability to reflect and transmit light.

(c) Direction of Reflected Lighting: Identify whether reflected lighting will assist or interfere with camera operation.

8.0 Signage

8.1 Fence Signage

(1) Post "No Trespassing" signs at 50-foot (15 m) intervals in multiple languages as consistent with local population. From a general legal standpoint, the fence and signage establishes a boundary that intruders must cross for violation.

(2) 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 (42 U.S.C. § 300 (i)(1)):

> a) 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.
>
> b) 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.
>
> c) 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.
>
> d) "Tamper" defined - For purposes of this section, the term "tamper" means –
>
> > (1) to introduce a contaminant into a public water system with the intention of harming persons; or
> >
> > (2) to otherwise interfere with the operation of a public water system with the intention of harming persons.

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.

8.3 Water Line Delineation

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

9.0 Electronic Security Systems

9.1 Intrusion Detection Sensors – General

(1) The intrusion detection system should be capable of detecting an individual (weighing 75 pounds (34 kg) or more) crossing the detection zone walking, crawling, jumping, running, or rolling (at speeds between 0.5 and 15 feet (0.2 and 4.6 m) per second), or climbing the fence, if applicable.

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

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

(4) Detection probability should be at a 95 percent confidence level. When calculating detection probability for multiple sensor systems, detection is assumed if any of the sensors detect the intrusion.

(5) Intrusion detection systems should cover the entire length of the perimeter of a detection area.

(6) Intrusion detection sensors should be provided with a redundant power source for a period of not less than four hours.

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

9.2 Exterior Intrusion Detection

(1) Prevalent sensor technologies include active infrared, microwave, dual-technology, buried-line, fence-mounted sensors, and video motion detection.

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

9.2.1 Active Infrared Sensors

(1) Active infrared sensors transmit infrared signals to a receiver. Interruption of the signal indicates an intruder or object has blocked the path.

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

(3) 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.

(4) 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.

(5) 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.

9.2.2 Microwave Sensors

(1) 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.

(2) 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 (large electric motors or generators) can affect the ability of the microwave sensors to function properly and should be avoided.

(3) Grass should be cut to less than 3 inches (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, trashcans, and electrical boxes. These dead spots create areas for intrusion attempts.

(4) 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, the protected area (because the signal can easily pass through standard walls, glass, sheet rock, and wood).

9.2.3 Dual Technology Sensors

(1) 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 degrees Fahrenheit (1.7 degrees Celsius).

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

(3) 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.

(4) Nuisance alarms for microwave sensors are described in 9.2.2. Nuisance alarms for PIR sensors include reflected light and radiated heat.

(5) 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 detections, false alarms are reduced.

9.2.4 Buried Line Sensors

(1) There are several types of buried line sensors, including fiber optic cable, ported cable, and ported coax cable.

(2) The two principle advantages of buried cable are that it is covert and it follows the terrain.

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

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

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

9.2.5 Fence-Mounted Sensors

(1) Fence-mounted sensors detect vibrations on fence fabric associated with sawing, cutting, climbing, or lifting the fence fabric.

(2) 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.

(3) 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.

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

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

(6) Nuisance alarms can be generated from shrubbery and tree branches as well as animals and severe weather that come in contact with the fence, causing it to vibrate.

9.3 Interior Intrusion Detection

(1) Provide appropriate interior intrusion detection according to the DBT and the building environment.

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

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

9.3.1 Dual Technology Motion Sensors

(1) Dual technology motion sensors use passive infrared and microwave technology to detect motion. Described in 9.2.3, these sensors are applicable for both interior and exterior applications.

(2) 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.

(3) 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).

9.3.2 Linear Beam Sensors

(1) 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.

(2) 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).

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

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

9.3.3 Glass-Break Sensors

(1) There are three basic types of glass-break sensors: acoustic sensors (listens for an acoustic sound wave that matches the frequency of broken glass), shock sensors (feels the shock wave when glass is broken), and dual-technology sensors (senses acoustic and shock vibrations).

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

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

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

(5) Regardless of the type of sensor, coverage typically does not exceed 100 square feet (9 square meters) of glass surface.

(6) 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.

9.4 Door and Hatch Contact Alarm Switches

(1) Door and hatch contact alarm switches should interface to a security monitoring system in addition to the SCADA system.

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

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

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

9.5 Pipeline Vibration Detection

(1) Emerging technologies are being developed that provide vibration detection within pipeline sections. By incorporating this technology, attempts at sabotage such as cutting, hammering or detonation of the pipeline can be detected and a response can be initiated. Such detection systems might be considered for critical pipeline sections without redundancy. The detection systems monitor vibration within the pipeline section. If the vibration level exceeds a threshold amount, then an alarm may be transmitted back to a central monitoring station. Such systems are relatively new technology, but are in operation currently for critical utility (oil, natural gas) pipelines within the United States.

10.0 Access Control Systems

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.

10.2 Locks and Padlocks

(1) Padlocks should be weather-resistant with a hardened-steel shackle.

(2) Padlock pulling resistance should be 4,500 pounds (lbs.) (20,000 Newtons) at minimum.

(3) Padlock pressure resistance to bolt cutters should be 10,000 lbs. (44,000 Newtons) at minimum.

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

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

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

10.3 Numeric Keypad Locks

(1) 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.

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

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

10.4 Card Reader Systems

(1) Card reader systems should incorporate:

(a) Alarm Display and Programming: A computer server or workstation that displays alarm conditions and allows programming of the system.

(b) Badge Creation: A badge station, allowing creation and programming of badges.

(c) Local Control: Local control panels that control the doors, card reader units, and access cards.

(d) Printer Unit: A printer unit that can print a report for each event and alarm condition.

(2) 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.

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

(4) 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.

(5) 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 free egress is permitted at all times.

(6) 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.

11.0 Closed Circuit Television (CCTV) Surveillance

11.1 General Considerations

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

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

(a) Imager: The size of the image-sensing device within the camera.

(b) Resolution: The measure of detail that the camera can distinguish, usually measured in horizontal TV lines per inch (25 mm). The larger the number, the sharper the image and the better the camera.

(c) Sensitivity: Typically, the minimum lighting illumination level required for full video. The lower the required illumination level, the more sensitive the camera.

(d) 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.

(e) 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.

(f) Backlight Compensation: A feature available in many cameras that automatically reduces contrast and silhouetting between near and far objects.

(g) Video Output: A measurement, stated in Volts peak-to-peak, between the darkest black to brightest light levels of the signal. Typical values are 1.0 Volts peak to peak.

(h) Synchronization: A means of controlling the imager scanning so that the camera image will not roll when switched between video monitors. Better cameras allow for synchronization adjustment to accommodate multi-phase power supplies.

(i) 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.

(j) Dimensions: The outside measurements of the camera case.

(k) Weight: The weight of the camera within its casing.

(3) 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.

11.2 Field of View

(1) Provide fixed-position or pan/tilt/zoom cameras depending upon desired field of view and intended application.

(2) Provide appropriate camera lenses corresponding to camera application and field of view requirements.

(3) 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 percent = 480 pixels).

(a) For intrusion detection purposes, the object should occupy a minimum of 10 percent of the screen height or be 48-pixels tall.

(b) For recognizing a person's face, the body of the person should be a minimum of 50 percent of the screen height or 240-pixels tall.

(c) To identify a license plate, the plate height should be a minimum of 5 percent of the screen height or 24-pixels tall.

(4) 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 with modern CCTV systems allows masking of these areas or views so that they cannot be seen by the attendant staff.

11.3 CCTV Housings and Mounts

(1) CCTV housings should be adequate for the intended application and site location.

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

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

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

11.4 Video Network Servers

(1) The video network server should be high-performance Internet-Protocol (IP) network-compatible video system.

(2) The network server should be capable of streaming images at a frame rate of 30 frames per second.

(3) 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.

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

11.5 Digital Video Recorders

(1) As a minimum, it is recommended to provide adequate digital recording capacity for all cameras at 30 days of continuous storage at 5 frames per second.

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

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

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

11.6 CCTV Computer Application Software

(1) CCTV application software should be full management software to monitor and manage single or multiple sites.

(2) Software should allow monitoring and recording of images from multiple simultaneous cameras at frame rates up to 30 frames per second.

(3) System should enable customized layouts for intuitive and interactive ways of representing the camera network.

(4) Software should provide flexible live and recording settings per individual camera input.

(5) 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.

12.0 Security, Controls, and SCADA Wiring

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

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

(3) The security wiring configuration at the end device should be a 4-state configuration using an end-of-line (EOL) resistor network where neither alarm nor normal condition are 0 ohms or open-circuit.

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

(5) Provide a backup power source (4 hours minimum) to security components and SCADA and other crucial control systems.

(6) Backup power sources may include battery units, auxiliary power supplies, uninterruptible power supplies (UPS), or generators.

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

12.1 SCADA and Electrical Control Panel Enclosures

(1) 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.

(2) Though panels should be locked, the electrical disconnect should never be locked.

13.0 Building Elements

13.1 General

(1) 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 the ASCE and SEI (Structural Engineering Institute) in "Minimum Design Loads for Buildings and Other Structures" (ASCE/SEI 2006) 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."

13.2 Doors

(1) Exterior doors should be heavy-duty steel-metal door, ASTM F476 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).

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

(3) Door frame should be heavy-duty with concrete fill.

(4) Hinge pins should be on the secure side or be non-removable/tamper-resistant to eliminate door compromise by removing hinge pins.

(5) Consider electronic door status monitoring for door forced and door ajar conditions.

(6) 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).

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

13.3 Security Grilles

(1) Base-level security grilles (for windows, louver openings, roof hatches, culverts, etc.) should be woven #10 wire gauge steel, 1.5-inch (38-mm) diamond mesh, or welded #10 wire gauge, 2-inch (50-mm) square welded mesh screens.

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

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

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

13.4 Security Cages

(1) Caged partitions (for critical equipment, pumps, motor control centers, and so on) should be #10 wire gauge steel with 2-inch (50 mm) welded openings in 1.25-inch by 1.25-inch by 0.125-inch (32-mm by 32-mm by 3-mm) angle iron framework.

(2) Ensure the partitions include framework supports, access gates, locks, and other accessories.

14.0 Hatches/Vaults and Vents

14.1 Hatch, Vault, and Vent Alarms – General

(1) Hatch, vault, and vent alarms should use similar alarm contact hardware such as magnetic door contact switches, depending on the final hatch/vault design.

(2) Interconnect alarm contacts to a security monitoring system.

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

(4) Provide locking covers for valve operators.

14.2 Roof or Sidewalk Hatches

(1) Provide a lock on a manufacturer's metal door system that is set into concrete curb with gutter and drain.

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

(3) Consider an elevated upper structure cover surrounding the 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.

(4) Alarm upper structure using exterior-rated balanced magnetic door contacts.

14.3 Roof Vents

(1) Provide metal roof vents with numerous small openings rather than vents with fewer, larger openings (96 square inches [62,000 square mm] 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.

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

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

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

(5) Alarm protective cover using exterior-rated magnetic door contacts.

14.4 Vault Hatch with Elevated Curb

(1) Provide lock on manufacturer's door system. Alarm the vault hatch using exterior-rated magnetic door contacts.

(2) Consider an additional protected key bar lock across the door that is mounted directly to the structural curb.

14.5 Vault Door Hatch Set Flush with Top of Structural Slab

(1) Provide a lock on a manufacturer's door system. Alarm vault hatch using exterior-rated magnetic door contacts.

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

15.0 Online Water Quality Monitoring

(1) A suite of online instruments to monitor some surrogate water quality parameters should be installed.

(2) Among parameters to monitor in water distribution systems are pH, chlorine residual (either total or free, depending on the type of residual maintained in the system), specific conductance, turbidity, and total organic carbon.

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

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

(5) 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, then the sampling location should be installed on the common pipe near the tank, ideally between the tank and the isolation valve.

16.0 Operator Devices

16.1 Man-Down Transmitter

(1) A man-down transmitter is worn by personnel for automatic man-down signaling.

(2) The unit should be portable, lightweight, and supplied with a belt clip or holster for mounting.

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

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

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

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

17.0 Chemical Fill-Line Locking Devices

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

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

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

18.0 Hydrants

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

(2) 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.

> (a) 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.
>
> (b) Provide the specialized wrenches in sufficient quantity to the fire department and other authorized persons so that they can operate the hydrants as needed. These wrenches are typically only sold to fire authorities and water utilities.

19.0 Manholes

(1) Securing manholes can be accomplished in three ways; tack welding, bolt locks, and pan locks:

(a) Tack welding provides a fast method of securing manholes. It is economical and effective for manholes not frequently accessed. The disadvantage is that the tackweld must be removed or broken before utility staff can access the manhole.

(b) Bolt locks anchor the manhole to the manhole frame. They have a specialized bolt head which 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.

(c) 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 into the pan unit. This system of locking manholes is more flexible than the tack welding and bolt locking methods, but more expensive to install.

APPENDIX B

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 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. American Society for Testing and Materials.

AWWA. American Water Works Association.

AwwaRF. American Water Works Association Research Foundation.

base. Minimum recommended.

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

CCTV. Closed-circuit television.

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.

CSC. Codes and Standards Committee.

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. Department of Defense.

DSTU. Draft American National Standard for Trial Use.

DVD. Digital Versatile Disc, Digital Video Disc.

EFI. Electronic frequency interference.

enhanced. Augmented with improved, advanced, or sophisticated features.

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. 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 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, 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.

lb. Pound.

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

luces. Plural of lux.

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.

protection in depth. The strategy of providing multiple layers of protective measures, therefore 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.

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.

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 over-ride 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.

TISP. The Infrastructure Security Partnership.

UL. Underwriters Laboratory.

UPS. Uninterruptible power supply.

USEPA. U.S. Environmental Protection Agency.

VA. 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 sally port. 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 sally port, 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.

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 non-terrorist 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™).

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.

APPENDIX C

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 (2004), the American Water Works Association (2004a), and the Water Environment Foundation (2004).

Reference	Annotation
American Concrete Institute (ACI). 1998. 371R-98: Guide for the Analysis, Design, and Construction of Concrete-Pedestal Water Towers (Reapproved 2003). www.concrete.org/bookstorenet/ProductDetail.aspx?itemid=37198	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 (ANSI)/National Association of Architectural Metal Manufacturers (NAAMM) Hollow Metal Manufacturers Association (HMMA). 2003. Guide Specifications for Commercial Security Hollow Metal Doors and Frames. Chicago, IL. www.naamm.org/hmma/pdfs/HMMA862-03.pdf	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 Industrial Security (ASIS). 2004. Protection of Assets. 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 Society of Civil Engineers (ASCE). 2006. Minimum Design Loads for Buildings and Other Structures, ASCE/SEI Standard 7-05. Reston, VA: ASCE. https://www.asce.org/bookstore/book.cfm?book=5581	This update to ASCE/SEI Standard 7-02 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 (ASCE). 2004. Guidelines for Designing an Online Contaminant Monitoring System. Reston, VA. www.asce.org/static/1/wise.cfm	USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at the ASCE, AWWA, WEF, and USEPA web sites.
American Water Works Association (AWWA). 2006. A100-06: Water Wells. Denver, CO. www.awwa.org/bookstore/product.cfm?id=41100	This standard provides the minimum requirements for vertical water supply wells, including geologic/hydrologic conditions and water quality and well construction.

Reference	Annotation
American Water Works Association (AWWA) and American Society of Civil Engineers (ASCE). 2005a. Water Treatment Plant Design, Fourth Edition. McGraw-Hill.	This book is a reference for water treatment plant upgrades or new construction. Topics included range from initial plans and permits, through design, construction, and startup.
American Water Works Association (AWWA). 2005b. D100-05: Welded Carbon Steel Tanks for Water Storage. www.awwa.org/bookstore/product.cfm?id=44100	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.
American Water Works Association (AWWA). 2004a. Interim Voluntary Security Guidance for Water Utilities. Denver, CO. www.awwa.org/science/wise/	USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at the ASCE, AWWA, WEF, and USEPA web sites.
American Water Works Association (AWWA). 2004b. D110-04: Wire- and Strand-Wound, Circular, Prestressed Concrete Water Tanks. Denver, CO. www.awwa.org/bookstore/product.cfm?id=44110	This standard details recommended practice for the design, construction, inspection, and maintenance of these types of water tanks.
American Water Works Association (AWWA). 2002. D120-02: Thermosetting Fiberglass-Reinforced Plastic Tanks. Denver, CO. www.awwa.org/bookstore/product.cfm?id=44120	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.
American Water Works Association (AWWA). 1998. Steel Water-Storage Tanks (M42). Denver, CO. www.awwa.org/bookstore/product.cfm?id=30042	This manual provides information on the selection, design, construction, and maintenance of steel tanks for potable water storage.
American Water Works Association (AWWA).1995. D115-95: Circular Prestressed Concrete Water Tanks With Circumferential Tendons. Denver, CO. www.awwa.org/bookstore/product.cfm?id=44115	This standard includes current and recommended practice for the design, construction, and field observations of circular prestressed concrete tanks using tendons for circumferential prestressing.
Association of State Drinking Water Administrators (ASDWA) and National Rural Water Association (NRWA). 2002a. Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems. May 30. http://www.asdwa.org/index.cfm?fuseaction=Page.viewPage&pageID=733	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 (ASDWA) and National Rural Water Association (NRWA). 2002b. Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3,300 and 10,000. November 13. http://www.asdwa.org/index.cfm?fuseaction=Page.viewPage&pageID=733	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 "Public Health Security and Bioterrorism Preparedness and Response Act of 2002."
ASTM International. 2005a. A 666, Standard Specification for Annealed or Cold-Worked Austenitic Stainless Steel Sheet, Strip, Plate, and Flat Bar. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/A.htm?L+mystore+qkng6334+1140140874	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.

Reference	Annotation
ASTM International. 2005b. A853-04, Standard Specification for Steel Wire, Carbon, for General Use. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/A853.htm?L+mystore+uidi9817	This standard specification covers carbon steel wire that intended for general use that is supplied in coils and is produced hard drawn, annealed in process, or annealed at finish size.
ASTM International. 2005c. F1043-06, Standard Specification for Strength and Protective Coatings on Steel Industrial Chain Link Fence Framework. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874	This specification covers the strength and protective coating requirements for industrial steel chain link fence framework. Details include the maximum allowable heights of framework, post spacing based the mesh size and gages of the fence fabric, and specified wind loads. Also include are factors to consider when determining wind load as well as the cross-sectional shape and approved fabrication methods for posts and rails.
ASTM International. 2005d. F552-02, Standard Terminology Relating to Chain Link Fencing. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874	This specification contains the standard terminology associated with aspects of chain-link fencing design and construction.
ASTM International. 2005e. F567-00, Standard Practice for Installation of Chain-Link Fence. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874	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, with the installation of a chain-link fence.
ASTM International. 2004a. A121-99(2004), Standard Specification For Metallic-Coated Carbon Steel Barbed Wire. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/A.htm?L+mystore+qkng6334+1140140874	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 International. 2004b. A176-99(2004), Standard Specification for Stainless and Heat-Resisting Chromium Steel Plate, Sheet, and Strip. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/A.htm?L+mystore+qkng6334+1140140874	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 International. 2003. F1910-98(2003), Standard Specification for Long Barbed Tape Obstacles. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874	This specification covers barbed tape materials and configurations used for security barriers. Referenced in this document are the ASTM specifications A764, F1379, A176, A666, A370, and A240.
ASTM International. 2002. F476-84(2002), Standard Test Methods for Security of Swinging Door Assemblies. http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/F.htm?L+mystore+qkng6334+1140140874	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.

Reference	Annotation
Department of Defense (DoD). 2002. Minimum Antiterrorism Standards for Buildings. Unified Facilities Criteria UFC 4-010-01. www.tisp.org/files/pdf/dodstandards.pdf	The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria.
Garcia, Mary Lynn. 2001 The Design and Evaluation of Physical Protection Systems. Burlington, MA: Butterworth-Heinemann.	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). New York, NY.	This guideline covers basic security principles, illuminance requirements for various types of properties, protocol 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, Garr M., Robert L. Sanks, George Tchobanoglous, and Bayard E. Bosserman, II. Eds. 2005. Pumping Station Design, 3rd edition. Butterworth-Heinemann.	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, NY, NY.	This handbook provides material to design, analyze, operate, maintain, and rehabilitate water distribution systems. Topics include from hydraulic design for pipelines and tanks to water quality issues, computer models, and rehabilitation/replacement information
Murphy, B., L.L. Radder, G.J. Kirmeyer. 2005. Distribution Systems Security Primer for Water Utilities. AwwaRF. Denver, CO.	This document provides tools to assess, prioritize, and address water distribution system vulnerabilities.
National Association of Clean Water Agencies (NACWA). 2005. Vulnerability Self Assessment Tool™ for Water & Wastewater Utilities (Version 3.2 Update). February. http://www.nacwa.org/pugs/index.cfm	Three versions of the Vulnerability Self Assessment Tool™ (VSAT™) software—wastewater, water/wastewater/ and water—can be ordered from this web site. This tool was originally developed under NACWA's former name, Association of Metropolitan Sewerage Agencies (AMSA).
National Association of Clean Water Agencies (NACWA). 2002. Asset Based Vulnerability Checklist for Wastewater Utilities©. http://www.nacwa.org/pugs/index.cfm	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).
National Environmental Training Center for Small Communities (NETCSC). 2002. Protecting Your Community's Assets: A Guide for Small Wastewater Systems. November. http://www.nesc.wvu.edu/netcsc/netcsc_tresource.htm#tool	This guide allows decisionmakers 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.

Reference	Annotation
National Fire Protection Association (NFPA). 2006. NFPA 101®: Life Safety Code®. Quincy, MA.	This code addresses those egress features necessary to minimize danger to life from fire and smoke, crowd pressures, and movement of individuals and groups, and 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.
National Fire Protection Association (NFPA). 2005. National Electrical Code® (NFPA 70) Handbook. Quincy. MA.	This code describes the safe installation and use of electrical equipment by consumers.
National Fire Protection Association (NFPA). 2002. NFPA 101B: Code for Means of Egress for Buildings and Structures. Quincy, MA.	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.
Naval Construction Battalion Center. 1990a. Federal Specification Sheet: Fencing, Wire and Post, Metal (Chain-Link Fence Gates) (Detail Specification). http://www.wbdg.org/ccb/FEDMIL/rrf1912d.pdf	This document provides detailed requirements for chain-link fence gates and accessories.
Naval Construction Battalion Center. 1990b. Fencing, Wire and Post Metal (and Gates, Chain-Link Fence Fabric, and Accessories) (General Specification). http://www.wbdg.org/ccb/FEDMIL/rrf191k.pdf	This specification covers general requirements for chain-link fencing and accessories including classification for various parts of fencing, wire and post metal, fencing fabric, gates, posts, top rails, braces, and accessories.
Naval Construction Battalion Center. 1990c. Fencing, Wire and Post, Metal (Chain-Link Fence Accessories) (Detail Specification). http://www.wbdg.org/ccb/FEDMIL/rrf1914d.pdf	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). 1999. Selection and Application of Vehicle Barriers (MIL-HDBK-1013/14). Washington Navy Yard, DC. www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_14.pdf	This handbook provides guidance to ensure that appropriate design, operational, environmental, cost, security, and safety considerations are included in the selection process for vehicle barrier systems. Topics covered in the handbook include: vehicle barrier requirements, vehicle barrier installation and design, and descriptions and data on commercially available vehicle barriers and passive barriers that can be constructed on site.
Naval Facilities Engineering Service Center (NFESC). 1993a. Design Guidelines for Physical Security of Facilities (MIL-HDBK-1013/1A). Washington Navy Yard, DC. www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_1a.pdf	This manual provides guidance to ensure that appropriate physical security considerations are included in the design of general facilities. Aspects considered in this manual include the pre-design phase, the assessment of physical security threats, and an overview of the design phase. Specific technical sections in the manual also describe exterior site physical security, building physical security, ballistic attack hardening, standoff weapon hardening, and bomb blast hardening.

Reference	Annotation
Naval Facilities Engineering Service Center (NFESC). 1993b. Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities (MIL-HDBK-1013/10). Washington Navy Yard, DC. www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_10.pdf	This military handbook provides guidance and detailed criteria for the design, selection, and installation of new security fencing, gates, barriers, and guard facilities for perimeter boundaries of Navy and Marine Corps installations or separate activities, and designated restricted areas.
Sandia Corporation. 2002. Risk Assessment Methodology for Water (RAM™). May.	This document is a two-volume training guide used in the RAM-W™ methodology workshops.
42 U.S.C. §300(i)(1). http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC300i-1	This web site provides the text of U.S. Code Title 42, Section 300i-1, "Tampering with public water systems."
U.S. General Services Administration (GSA). 2005. Facilities Standards for the Public Buildings Service. Washington, DC. http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8195&channelPage=%2Fep%2Fchannel%2FgsaOverview.jsp&channelId=-17304	These design standards and criteria are to be used in the programming, design, and documentation of GSA buildings.
Water Environment Federation (WEF). 2004. Interim Voluntary Security Guidance for Wastewater/Stormwater Utilities. Alexandria, VA. www.wef.org/Conferences Training/TrainingProfessionalDevelopment/WaterSecurity/	USEPA WISE ASCE/AWWA/WEF Phase 1 Documents (December 9, 2004) are available at the ASCE, AWWA, WEF, and USEPA web sites.
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. www.epa.gov/safewater/ndwac/pdfs/wswg/wswg_report_final_july2005.pdf	This report presents the consensus reached by WSWG on 18 findings that: (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. AwwaRF. Denver, CO.	This report documents the security incidents, threats, and hoaxes that have occurred involving or 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 categorization. The report reviews the incidents and discusses specific types of contaminants and the purported motivation of attackers.